



Firewalls Don't Stop Dragons

A Step-by-Step Guide to Computer
Security and Privacy for Non-Techies

Fifth Edition

Carey Parker

Apress®

Firewalls Don't Stop Dragons

**A Step-by-Step Guide to Computer
Security and Privacy for Non-Techies**

Fifth Edition

Carey Parker

Apress®

Firewalls Don't Stop Dragons: A Step-by-Step Guide to Computer Security and Privacy for Non-Techies

Carey Parker
North Carolina, NC, USA

ISBN-13 (pbk): 978-1-4842-9035-4

<https://doi.org/10.1007/978-1-4842-9036-1>

ISBN-13 (electronic): 978-1-4842-9036-1

Copyright © 2023 by Carey Parker

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Susan McDermott
Development Editor: Laura Berendson
Coordinating Editor: Jessica Vakili

Distributed to the book trade worldwide by Springer Science+Business Media New York, 1 NY Plaza, New York, NY 10004. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail booktranslations@springernature.com; for reprint, paperback, or audio rights, please e-mail bookpermissions@springernature.com.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on the Github repository: <https://github.com/Apress/firewalls-dont-stop-dragons>. For more detailed information, please visit <http://www.apress.com/source-code>.

Printed on acid-free paper

To my mother, my father, and my daughters.

Table of Contents

About the Author	xxi
About the Technical Reviewer	xxiii
Preface	xxv
Chapter 1: Here Be Dragons.....	1
I Dub Thee.....	1
An Ounce of Prevention.....	4
How Worried Should I Be?.....	7
What Should I Be Worried About?	9
Indirect Threats.....	12
A Few Final Thoughts Before We Begin	12
How to Use This Book	14
Reader Prerequisites	15
Operating Systems Covered	15
Navigating the Checklists.....	16
Objects in the Book May Seem Larger Than They Appear	18
Always Go to the Source.....	19
Updates and Bonus Content.....	19
Other Resources	20
Feedback Welcome	21
Summary.....	22
Going Further	23
Checklist	24
Tip 1-1. Take Good Notes.....	24
Tip 1-2. Determine Your Computer Type and Version	25
Tip 1-3. Determine Your Mobile Device Type and Version	30

TABLE OF CONTENTS

Chapter 2: Privacy Matters..... 33

Privacy vs. Security..... 33

 Why Privacy Matters for You..... 35

 Why Privacy Matters for All of Us 37

 Enter the Panopticon 38

Selling Privacy by the Pound..... 41

 Ever Feel Like You’re Being Watched?..... 45

Solving the Privacy Problem 47

Who Can You Trust?..... 48

Step Away from the Ledge..... 50

Summary..... 52

Going Further 53

Checklist 55

 Tip 2-1. Know What They Know..... 55

 Tip 2-2. See What Your IP Address Reveals..... 56

 Tip 2-3. Opt Out Where You Can..... 57

 Tip 2-4. Investigate Your Own Public Information 57

 Tip 2-5. Get Your Stories Straight 58

 Tip 2-6. Operate on a Need-to-Know Basis..... 58

Chapter 3: Castle Guard Certification 61

Castle Guard in Training 61

 Computer Lingo 62

 Hardware and Software..... 63

 File Manager..... 64

 Bits and Bytes..... 64

 Storage 66

 Networks (Wired and Wireless) 67

 Bandwidth 68

 Bluetooth 69

Computer and Internet Buzzwords	69
Clients and Servers	70
The Cloud.....	70
Net Neutrality	71
The Internet of Things (IoT).....	72
Know Your Enemy	72
Zero-Day Exploit	73
Malware.....	73
Hardware Bugs.....	79
Cryptic Codes and Confidential Communications	80
How the Internet Works	80
How Encryption Works.....	84
Modern Cryptography.....	91
Authentication and Message Integrity.....	95
Putting It All Together	99
Newer Isn't Always Better	101
Quantum Computing.....	101
Graduation Ceremony	102
Summary.....	103
Going Further	104
Checklist	105
Tip 3-1. ★ Don't Click Links, If Possible	105
Tip 3-2. Watch Out for Shortened URLs	105
Tip 3-3. ★ Don't Open Email Attachments, If Possible	106
Chapter 4: Get Your Castle in Order	107
Backups	107
External Hard Drive Method.....	108
Cloud Backup Method	109
Cloud Drive Method	111
Choosing Your Best Backup Solution.....	111
Keeping the Lights On	112

TABLE OF CONTENTS

Minimization: Less Is More	113
Spring Cleaning	114
Data Minimization.....	114
Update All the Things	115
Major Software Updates	116
Minor Software Updates.....	117
Summary.....	119
Going Further	120
Checklist	121
Tip 4-1. How to Change Computer Settings	121
Tip 4-2. ★ Back Up to an External Drive	131
Tip 4-3. ★ Back Up to the Cloud	146
Tip 4-4. Buy a UPS.....	163
Tip 4-5. ★ Clean Up Your Apps.....	164
Tip 4-6. ★ Turn on Auto-Update for Your OS	169
Tip 4-7. ★ Turn on Auto-Update for Your Applications	173
Tip 4-8. Download Software Safely	175
Tip 4-9. Scan Your Paper Documents	176
Tip 4-10. Shred Your Paper Documents.....	176
Chapter 5: Who Goes There?	179
How Did We Get Here?	179
May I See Some ID?	180
Something You Are	181
Something You Have.....	181
Passwordless	184
Understanding Password Strength	185
How to Crack a Password.....	185
Doing the Password Math	189
Using a Password Manager	192
Choosing a Master Password	194
Using a Passphrase	195

Doing the Two-Step.....	197
Periodically Changing Passwords.....	198
A Rose by Any Other Name	200
Summary.....	203
Checklist	205
Tip 5-1. ★ Choose a Strong Master Password.....	206
Tip 5-2. ★ Sign Up for Bitwarden.....	206
Tip 5-3. ★ Install the Bitwarden Browser Plugin	208
Tip 5-4. ★ Transfer Existing Passwords to Bitwarden	209
Tip 5-5. ★ Enable Two-Factor Authentication	213
Tip 5-6. Take a Tour of Bitwarden	217
Tip 5-7. ★ Install the Bitwarden App on Your Smartphone	218
Tip 5-8. Use Bitwarden to Fill in Passwords.....	219
Tip 5-9. Disable Password Saving on Your Browser.....	220
Tip 5-10. Delete Saved Passwords from Your Browser	222
Tip 5-11. Store Credit Cards in Bitwarden.....	223
Tip 5-12. Store Personal Info in Bitwarden.....	224
Tip 5-13. Run a Vault Health Report	224
Tip 5-14. ★ Generate Strong Passwords for Key Accounts	225
Tip 5-15. Generate and Store Offline Passwords.....	229
Tip 5-16. Peppering Your Passwords.....	230
Tip 5-17. Guard Your True Identity	232
Chapter 6: Raise the Drawbridge!	233
Macs Are Safer Than PCs.....	233
Non-admin Accounts.....	234
iCloud and Microsoft Accounts	237
Built-in Security Features	238
The Pros and Cons of Antivirus Software.....	241
Sticky Bits	242
Summary.....	244

TABLE OF CONTENTS

Checklist 245

 Tip 6-1. Upgrade Your Computer 246

 Tip 6-2. ★ Require Passwords for Computer Accounts..... 246

 Tip 6-3. ★ Create a Separate Admin Account 253

 Tip 6-4. Install Free Antivirus Software 279

 Tip 6-5. Restrict Access to Important Files..... 283

 Tip 6-6. Disable Unneeded Startup Software 288

 Tip 6-7. Don't Install Apps That Come with Peripherals 291

 Tip 6-8. ★ Turn on Disk Encryption 292

 Tip 6-9. Securely Erase Sensitive Files 297

 Tip 6-10. ★ Prepare a Computer for Sale, Donation, or Recycle 301

 Tip 6-11. Prepare Printers for Sale, Donation, or Recycle..... 303

 Tip 6-12. Enable Laptop Location Tracking..... 303

 Tip 6-13. Use Lockdown Mode (macOS Only)..... 309

 Tip 6-14. Don't Trust Other Computers..... 310

 Tip 6-15. Avoid Strange USB Devices and Ports..... 311

 Tip 6-16. Restart Your Computer Periodically..... 312

 Tip 6-17. Don't Use Adobe Reader to Read PDF Files..... 312

 Tip 6-18. Unplug or Cover Webcams When Not in Use 313

 Tip 6-19. Beware Cold Calls for Computer Support..... 313

Chapter 7: Guard the Castle Gate..... 315

 Network Overview..... 315

 Modem..... 318

 Wi-Fi Router 319

 Network Address Translation (NAT) 320

 Firewall..... 321

 Wireless Connections and Quality of Service 322

 Keep Your Gatekeeper on Your Payroll..... 323

 The Internet of Things 323

 IoT Security (or Lack Thereof)..... 324

IoT Privacy (or Lack Thereof)	325
A Note About Virtual Assistants	326
Virtual Private Network (VPN).....	328
What a VPN Is	329
What a VPN Isn't	330
When Should I Use a VPN?	331
Summary.....	332
Going Further	333
Checklist	334
Tip 7-1. Get Your Own Modem.....	336
Tip 7-2. Get Your Own Wi-Fi Router	336
Tip 7-3. ★ Change Your Default Router Password	337
Tip 7-4. ★ Update Your Router's Firmware	338
Tip 7-5. ★ Lock Down Your Wi-Fi.....	338
Tip 7-6. Use the Guest Network.....	338
Tip 7-7. Create a QR Code for Easy Guest Network Access.....	339
Tip 7-8. Put Internet of Things Devices on the Guest Net.....	340
Tip 7-9. Disable External Admin	340
Tip 7-10. Disable WPS	340
Tip 7-11. Disable Universal Plug and Play (UPnP)	341
Tip 7-12. Probe Your Router for Vulnerabilities.....	341
Tip 7-13. Disable IPv6.....	342
Tip 7-14. Change Your Default SSID	342
Tip 7-15. Register Your Devices.....	343
Tip 7-16. Periodically Reboot Modem, Router	344
Tip 7-17. Disable Network Sharing Features.....	344
Tip 7-18. Change Virtual Assistant Privacy Settings.....	344
Tip 7-19. Use a VPN	345
Tip 7-20. Avoid Public Wi-Fi and Use Cellular Data	346
Tip 7-21. Disable Auto-Connect to Wi-Fi.....	346
Tip 7-22. Dumb Down Your Smart TV	347

TABLE OF CONTENTS

Chapter 8: Spies in Your Midst 349

 Certified Secure 350

 Trust the ID, Question the Issuer..... 353

 Tracking Tech 355

 The Webs We Weave..... 356

 You’re Being Stalked 359

 Hey, I Know You 360

 Tracking in Real Life..... 362

 Information Leakage 364

 DNS Queries 364

 Referer Header 365

 Web Form Data Leakage 365

 On the Ethics of Ad Blocking..... 366

 Choose Your Weapon..... 368

 Most Secure Browser 369

 Most Private Browser 369

 And the Winner Is... 370

 Summary..... 372

 Going Further 373

 Checklist 374

 Tip 8-1. ★ Use a Privacy-Protecting Browser 374

 Tip 8-2. ★ Configure Browser for Security and Privacy 375

 Tip 8-3. ★ Change the Default Search Engine 384

 Tip 8-4. ★ Install Password Manager Add-on 385

 Tip 8-5. ★ Install uBlock Origin Add-on 391

 Tip 8-6. Remove All Unnecessary Add-ons..... 392

 Tip 8-7. Be Careful on “Shady” Sites..... 394

 Tip 8-8. Beware of Pop-Ups Offering/Requiring Plug-ins..... 394

 Tip 8-9. Use Private Browsing 394

 Tip 8-10. Delete Personal Info from Google Searches..... 395

Tip 8-11. Be Careful When Entering Form Data.....	396
Tip 8-12. Use a Privacy-Respecting DNS Provider	396
Tip 8-13. Use DNS over HTTPS (DoH)	398
Chapter 9: Coded Messages and Wax Seals	401
Email	402
Text Messaging	404
Spam and Spoofed Messages.....	405
Looks Can Be Deceiving	406
Redirecting Links and Tracking Pixels	407
Dealing with Spam	408
How to Recognize a Fake Email	409
Pseudonyms R Us	412
Securing Communications with End-to-End Encryption	414
Encrypting Message and Files.....	415
Secure Text Messaging.....	419
Secure Video and Voice	420
Summary.....	421
Going Further	422
Checklist	423
Tip 9-1. Scan Files Before Sending	423
Tip 9-2. Encrypt Your Message and Files	423
Tip 9-3. Send Files Securely Using the Web	430
Tip 9-4. ★ Use a Secure Email Service.....	431
Tip 9-5. ★ Use Secure Messaging Apps	431
Tip 9-6. Use Secure Voice and Video Apps	432
Tip 9-7. Open Attachments Safely	433
Tip 9-8. Use Email Aliases	434
Tip 9-9. Review Unused Email Accounts	436
Tip 9-10. Monitor Your Account Activity.....	437
Tip 9-11. Deal Properly with Spam.....	437

TABLE OF CONTENTS

Chapter 10: Protect the Market and Town Square..... 439

Banking and Shopping Online..... 439

 Credit vs. Debit Cards..... 439

 Online Banking 440

 Mobile Payment Systems 441

 Financial Account Aggregators..... 442

Credit Bureaus and Identity Theft 443

 Planting Your Flag..... 444

Cloud Storage Services..... 445

Social Media 447

Giving Away Your DNA..... 449

Summary..... 451

Going Further 452

Checklist 453

 Tip 10-1. ★ Lock Down Your Apple/Microsoft Accounts 453

 Tip 10-2. ★ Enable Two-Factor Auth Wherever You Can 470

 Tip 10-3. ★ Use Credit Cards Online (Not Debit Cards)..... 470

 Tip 10-4. Use Virtual Credit Card Numbers..... 470

 Tip 10-5. Be Careful Using Mobile Payment Services 471

 Tip 10-6. Give Your Credit Card Company a Heads-Up 472

 Tip 10-7. Set Up Restrictions on Your Financial Accounts..... 472

 Tip 10-8. Turn On Account Alerts 473

 Tip 10-9. ★ Freeze Your Credit..... 473

 Tip 10-10. ★ Plant Your Flag..... 474

 Tip 10-11. Use Private Cloud Storage Services 475

 Tip 10-12. Don't Broadcast Your Travel Plans..... 476

 Tip 10-13. Read the Terms of Service (or Not) 476

 Tip 10-14. Review Social Media Privacy Settings 477

 Tip 10-15. Don't Share Your Email Credentials..... 478

Tip 10-16. Don't Sign In Using Facebook, Google.....	478
Tip 10-17. Stop Tagging Other People in Photos	479
Tip 10-18. Scrub File Metadata Before Sharing	479
Tip 10-19. Stop Oversharing Personal Information	480
Tip 10-20. Close Accounts You Don't Use	481
Tip 10-21. Delete Your Facebook History	482
Tip 10-22. Avoid DNA Heritage Services.....	482
Tip 10-23. Account Recovery Questions: Lie	483
Tip 10-24. De-Google Your Life.....	484
Tip 10-25. Avoid TikTok Entirely.....	484
Chapter 11: Watch over the Lads and Lasses	485
The Internet Is Everywhere	485
The Internet Is Forever.....	486
Cyberbullying	487
Big Brother for Little People.....	488
Porn and Predators	489
Don't Panic.....	490
Summary.....	491
Going Further	492
Checklist	493
Tip 11-1. ★ Create a Dedicated Account for Each Child.....	493
Tip 11-2. Use Parental Controls for Young Children.....	493
Tip 11-3. Creating Email Accounts for Young Children	499
Tip 11-4. Research Before Your Kids Sign Up.....	500
Tip 11-5. Teach Your Kids to Protect Their Identities	500
Tip 11-6. Be Able to Access All Accounts and Devices	500
Tip 11-7. Honor the Age Restrictions.....	501
Tip 11-8. Friends Must First Be Met in Person	501
Tip 11-9. Lock Down Chromebook Settings	501

TABLE OF CONTENTS

Tip 11-10. Teach Kids the Rules of the Internet..... 502

Tip 11-11. Beware of Connected Toys 502

Tip 11-12. Keep Computers in a Common Area of the House 502

Tip 11-13. Use Family-Friendly DNS..... 503

Tip 11-14. Use Device Tracking (Judiciously and Fairly) 503

Tip 11-15. Create a Contract for Your Kids 504

Tip 11-16. Great Parental Resources..... 504

Chapter 12: Armored Carriage: Your Mobile Castle..... 505

 iPhone vs. Android 505

 iOS Is More Secure Than Android 506

 iOS Is More Private Than Android 507

Wireless Madness..... 508

To Hack or Not to Hack..... 509

 Third-Party App Stores 510

A Mole in Your Pocket 511

 Biometric vs. PIN Code Locks..... 512

Give and Take..... 514

Summary..... 516

Going Further 516

Checklist 517

 Tip 12-1. ★ Back Up Your Phone to the Cloud..... 518

 Tip 12-2. Back Up Your Phone to Your Computer..... 520

 Tip 12-3. ★ Keep Your Device Up to Date..... 521

 Tip 12-4. ★ Restrict Application Permissions 522

 Tip 12-5. ★ Lock Access to Your Device 523

 Tip 12-6. Enable Emergency Lock Mode 524

 Tip 12-7. ★ Use Secure Messaging Apps..... 525

 Tip 12-8. ★ Limit Ad Tracking..... 526

 Tip 12-9. Remove Unused Apps..... 527

 Tip 12-10. Enable (Self) Tracking..... 528

Tip 12-11. Use Firefox Mobile Browser	529
Tip 12-12. Avoid Cheap Android Phones.....	529
Tip 12-13. Get a Burner Number	530
Tip 12-14. Use a Mobile VPN	530
Tip 12-15. Don't Use Mobile Antivirus	531
Tip 12-16. Disable Wi-Fi Auto-Connect.....	531
Tip 12-17. Know Your Rights When You Travel.....	532
Tip 12-18. Disable Wireless When You Can	532
Tip 12-19. Erase Your Device Before Getting Rid of It	533
Tip 12-20. Enable Medical ID.....	535
Tip 12-21. How to Safely Lend Someone Your Phone.....	536
Tip 12-22. Don't Hack Your Device	537
Tip 12-23. Periodically Restart Your Phone	537
Tip 12-24. Never Install Spyware	538
Tip 12-25. Check Your Phone for Spyware	538
Tip 12-26. Use Lockdown Mode (Apple Only).....	539
Tip 12-27. Use a USB Condom.....	540
Chapter 13: Odds and Ends	541
Privacy for Cars.....	541
Tip 13-1. Erase Phone Data Before Selling Your Car	542
Tip 13-2. Don't Pair Phones with Rental Cars.....	542
Tip 13-3. Don't Use Insurance Trackers.....	542
Tip 13-4. Don't Install Car Maker Apps.....	543
When Bad Things Happen	543
Tip 13-5. Recovering a Hacked Account.....	544
Tip 13-6. Website Password Breach.....	545
Tip 13-7. Your Computer Has a Virus	546
Tip 13-8. You've Got Ransomware!.....	547
Tip 13-9. Restoring a Lost or Messed-Up File	548

TABLE OF CONTENTS

And When I Die..... 548

 Tip 13-10. Get a Will 549

 Tip 13-11. Add a Backup to Your Safety Deposit Box 549

 Tip 13-12. Ensure Access to Your Accounts 549

 Tip 13-13. Ensure Access to Your Two-Factor Device..... 550

 Tip 13-14. Appoint a “Digital Executor” 550

 Tip 13-15. Stop ID Theft After Death..... 551

Gold Stars and Tinfoil Hats..... 552

 Tip 13-16. Nuke Your Hard Drive Data 552

 Tip 13-17. Install Haven on an Old Android Phone 552

 Tip 13-18. Add a Dedicated Guest Wi-Fi Router 553

 Tip 13-19. Install Custom Router Software..... 553

 Tip 13-20. Install a Reverse Firewall 554

 Tip 13-21. Install and Use PGP 554

 Tip 13-22. Host a PGP Key-Signing Party 555

 Tip 13-23. Use Tor to Protect Your Identity 555

 Tip 13-24. Need to Blow the Whistle? Use SecureDrop..... 555

 Tip 13-25. Set Up a Virtual Machine 556

 Tip 13-26. Use a Dedicated Secure Computer..... 556

 Tip 13-27. Shut Your Pi Hole 557

 Tip 13-28. Use Open Source Hardware 558

 Tip 13-29. De-Google Your Android Phone..... 558

Chapter 14: Parting Thoughts..... 559

 Keep Calm and Carry On 559

 The More the Merrier 560

 The Case for Optimism..... 560

 Don’t Take This Lying Down 561

 Summary..... 564

Checklist	565
Tip 14-1. Expand Your Security and Privacy Education	565
Tip 14-2. Fight the Good Fight (or at Least Fund It)	568
Tip 14-3. Spread the Word, Help Others	569
Glossary	571
Index	577

About the Author



Carey Parker was born and raised in Indiana, an only child who loved to tear apart his electronic toys and reassemble them in interesting ways. He began programming computers in middle school when personal computers were just starting to become popular. For years, these twin interests percolated until he attended Purdue University and learned you could get paid to do this stuff—it was called electrical engineering (EE)! After obtaining a bachelor's and a master's degree in EE, Carey launched his career in telecommunications software development at Bell Northern Research (a.k.a. the “Big Nerd Ranch”). Over the next 28 years, Carey wrote software for multiple companies, large and small, and lived in various cities across the southern United States. In recent years, particularly after the Edward Snowden revelations in 2013, he became deeply concerned about computer security and online privacy. In 2014, he combined his passion for computers, cybersecurity, and fantasy novels with the long-time desire to write a book: *Firewalls Don't Stop Dragons*. As of October 2020, Carey has retired from the rat race of the 40-hour workweek and is now focused on educating as many people as possible about cybersecurity and personal privacy through his book, blog, podcast, newsletter, seminars, and public speaking.

About the Technical Reviewer



Now semiretired, **Dean Keith** is an adjunct instructor teaching technology classes for senior citizens at Dallas College in Dallas, TX. A popular class Dean teaches is a computer security class using this book! He also teaches classes on how to use an iPhone, Windows 10, and Microsoft 365. Dean and Kathy have two adult daughters who still, periodically, ask him for help with technology.

While attending Rutgers College in the early 1970s when the faculty did not recognize computer science as a legitimate degree, Dean was approved for an individualized major with courses from the computer science major at Livingston College (part of Rutgers University) and the economics major at Rutgers.

Having grown up in a military family and attending three different high schools in three parts of the country, Dean and Kathy settled in Texas after he served (4.5 years) in the USAF. Moving from Aviano, Italy, to Texas was a bit of a culture shock, but the weather there is much warmer than it was during those four years at the Glasgow Air Force Base in Montana.

As the years went by, Dean kept up with changes in technology from using a TI-99a to a Commodore 64 to a Windows PC. Dean is honored to have had a small part in the formidable work Carey is doing to help educate people about keeping safe in the digital world in which we live.

Preface

Let's take a little quiz. If I asked you right now to rate your personal computer security on a scale from one to ten—with ten being Fort Knox and one being a wet paper bag—what rating would you give yourself? Seriously, give that some thought right now. Try to pick an actual number.

Unless you're a techie person, I'm going to guess that you don't really know how to pick a meaningful number. And that almost surely means your ranking is closer to the wet paper bag end of the scale. Now, do you really need to be as secure as Fort Knox? No, of course not, and that's not what this book is about. However, there are many things you can do (or avoid doing) that will significantly increase your security and privacy, and this book is chock-full of them. You don't have to do them all—even I don't do them all—but I firmly believe that everyone should at least consider implementing each of the tips described in this book.

I'm guessing that a few questions are popping into your mind right now. Do I *really* need to read this book? Do I need to be a “computer person” to understand it? How much effort is this going to take? All good questions! Let's answer them right up front.

The answer to the first question is easy: yes! So the real question is: *Why* do you need to read this book? Because so many important parts of our lives are on the Internet now—banking, shopping, paying bills, telehealth, gaming, you name it. And it's not just our desktop computers that are connecting to the Internet. It's our laptops, smartphones, tablets, and all manner of “smart” devices. Unlike the days of dial-up modems, our devices are now connected 24/7. These facts have not gone unnoticed by the bad guys. As the famous saying goes, why do criminals rob banks? Because that's where the money is!¹ You need to read this book because it will make you safer—significantly safer, if you follow most of the advice. In fact, not only will it make you safer but it will also make those around you safer, even if they don't do any of the things I recommend in this book. (I'll explain that bit of magic later in the book.)

¹This line is often falsely attributed to bank robber Willie Sutton: <https://www.snopes.com/quotes/sutton.asp>

Who This Book Is For

This book is for my mother, my friends, my neighbors, and all the other totally normal, everyday people like them: people who use computers and smartphones but don't really know (or frankly care) how they work. This book is for people who just want to know what they need to do to protect themselves—step by step, without judgment, and with as little jargon as possible.

I've structured this book to give you the maximum benefit with the least amount of effort (and cost). The purpose of this book is to cut to the chase and clearly explain the things you need to do to protect yourself in this constantly connected world of ours. Along the way, if you want to learn a little of the “why” and “how,” using language you can understand, I've included a good bit of that too. In this book I use a lot of helpful analogies to explain these technical topics in ways that everyone can understand. I also throw in some fascinating stories and interesting anecdotes that help drive the points home. However, I went further than just trying to make this book easy to understand—I tried very hard to make it entertaining, as well! Trust me, I've read a gazillion dry, boring tech books in my life—I've taken great pains to make sure this book isn't one of them.

“But can't I find all this information on the Web?”, you ask. Sure, you can! The problem is not lack of information—the problem is that there is *too much*. How do you find what you need and weed out the stuff you don't? Most people wouldn't even know what to search for. Even if you knew some of the technical terms, you'd still have to read a ton of info from different sources and figure out what parts are relevant to you. To make matters worse, the common news sources that most people turn to have done a horrible job covering these topics (when they cover them at all). They tend to focus on the wrong things, crank the hype up to silly levels, and generally give poor advice. There are lots of good websites that get it right, but you've probably never heard of them, and they tend to be very technical. If only someone could find all the most important stuff, break it down into manageable pieces, and explain it so anyone can get it!

That's the main reason I wrote this book. I firmly believe that in this day and age, everyone needs a fundamental understanding of computer safety—not only for each individual's sake but also for everyone's sake—because we're all connected now. It's not just about protecting ourselves from criminals who want our money but also from corporations and governments that want to track what we do, what we say, whom we associate with, what we buy, what we read... well, basically everything. It's important

that we understand all of these threats. My goal is not only to give you the tools you need to protect your data and your privacy but to arm you with the knowledge you need to be an informed consumer and an informed citizen. We need to vote with our wallets *and* at the ballot box.

Helpful for Techies Too

As a software engineer, many of my friends are techies. While they understand computers and the Internet, that doesn't mean they understand security and privacy. It's a highly specialized area within my field, and frankly it's just something that most people don't spend enough time thinking about. Even my tech buddies have learned from the tips, tools, and techniques that I cover in this book.

But if you're a techie, then your family and nontechnical friends probably look to you for advice on "computer stuff." You field questions about networking, computers, viruses, online scams, web tracking, and on and on. Believe me, I know—I get those same queries. I'm sure you do your best to answer their questions or to at least direct them to some helpful resources you're aware of. Maybe you share important security and privacy tips on social media from time to time. If you're a real softie, you might even sit down with them to help with some of these things. But you can only do so much.

That's where this book comes in. Not only can you learn stuff for yourself but you can use the book to save you hours and hours of consulting. The purpose of this book is to walk the average, non-techie person through the basic things everyone should do to protect their computers and their data. It also takes the time to explain why these things are important and how they work, at a high level. This is the stuff you wish you had the time and patience to explain to all your friends and family. It comes complete with step-by-step instructions and pictures. Hit the "easy button"—just give them a copy of this book!

What's New in This Edition

I was lucky enough to be able to stop working a 9–5 job about two years ago. When COVID hit, my company (like most companies) took a significant hit to their revenue. They needed to lower headcount. To their credit, they decided to start with voluntary attrition—they offered early retirement packages to senior employees. I honestly would never have considered retiring as early as I did without this offer. I did the math and was

PREFACE

shocked to find that I could make it work. So I did it. Two years later, I have zero regrets—it was absolutely the right decision for me. Several of my friends are jealous, but also tell me that they're a little scared to retire because they have no idea what they would do with all that free time.

Lucky for me, I already had a retirement gig lined up! Until I quit work, the time I spent on the book, the blog, the newsletter, and the podcast was all on top of my day job. Once I retired, I was finally able to focus on my passion project! I attended conferences (most of them virtual, due to the pandemic). This allowed me to meet more experts in the industry. Through those contacts, I found new people to interview on my podcast. It was a truly synergistic thing, a virtuous cycle. In the last two years, I've expanded my knowledge of privacy and security, learned more techniques to protect them, refined my advice, and honed my messaging.

But a lot has also changed in the realm of security and privacy in the last two years. Yes, there have been some serious cyberattacks and data breaches. But what's more significant to me is that we're finally starting to see changes in people's attitudes. Governments at all levels are starting to act. Companies—new and old—are beginning to offer more secure and private products. I feel like we may have finally hit a tipping point. (I sure hope we have.)

Security and privacy have never been more important than they are right now. As consumers, we need to choose more secure and private products—and demand them if they don't exist. As citizens, we need to elect representatives who will fight to improve our security and privacy. To do those things, we must be educated.

This new edition of the book is by far the best one yet. I've captured all the things I've learned in the last two years and updated all the existing advice with the latest and greatest information. I've added many more tips and updated several others. This book is truly a one-stop shop for protecting your computers and your data.

Your Road Map to Security

So what exactly can you expect to find in this book? I did my best to cover every topic that I felt was important—and turns out, that's a lot of ground to cover. I laid the topics out very carefully and methodically, like a road map—here is the path we're going to take together:

Chapter 1: Before we can try to improve our security, we need to take a minute to think about what it is that we're trying to protect and what we're trying to protect it from. I also want to level with you about how bad it is out there and set some expectations on how much we can really do to make ourselves safer. (Spoiler alert: It's not as bad as you think.)

Chapter 2: You can't talk about security without also talking about privacy. It turns out that this is where some of the biggest dangers lie. While you may be aware of some of the threats to privacy, I'm guessing you don't fully appreciate the breadth of the problem or the depth of the consequences. In this chapter, I make my case for why privacy is so important and why things are so bad right now.

Chapter 3: In this chapter, I'll review several important concepts to set the stage for later chapters. Some of this will just be a review for many of you. But I will also delve into topics that I'm guessing will be new to you and are very important to understand at a high level—like how the Internet and encryption work. Don't worry! I've put together some fun analogies that will help you make sense out of all of this.

Chapter 4: Before we start making a bunch of changes, it's crucial that we do some housekeeping first. We need to make sure we have backups of all our stuff and clean out the cruft. Think of it like tidying up your workshop and sharpening your tools before starting a big project.

Chapter 5: The first major topic I'll cover is authentication—that is, passwords and other things we do to prove that we are who we say we are. Strong passwords are critical for locking down our computers, our accounts, and our data. This is the foundation we'll build on for many other aspects of security and privacy.

Chapter 6: Now that we've laid the groundwork, we can start our quest in earnest! We'll start by securing your computer and the related accounts. I'll address perennial topics like the need for antivirus software and whether Macs are more secure than PCs. I'll also show you how to get the most from the security features that are built into macOS and Windows.

Chapter 7: Nothing defines modern life more than the Internet. Our computers and smartphones are all interconnected now. To make matters much worse, we also now have tons of "smart" devices in our homes—and it turns out that they're pretty dumb when it comes to security.

PREFACE

Chapter 8: So much of our daily lives now revolve around the World Wide Web. This only accelerated during the global pandemic when we were forced to stay home. We arguably spend more time in the virtual world now than in the physical one. So it's critical that we know how to surf the Web safely, particularly when it comes to preserving our privacy.

Chapter 9: When we surf the Web, our browsers are communicating with faceless servers. But when we send an email, exchange text messages, or participate in a Zoom call, we're exchanging information and data with real, live people. To do this safely, we need to verify whom we're talking with and make sure that no one else can eavesdrop on our conversations.

Chapter 10: We have accounts online now for just about everything: shopping, banking, investing, sharing files, healthcare, and much more. Most of us also have social media accounts where we share...well, everything. If one of these accounts is compromised, we may not only lose money or sensitive information, but we may also jeopardize our other accounts. Hacked accounts can even be used to scam people who are connected to us.

Chapter 11: Kids today have grown up with the Internet and smartphones. These are powerful tools that have amazing benefits but can also cause serious harm. Without the wisdom of life experience, it can be easy to make bad decisions. As parents and guardians, we need to take special care to educate our kids about the risks without denying them the rewards.

Chapter 12: For many people today (particularly younger people), smartphones have supplanted computers. While they perform many of the same functions, they are vastly different when it comes to security and privacy. I'll show you how to configure them properly and use them safely.

Chapter 13: In this penultimate chapter, I'll cover a handful of topics that didn't really fit in anywhere else—like privacy and security for your car (yeah, that's a thing now). And if you want to kick things up a notch or two, I'll give you some of my favorite bonus tips.

Chapter 14: In the final chapter of the book, I'll offer my thoughts on what the future holds with respect to computer security and data privacy. There is reason to hope that things will get better, but to maximize the odds, we need to stay educated and get involved. I'll give you several ways to do both.

CHAPTER 1

Here Be Dragons

Before we get into the nitty-gritty details of securing your devices and your data, I want to provide some motivation and set some expectations. In this chapter, I'll help you understand what your real risks are and how safe you can expect to be. Being that this is the first chapter, I'll take this opportunity to explain how this book is organized and help get the most out of it.

Before you can solve any problem, you must first understand what the problem really is—the rules, goals, parameters, and context. When it comes to cybersecurity, we first need to know what it is that we're trying to protect and who we're trying to protect it from. We call this the *threat model*.

I know, I'm already throwing around tech jargon! But I'm now going to explain that jargon in terms that will be easy to understand. I love to use analogies at times like these, and I find that you can explain lots of aspects of computer security using the example of defending a medieval castle. You have people and valuables you would like to protect from various types of threats and perils. In the old days, people defended their stuff by erecting physical barriers like walls and moats and sometimes even hired armed guards. It turns out that these concepts work well to describe computer security too. With that in mind, let's examine the fundamentals of computer security by comparing it to safeguarding a classic medieval stronghold.

I Dub Thee...

Congratulations! Your king, in his infinite wisdom and generosity, has granted you a lordship and has given you huge tracts of land! You have been charged with populating and protecting this new territory, all the better to generate more tax revenue for your liege. To this end, you have been provided a fixed budget of gold and raw materials. Now what? What do you do?

Well, the first thing you need to do is to determine what and whom you need to protect. Obviously, you will need to protect yourself, as well as your gold and other valuables. You will also need to protect the natural resources of your realm—farmlands, mines, quarries, forests, and sources of fresh water. You will want to control access to your realm, particularly the highways and waterways. The safety of the people within your realm is also paramount. This isn't just altruistic. Sure, you love your people, but they are also needed to farm the land, work the mines, create the goods, pay the taxes, and populate your army and personal guard.

The next thing you need to determine is what and whom you need to protect your people and resources from. Unfortunately, the threats to your people and assets are many and varied.¹ Not only do you need to consider malicious marauders and adversarial armies, but you must beware of feral fauna, perilous pestilence, and even crafty con men. (Oh my!) It's also helpful to understand the resources of your opponent. Are they well-funded? What types of weapons do they possess? What attack techniques do they employ? Last but certainly not least, you need to understand the motivations of your attackers. Are they greedy or just hungry? Are they looking to make some sort of political or social statement? Do they have a reason to target you specifically?

You have a vast realm but only finite resources. You want to keep out the bad guys, but you must still allow for trade and travel. There are many possible attackers, but the risk of attack from each type of adversary is not the same. Likewise, while you have many different types of people and assets to protect, let's face it—you're of the strong opinion that some are more important than others (you and your gold, for instance). In short, you will need to make some trade-offs. Security is *always* about trade-offs. But now that we've done your threat analysis, you have a much better idea where to spend your limited resources.

As a consumer with a finite budget, you also need to evaluate your threats and decide where to spend your time and money. Luckily for you, I've done most of that work for you in this book!

It should be noted that if your attackers are much better funded than you are or have a lot more resources, then you're pretty much screwed. For example, if the Russian mob or the National Security Agency (NSA) wants to specifically target you, as an individual, you'd

¹ I really wanted to say “myriad and legion” here, but it sounded a little too pretentious. But I also thought it sounded really cool, so I've said it here. Now I've had my cake and eaten it too. Because what good is cake if you can't also eat it? Who buys a cake with no expectation of ever consuming it? I never understood that expression.

be hard-pressed to stop them. In our analogy, this would be like trying to defend your realm against a dragon. Prior to Edward Snowden's shocking revelations in June 2013, I think many people would have put the likelihood of mass warrantless surveillance on par with that of the existence of dragons—something crazy people wearing tinfoil hats might have raved about but almost surely wasn't commonplace. But to rework the classic line from *Catch-22*, just because you're *not* paranoid doesn't mean they're not out to get you.

If our fictional lord believed that dragons were real and posed a potential threat to his people and his stuff, what could he *reasonably* do to defend against them? No wall could be built high enough to stop a flying beast. Regular weapons would be mostly useless against such a powerful, magical creature. You could certainly *try* to construct some sort of domed fortress and an array of mighty, dragon-sized weaponry, but you would probably go bankrupt in the process. Even if this could be done, how exactly would you test these defenses? As if that weren't enough, it might well be that the act of attempting to create such a worthy stronghold would actually *attract the attention of the dragon*! Why else would someone build such a fortress unless they had something extremely valuable to protect (such as hordes of gold and jewels)? No, the only real hope of security in the face of such an adversary would be to hide in a deep, dark cave, strive to escape notice, and remain out of reach. But what sort of a life is that for your family and your subjects?

The point of this book (and the inspiration for the title) is that you shouldn't be trying to defend yourself against dragons. Furthermore, in our analogy, you're not the lord—you're a commoner. You don't have a lot to protect compared with rich people or large corporations. And yet, what you have is yours, and you would like to take some reasonable, cost-effective measures to safeguard your family and possessions. Think about your current residence. You probably have tens of thousands of dollars' worth of stuff inside—clothes, electronics, jewelry, and furniture. But what stands between burglars and all that stuff? Probably a simple dead bolt that costs \$25 at the hardware store. Could it be picked? Yes, without a doubt. (You'd be surprised at how easily standard door locks can be picked. I learned how to do it in about 15 minutes.) And yet, in most neighborhoods, this simple lock is enough.

By the same token, your goal isn't to protect your computer and its contents from the Russian mob or the NSA. The only way you could hope to prevent that would be to go "off the grid." Just in case you're curious, here's how that might work. First, buy a brand-new laptop (still sealed in shrink wrap) from a big-box store. Before you even power it up, open the laptop chassis and completely remove any hardware necessary for wireless communication (e.g., the Wi-Fi and Bluetooth chips). Set up your new computer in a

windowless basement. Line the walls and ceiling of the basement with wire mesh or metal foil to block radio signals. Never, *ever* connect the laptop to the Internet or to any sort of peripheral device (mouse, printer, or anything with a USB plug).

Now...how useful would that be? A computer that can't connect to the Internet is almost useless today. But even if you could live with all of this, these drastic security measures still wouldn't stop a law enforcement officer with a warrant or a burglar who breaks into your home. If you really need to protect yourself from this sort of threat—for example, if you're a political dissident, corporate whistleblower, or just uber-paranoid—then the advice in this book isn't going to be sufficient. And I didn't intend it to be.

The point here is that, statistically speaking, the Russian mob and the NSA are not likely to single you out *specifically*. For the average person, the most common threats are opportunistic hackers, automated attacks, and mass surveillance—that is, attacks that are general in nature, not targeted. For these threats, you can do quite a bit to protect yourself without spending a lot of time or money, and that is the focus of this book.

An Ounce of Prevention

So now that we've thoroughly examined our situation, what is our goal? How secure do we need to be? Another tried-and-true technique for solving a problem is to break it down into parts. Security generally has three phases: before, during, and after—more formally referred to as prevention, detection, and recovery. Prevention is about trying to keep something bad from happening in the first place. Detection is about knowing definitively that something bad is happening right now or just happened. And recovery is about repairing or mitigating the damage after that bad thing happens. Obviously, most people prefer to focus on prevention so that detection and recovery will be unnecessary. But no security plan is complete without all three.

Let's return to our newly minted lord and the defense of his realm. The most common defense mechanism in medieval times was the venerable castle. It's not practical to build a 75-foot-high wall around the entire realm, so a lord would build walls around the most important stuff. Castles were usually built on high hills to better monitor the surrounding countryside for incoming threats and to put attacking armies at a disadvantage. In times of war, the peoples of the realm could come within the walls for protection. Castles were built mostly to defend against people on foot or on horseback. There were no airplanes, so you didn't need to protect yourself from the air. But the walls had to be high enough to

stop attackers with ladders, arrows, and maybe stuff launched from catapults. In addition to walls, castles often had moats surrounding the walls to make it difficult for opposing armies to scale them. Because people still needed to come and go, the walls required at least a few openings. You would fortify these openings with large wooden or iron gates, sometimes even multiple, staggered sets of gates per opening. Armed guards, charged with evaluating who would be allowed to pass (in either direction), would protect these openings. The walls and interior grounds were also patrolled by a different set of guards who were charged with identifying and detaining bad people who might have somehow gotten through the outer defenses.

Castles had *defense in depth*. That is, they didn't have just one mechanism for keeping out attackers; they had many. Each mechanism was different, not just because different attackers had different capabilities but also to diversify the overall fortifications in case the attacker found some clever way to neutralize one of the defenses. Some defenses were passive, like the walls and the moat. Once in place, they required little to no maintenance. Other defenses were active, like the castle guard. The guards could think for themselves, take orders, and evaluate and respond to individual threats on the fly. Once given comprehensive orders and training, though, even the guards could function pretty well on their own.

It turns out that setting up defenses for your computer is similar in many ways to defending a castle. First, your main gate is your Internet router. This is what separates you from the outside world, from both good people and bad. You need to have access to the outside world to get your food, water, and supplies, as well as to sell your goods, but you have to be careful not to let the really bad guys inside. Your router has a built-in mechanism for this called a *firewall*. Using the castle analogy, the firewall allows people from inside the castle grounds to get out and come back, but it prevents all foreigners from entering unless you say it's okay. That is, the firewall allows your computer to initiate connections to the Internet (like google.com) and knows to allow the recipient to reply to your request (like giving you back your search results). But if something on the Internet tries to initiate contact with your computer, the connection is refused (or simply ignored), unless you've given it explicit instructions to allow the incoming request. By default, almost all external connections are refused by firewalls.

Antivirus (AV) software is sort of like your armed guards. They actively watch your system for suspicious behavior, and if they find it, they try to stop it. Often the AV software will then make you aware of the suspicious behavior and ask if you want to allow it. But if it's sure that it found something bad, antivirus software will usually just go ahead and neutralize it for you.

But not all threats to your computer come from the Internet. Gaining physical, in-person access to your computer, while not as likely, is still a real threat. In this case, your “castle walls” are made of 2 × 4s and drywall. Your “moat” is just a well-lit yard with some thorny shrubbery in front of the windows. As long as your computer is inside your home or some place you trust, you’re counting on the locked doors, solid walls, and other physical features to keep bad people away. However, if you have a laptop and you take it out of your home, then you have a lot less physical protection—maybe a locked car or just a laptop bag. At that point, *you* are the best protection—keeping the laptop with you, in a bag, probably over your shoulder. For laptops, you really need to set a password for your computer so that if someone does manage to steal or gain physical access to it, they can’t actually access your data. You should also encrypt your hard drive, particularly on laptops. There are sneaky ways to get at the laptop data without having to log in, so encrypting the data on your drive will make that data useless if the attacker manages to circumvent the login process.

This is defense in depth. You should have multiple layers of security for your computer and the data it contains. The more layers, the more secure you’ll be. This book will help you add those layers.

We won’t spend a lot of time in this book on detection. Determining that your computer is actively being attacked or has recently been attacked is tricky to do. Antivirus software can help, but to do this right, you need more sophisticated software, like an *intrusion detection system* (IDS). Intrusion detection systems have elements that are similar to firewalls, but whereas firewalls are generally used to prevent intrusion in the first place, an IDS will monitor background activities and communications on the computer for signs that the attackers have already gotten in and are trying to do bad things. Most intrusion detection systems are marketed toward owners of large, public servers.

In our analogy, castle guards are charged with monitoring the people moving around within the walls, looking for suspicious behavior and illicit communications with outside agents. When intruders are identified, alarms are sounded, and the rest of the guard is put on high alert until the threats have all been identified and neutralized. If guards at the gates are like antivirus software, then the elite castle guards roaming the interior grounds are more like an intrusion detection system. The two functions are similar but differ in scope and complexity.

The role of detection is quite important in other areas that we see every day. For example, the sealing wrappers and pop-up lids on food products are there to tell you whether the jar or bottle has already been opened. The paper or foil seals covering

the openings of over-the-counter medicine were implemented as a direct result of the Tylenol murders in Chicago in the early 1980s. The seal is there not to *prevent* tampering but to make tampering *evident*. If you see the seal has been broken, you know someone has been messing with it, and therefore you shouldn't use it. In the old days, wax seals were used to secure important letters—not to prevent them from being opened but to make it obvious if someone had opened the letter prior to the intended recipient.

Despite your best efforts, you may not be able to prevent all attacks, so you also need a plan for handling the case where something bad does happen. In some cases, if you know your security has been compromised, you can take steps to mitigate the impact after the fact. You can run malware removal tools, change your passwords, close your accounts, or remotely wipe your data in the case of a stolen computer or device. We'll discuss all of these in this book.

So, to summarize, our primary goal is to prevent bad things from happening in the first place. And because security is never absolute, our secondary goal must be to prepare ourselves to respond if something gets past our defenses.

How Worried Should I Be?

I'd say people fall into three camps when it comes to worrying about computer security. There's a large camp of people who are blissfully ignorant. They like their computers and gadgets but don't give a lot of thought about security. Let's call this Camp Pollyanna. In my experience, people in this camp tend to be younger. They've grown up with computers and smartphones. These devices are an integral part of their lives, and they can't imagine being without them. They probably haven't had anything bad happen to them, and they feel safe enough. (They're almost surely not.)

There's another camp of people who are intimidated by computers and online life in general. They refuse to shop or bank online, but maybe they send some emails, surf the Web to look something up, and dabble in Facebook. This would be more like Camp Luddite.² In my experience, the folks in this camp tend to be older—they didn't grow up with computers and can live just fine without them. But in today's world, computers are everywhere. We can no more avoid them than we can avoid horseless carriages.

²The term comes from a group of English workers in the early 1800s who destroyed the newfangled textile manufacturing equipment because they felt it was threatening their livelihoods. A Luddite is someone who shuns new technology.

Then there's a small camp of folks who understand the likely risks, take proper precautions, and proceed confidently with a wary respect for the dangers. I like to call it Camp Goldilocks—not too scared, not too indifferent, just cautiously confident. The goal of this book is to bring everyone into this camp.

As I alluded to earlier, the threats that most people need to worry about in the virtual world are mostly environmental or indiscriminate. In the real world, this is akin to random crime and general misfortune. What are your odds of having your house broken into or being injured in a car accident? It depends on where you live and how you drive, certainly, but it's still somewhat arbitrary. But you can always take precautions that will lower your odds and mitigate your losses. We wear a seatbelt and maybe spend a little extra money for a car with lots of airbags. We lock our house when we leave and maybe even install security cameras. These are inconveniences we've decided to live with and costs we've decided we're willing to pay.

Despite the fact that computers and even the Internet have been around for decades now, we still haven't really gotten used to thinking about virtual threats like we do physical threats. This is partially because, as humans, we don't have senses that work in the virtual world. Unlike most physical objects in the real world, what computers do and how they interact is often not directly perceivable.

A networked computer is an amazingly powerful tool, but like any tool, it can be used for good and for ill. We shouldn't shun the tool because we don't understand it, but we also need to learn to use it properly so that we don't endanger ourselves or others. Automobiles can be lethally dangerous, but the benefits of mobility are undeniably worth the risks.

However, though we are carefully trained and licensed before being allowed to drive on the highway, there is no permit required for the surfing on the information superhighway. Furthermore, the dangers of piloting a 3500-pound metal box at 70 miles per hour are readily apparent to the driver. But the dangers of surfing the net are not intuitively obvious. People just don't have an instinctual feel for the risks.

In the physical world, we've developed senses that help keep us safe: we smell smoke, we hear footsteps coming up behind us, we see a rustle in the bushes, we taste that something is going rotten, or we feel that something is radiating heat. We don't have similar senses for the virtual world.

Before computers were connected to the Internet, this lack of senses didn't matter as much. If you had computer problems, they were probably caused by you and affected only you. Today, our computers are connected 24/7. A security lapse by one person can have perilous effects on many others. The advent of the Internet is to computer viruses what the emergence of air travel was to human viruses. Viruses went from a local concern to a global concern. (Unfortunately, we're now all too familiar with a global pandemic.)

That leads to a very important conclusion: your security affects my security too. If your network gets hacked or your computer is infected by a virus, the other devices you interact with are now in danger, as well. But this can also work in our favor. I'll come back to that at the end of this chapter.

So, to answer the original question, I'm not going to lie—you definitely have plenty to worry about. Like the lord in our analogy, your threats are many and varied. (I'll enumerate the main ones in the next section.) But know that most of the threats are avoidable and most of the risks can be significantly mitigated. The main goal of this book is to help you do those things. I like to say that you should be more *wary* than worried.

But I also want you to learn enough about how computers and the Internet work so that you can start to develop your “cyber” instincts and senses. Arthur C. Clarke once said that any sufficiently advanced technology is indistinguishable from magic. This stuff isn't magic. It's knowable and even predictable. With a little education, you can make better decisions and avoid bad outcomes. By understanding some fundamental concepts, you can adapt the suggestions in this book for your particular situation and even extrapolate beyond the specifics of this book when the situation requires it.

What Should I Be Worried About?

Throughout the course of this book, I'll talk about individual threats more specifically. But for now, I'll give you my list of what I consider to be the most *impactful* threats today. There are two key aspects to any given threat: what's the probability of it occurring, and how dire are the consequences if it does happen? I'm going to roll those two things up together here.

Bank card fraud: People worry a lot about their credit card information being stolen online, but in reality, this is probably one of the least scary scenarios. Why? Well, as long as you report the fraudulent charges in a timely manner, you won't be responsible for

them. Sure, you might have to get a new credit card, which is annoying, but you haven't actually lost any money. It shouldn't even affect your credit score. The credit card companies have insurance, and they charge all sorts of fees to cover losses like these. They're also getting really good at spotting suspicious activity—they will probably catch the bad charges before you do. So, while credit card fraud is a real problem for the credit card *companies*, it's really not a major problem for the card *holders*. Debit card fraud, on the other hand, can be extremely impactful. Charges and withdrawals via debit card immediately remove funds from your account.

Spam and scams: The Internet is a con artist's dream come true. You no longer have to find and meet your marks one at a time; you can reach millions of gullible people for almost zero cost (and almost zero risk) via email or text message. I've seen estimates that almost 85 percent of emails are junk or "spam."³ That's a staggering figure. Junk mail filters now catch most of these emails, and most of the rest are rightly ignored and deleted. Text message spam filters aren't very good, at least not yet. But if I can send a million messages for almost no cost and only 1 percent of these messages are read, I've still reached 10,000 people. The math is not in our favor.

The list of scams is long and limited only by the perpetrator's imagination. They will use "social engineering" techniques to capture your interest and play on your emotions: guilt, shame, fear, even generosity. It's a classic tale, just told via a new medium.

Phishing: Unfortunately, this has nothing to do with a rod and a reel and whistling the theme to *The Andy Griffith Show*. Phishing is a technique used by scammers to extract sensitive information from people by pretending to be someone else, usually via email or text message. Basically, they trick you into thinking you're dealing with your bank, PayPal, Apple, eBay, Amazon, or even the government (particularly the Internal Revenue Service, or IRS). Sometimes they entice you with good stuff (winning a prize, giving away free stuff, or a special opportunity). Sometimes they scare you with bad stuff (locking your account, reporting you to some authority, or warning you of an account breach). But in all cases, they try to compel you to give up information such as login credentials or credit card numbers.

Malware: Emails and text messages are often used to lure unsuspecting people to fake and/or malicious websites. These websites can use bugs in your web browser to surreptitiously download malicious software (malware) to your computer. Or they might

³https://talosintelligence.com/reputation_center/email_rep

try to convince you to download and install a phony plugin or software update or even a fake virus scanner. Sometimes the message has infected files or applications directly attached that are laced with malware. Malware can be used to steal information, cause senseless harm to your computer or data, or make your computer a slave in a robot army to wage war on some third party. That sounds like a science-fiction story, but it's very real.

Identity theft: When someone uses your information to impersonate you for the purpose of gaining access to your money or your credit or benefits like healthcare, this is called *identity theft* or identity fraud. This is probably the most serious threat for the average person. If someone can successfully pretend to be you to your bank or credit card company, they can drain your bank accounts, open loans in your name, or run up huge bills on your card. Now you have to convince the bank and the credit agencies that it wasn't really you and that you weren't somehow negligent in allowing it to happen. If you're lucky enough to get your money back and get the debt waived, you may still have a big black mark on your credit history.

Email hacking: While it's obvious why criminals would want to target your bank accounts, it might surprise you how lucrative it can be to hack into someone's email account. When you forget your password, how do you recover it? The most common method today, by far, is via email. If a crook can gain access to your email account, they can use the automated password reset service on your bank's web page to change your password—locking you out and giving them full access all in one fell swoop.

Furthermore, they can use your email to get money from your friends and family. One of the more popular scams is to email everyone in your contact list and tell them you're stranded somewhere—your wallet, passport, and cell phone have been stolen, and you need emergency money wired right away. If you got this email from someone you didn't know, you would surely ignore it. But if you got it directly from your son, your best friend, or your mother—maybe even a reply to an earlier email from them—you could very well be duped into believing it was real.

Tracking and surveillance: We freely give away all sorts of information in return for “free” services. And we collectively shrug when whistleblowers reveal astonishing levels of surveillance on the entire population by our governments. Our online activities are being tracked at unbelievable levels today. Personal information is gold to advertisers, and they have built massive profiles on each one of us. This data is used to target you with ads but is also sold to whoever is willing to pay (including the government). This has profound risks, which I will talk about in the next chapter.

Indirect Threats

So far, we've only discussed direct threats—bad guys targeting individuals (even if they sometimes do it on a massive scale, as with spam). While some crooks prefer to mug a series of people in dark alleys, more ambitious thieves might prefer to just rob one bank vault and be done with it. It's the classic risk vs. reward trade-off. While we've had centuries to figure out how to properly protect physical assets like jewels, gold, and cash, we're still trying to figure out how best to protect our digital assets.

That “we” doesn't just refer to you and me—it also refers to large corporations. It seems like nary a month goes by now without hearing about another massive security breach at a brand-name company—the theft of financial details of 100 million Capital One users, the colossal breach at Equifax that divulged gobs of personal and financial data, and the realization that Facebook “overshared” the data of tens of millions of users with Cambridge Analytica. While those were high-profile breaches that made the headlines, there were many others that didn't make the nightly news, either because they were smaller and escaped notice by the mainstream press or because the companies just kept the breaches quiet.

As regular consumers, we can't do anything to improve the security of these corporate servers. However, there's a lot we can do to mitigate the impacts of these now-inevitable breaches. For example, bad guys know that people reuse the same password on multiple sites. If they can get your password for *somesite.com*, they will immediately try that same password on several other popular websites. This is called *credential stuffing*, and the bad guys have this process completely automated today. So just by using unique passwords for each website, we have prevented credential stuffing attacks.

A Few Final Thoughts Before We Begin

I have a few more points and provisos that I want to put out there, and then we can go through some logistical and housekeeping stuff.

First of all, **DON'T PANIC!** (Bonus pop culture points to anyone who immediately verified the location of their towel.⁴) Out of necessity, this book is going to be focused on all the things that *could* go wrong. It's like your sex ed class in high school: they spent a lot of time warning you about all the bad things that could happen—the good parts were

⁴See *The Hitchhiker's Guide to the Galaxy*: <https://hitchhikers.fandom.com/wiki/Towel>

taken for granted. Armed with the knowledge and simple precautions outlined in this book, you will be a card-carrying member of Camp Goldilocks! The good news, when it comes to cybersecurity, is that there are many simple and affordable things you can do to significantly reduce your risks. And that's the whole point of this book.

Second, taking steps to protect yourself will also increase the security of those around you, even if they don't read this book. If your computer or online accounts are compromised, they can be used to compromise others—particularly those with whom you are connected directly. When you leave yourself vulnerable, you're not just risking your own safety—you're risking the safety of others, as well. Conversely, protecting yourself will also help protect your friends and family. And if enough people take these basic precautions, we can even develop a sort of herd immunity in the cyber world.

I do need to throw in a few caveats too.

First, I promised that this book would make you safer—and if you do even some of the things I recommend, it will absolutely do that. But note that I did not say that it would make you *safe*. The topic of security is unbelievably vast, and the playing field is changing constantly. One book couldn't possibly cover every possible threat, and that wasn't my intent. There are so many small and simple things that everyone can do to mitigate most risks, and most people just don't know about them (or don't understand how important they are). Those are the things I want to cover in this book. Also, security is never absolute. Look at the National Security Agency (NSA). You'd think they'd be secure (it's right there in the name!), but they were still beaten by one guy (Edward Snowden). It's not about being 100 percent secure. That's impossible. It's about being secure *enough*. As the saying goes, you don't need to outrun the bear; you just need to outrun the other guy. However, when it comes to computer security, most people have honestly done little or nothing to protect themselves. With this book, I will give you many simple, reasonable steps you can use to protect yourself. I'll even tell you some of the more arcane things you can do if you really want to kick it up a notch.

Second, convenience is generally the enemy of security. That is, the more convenient something is, the less secure it probably is. Therefore, increasing your personal security is going to decrease your personal convenience and probably make your life more complicated than it is now. That's the hard truth of the matter. We're used to the inconveniences of real-world security. Having to lock your house and your car all the time is inconvenient, but these simple precautions are a fact of modern life, and most of us don't give them a second thought. Having to show an ID to cash a check and having

to enter a PIN to withdraw money from an ATM are things we're just used to doing. However, computer security is another story entirely. Most people are *not* used to doing the things that they really should be doing, and therefore some of the things that I'll recommend in this book are going to seem really inconvenient at first. Give them a try—you might be surprised how quickly you get used to doing them.

And finally, I know a lot about security and privacy, but I'm not infallible, nor am I free from bias. I have many colleagues in this arena, and it's not uncommon for us to disagree amongst ourselves on specific solutions to specific situations. It's just the nature of the beast. So I encourage you to seek information from other sources, and I will point you to several good ones throughout this book.

Okay, now that that's out of the way, let's help you get the most out of this book!

How to Use This Book

My primary goal is to make you safer. The most efficient way to do this is to just tell you what to do. While I strongly believe that you need to understand *why* you're doing these things, when all is said and done, that's secondary to actually doing them. It's like eating right and exercising. Sure, it's good to know why it will help you, but you can get all the benefits just by doing it, whether you understand it or not. If you're like me, though, I can't get properly motivated to do something unless I know why it's important and what the benefits will be. But I get it—not everyone is like me.

Each chapter has two parts: the part that tells you what to do and the part that explains why it's important. The “what” part is in the form of a checklist, which you will find at the end of each chapter. The “why” part precedes the checklist, and I strongly encourage you to read it. But if you truly don't care about the “why” and you're willing to just trust me, then by all means just skip straight to the checklists. You can always come back later and read the “why” parts.

You do NOT have to do everything in this book! Not all these tips will make sense for everyone. That's why I went out of my way to explain the “why” first so that you can make an informed decision about which suggestions might do you the most good and which ones don't really apply to your situation. You bought this book (or perhaps some highly intelligent, thoughtful person bought it for you) with the goal of being safer. If you do even some of the things in this book (particularly the ones I've marked with a star), you will absolutely achieve that goal. And don't feel like you need to race through this book

and implement everything today. It's more important to take your time, understand what I'm telling you, and then start ticking things off the checklists.

I've tried to make this book as simple as possible to use, and that required that I make some key decisions to reduce the number of choices. I've tried to make it clear in each place where I've made such choices, giving you pointers on how you can make different ones. But for the sake of simplicity and brevity, I had to just make the call in some cases.

Finally, the sequence of the chapters is important, and you should tackle them in the order presented, even if you intend to skip the explanation parts and jump straight to the checklists.

Reader Prerequisites

To keep this book a reasonable length, I've had to make some assumptions about the capabilities of the reader. For example, I assume that you know how to restart a computer, how to search the Internet using a web browser, and how to download and install software. *If you do not meet these requirements, please do not let this stop you from reading this book!* If you are truly a novice user, you probably need the advice in this book more than most. I urge you to either enlist the help of a friend or family member, consider taking a local computer class, or find a good entry-level computer book for your operating system to help you learn your way around your computer.

Operating Systems Covered

For owners of PCs running the Microsoft Windows operating system (OS), this book will cover both versions 10 and 11. Note that the Windows OS comes in different flavors: Home, Enterprise, and Pro. This book will focus on Windows Home, which is the entry-level version of Windows that comes with most PCs. However, the advice in this book will usually apply to the other flavors, as well.

For Apple Macintosh computer owners, this book will cover versions "Monterey" and Ventura" of macOS.⁵ Apple annoyingly uses both names *and* numbers for their OS versions, but usually refers to them by name, so I will follow suit. I'll use "Ventura" to refer to macOS version 13 and "Monterey" to refer to macOS version 12. If your Mac is not running the latest version of macOS, I strongly encourage you to upgrade to the

⁵ Yes, that's really how they capitalize it.

latest version that your computer will support. Apple continues to add new security and privacy features in their OS updates, and the updates are free. There's just no good reason not to upgrade to the latest version that your system supports.

For mobile operating systems, this book focuses on the iOS version 16 for Apple products and Android version 13 for phones running Google's operating systems (e.g., Pixel, Samsung, Xiaomi, Oppo). Note that the look and feel of Android versions can vary wildly between major release versions and even between different cell phone manufacturers and cellular providers. This has important implications for security, which I will discuss later in Chapter [12](#).

Don't worry if you're not sure what operating system you have—I will help you figure this out at the end of this very chapter!

Navigating the Checklists

The most important parts of this book are the checklists at the end of each chapter. I've tried to make them as easy to follow as possible. Each checklist item will have a number and a title, followed by instructions for how to complete the checklist item. In some cases, this will just be a short paragraph; in others, there will be a series of steps that you will need to complete in order. Wherever it was helpful, I included images that show what you should see on your computer screen.

In some cases, the steps you need to take will depend on your particular situation, such as what operating system you have. In those cases, there are subsections under each tip for each possible situation—you just need to find the one that applies to you, and you can ignore the other sections.

Here are some examples.

Tip 1-1. Simple Tip

For simple tips, there may only be a short paragraph describing what you need to do (or, in some cases, not do). Many tips will have a list of numbered steps that you should do in order. I also tried to put the tips themselves in the order that makes the most sense—so try to do them in the order given. Of course, you can always skip any tip if it doesn't apply to you—or frankly if you just don't feel like doing it. Remember, you don't have to do everything in this book!

Tip 1-2. ★ Tip with Stars

Tips marked with a star are the most important tips in the book—the ones that I feel have the most impact on your security and privacy. Try to do all of these tips, if you can.

Tip 1-3. Tip with Variations

A tip that has variations depending on your setup (like your computer operating system or mobile device type) will have subsections for each variation. You just need to find the subsection that applies to your situation and ignore the other subsections. In the following examples, there are variations depending on your operating system type. The subsections will all have the same base number, with a different letter suffix (a, b, c, etc.).

Tip 1-3a. Windows

If a tip subsection title just says “Windows,” without a Windows version number, then you can assume that it applies to both Windows versions 10 *and* 11. I will do this whenever possible, to keep things as simple as I can.

Tip 1-3b. Windows 10

If a tip subsection title calls out a specific version of Windows (like “Windows 10” here), then follow the instructions for your specific version of Windows and skip the other Windows subsection.

Tip 1-3c. macOS

Similarly, if a subsection is generically labeled “macOS,” then you can assume that it applies to both macOS Ventura and Monterey.

Tip 1-3d. macOS Monterey

If a tip subsection title calls out a specific version of macOS (like “Monterey” in this example), then follow the instructions for your specific version of macOS and skip the other macOS subsection.

Objects in the Book May Seem Larger Than They Appear

Some computer dialog screens aren't laid out well for screenshots in books. So, in some cases, I've taken the liberty to crop the images to focus on the important parts. For example, I might cut out blank parts in the middle to eliminate a lot of wasted space. If you see an image that looks a little odd, it may be due to some creative cropping on my part.

Let's look at an example, so you know what I mean. Figure 1-1 is the actual image I captured from my computer. You can see there's a lot of extra space in the middle there. To get all of that into the width of a page, it makes the image text smaller and harder to read.



Figure 1-1. Actual screenshot (unaltered)

To make better use of space and make the text easier to read in this book, I can edit this image to show the important parts and remove the wasted space. See the edited image in Figure 1-2.

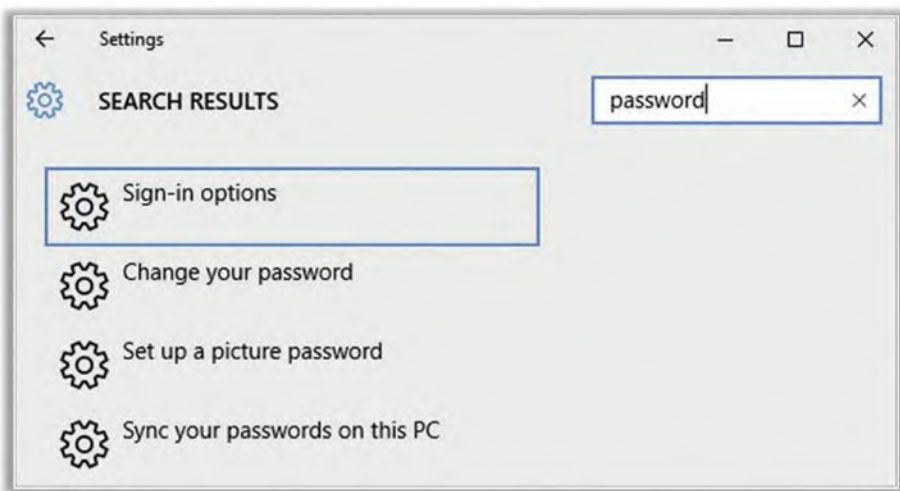


Figure 1-2. Screenshot edited to eliminate extraneous space for better readability

Figure 1-2 still has all the important information, but it's more compact and therefore much easier to read. However, on your computer, you will see something more like the first image. So I just wanted to let you know that sometimes I make changes like this for the book, and hence some of the images here might look a little different compared with what you see on your computer.

Also note that some information has been “redacted” in several images. You'll see black boxes around any text that would have given away personal information.

Always Go to the Source

For many of the tips in this book, you'll need to download something from the Internet. In most cases, I give you the link you need to do this. But in general, be sure to **always** go to the source whenever you download any piece of software. There are several popular software download sites that aggregate, rate, and review software. Feel free to *consult* them, but when it comes time to actually download the software, *don't download anything from these sites*. Instead, go to the official website for the software maker. These aggregator sites are a favorite target for bad guys and overzealous marketers who will taint the software with viruses or bundle additional software in the installer that you definitely do not want. (This is actually one of the tips later in the book, but it's important to call out now, before you start downloading anything.)

Updates and Bonus Content

All of the information in this book and the steps in the checklists were as accurate as possible when I wrote them. However, the wild and woolly world of the Internet is constantly changing.

Also, this book is full of web addresses. If you happen to be reading the electronic version of this book, you can just click these links. If you have the paper version, this is obviously not an option. And web links have a nasty habit of changing too.

To stay as current as possible and to make it easier for you to access the web links, I've created a special companion page for this book on my website:

<https://firewallsdontstopdragons.com/book-updates>

On this page, you will find

- *Web links*: A full list of every web link, in order by chapter. As links inevitably change, I will endeavor to update this web page with the new addresses.
- *Errata*: If I find mistakes in the book, I will correct them here.
- *Updates*: If my recommendations change or if the steps to some instructions need to be updated, I will record them here.
- *Bonus content*: I'm hoping to add some useful, free bonus content on this site, possibly including a downloadable workbook.

Please check out that link before reading too far in case there are important changes or updates. I would definitely bookmark the web address for future reference. Like software, this book will have “bugs” and need updates from time to time. I'll try to capture all of that on the preceding web page.

Other Resources

I have a few other ways for you to stay up to date on privacy and security. I have a newsletter and a blog, which usually cover the same topics. They're published every two weeks. If you like having these things delivered to you on a regular basis, I suggest signing up for the newsletter; if you would rather read these at your own pace or perhaps catch up on past articles, check out my blog. Both can be found on my preceding website.

I also have a weekly podcast, if that's more your speed. (And if you've never tried a podcast, this would be a great one to try first.) In addition to timely news topics, I interview top experts in the fields of cybersecurity and privacy about current events, how they impact us, and what we can do to be safer. See the “Podcast” tab on my website for details.

For more up-to-the-minute security and privacy news, you can follow me on social media. I post video versions of my podcast on social media, as well (Facebook and YouTube), if you prefer that format. See the “Contact” tab on my website for all my social media information.

Finally, you shouldn't just take my word for it when it comes to privacy and security. In the spirit of this, I've added “Going Further” sections to many of the chapters, pointing you to other top-notch resources. You can find several others on the “Resources” tab of my website, as well.

Feedback Welcome

If you find an error in this book or if you have ideas for ways I can improve the next edition, please send me an email. My goal is to make this book the best it can be:

`feedback@firewallsdontstopdragons.com`

As I find errors and updates, I will note them on my book update page (see earlier).
Please check this list before submitting feedback.

I will head one thing off at the pass right now, though: grammar. I know I broke some rules in this book. I specifically tried to make this book very conversational and accessible. That means sometimes using “who” when it should be “whom,” using “they” as a singular pronoun, and ending sentences with prepositions from time to time. If you are an English teacher, a formal writer, or just someone who is a stickler for grammar, I will just beg your forgiveness now and ask you to chalk it up to artistic license.

Summary

We covered a lot of ground in this first chapter! Let's recap the highlights:

- The first step in any cybersecurity undertaking is understanding the threat model. That is, before we can take steps to protect ourselves, we need to figure out exactly what it is we're trying to protect and who or what we're trying to protect it from. This will help us decide where to focus our efforts and what types of defenses we're going to need.
- For 99 percent of the population, the threats to your computer security are generic and indiscriminate. That is, you are not likely to be specifically targeted by bad guys—and certainly not by nation states or organized crime groups. In our castle analogy, that means you're worried about random crime and misfortune, not a dragon that's scouring the kingdom looking for *you*.
- Nothing is 100 percent secure. Your goal is to be secure *enough*. You don't have to implement all the recommendations in this book, and you don't have to do them right now. But every tip you check off will make you incrementally safer, and you should strive to do as many as you can. I've provided you with the information you need to understand why you need to do these things and which of these things are most important for your situation.
- The recommendations in this book are designed to give you the most protection with the least amount of effort and cost, but there will be trade-offs when it comes to convenience. We've become accustomed to minor inconveniences to improve our security in the physical world. We don't think twice about them. You will also get used to inconveniences that will make you safer in the virtual world.
- Your security overlaps mine. Our devices are networked and connected 24/7. If your computer is infected with a virus, then my computer will be at risk of catching it too.

- The advice in this book has been painstakingly compiled from years of research, reflecting the best practices espoused by top security and privacy experts. But at the end of the day, I'm human—and therefore my advice is still going to be colored by my personal biases and blind spots. You should always seek out other opinions. I'll point you to many excellent sources throughout the book.

In the next chapter, I'll dig into the thorny topic of privacy—how it relates to security and why it's more important than you probably think it is.

Going Further

- *Consumer Reports Security Planner*: This is a handy little tool that will help you figure out your threat model and give you a customized list of things to do. Note that many of them will probably be covered by this book already:

<https://securityplanner.consumerreports.org/>

- *Security self-defense guide*: The Electronic Frontier Foundation has some great tutorials on security and privacy:

<https://ssd.eff.org/>

- *You are not Batman*: Ars Technica has a great article about understanding your threat model:

<https://arstechnica.com/information-technology/2017/07/how-i-learned-to-stop-worrying-mostly-and-love-my-threat-model/>

Checklist

As promised, here is your very first checklist! Every chapter of this book will have one. If you really just want to take my word on everything, you can skip all the stuff at the beginning of each chapter and just work through these tips. (You might at least read the chapter summary, though.)

These first tips will lay the groundwork for many others. We need to take a moment to note some key information that you will need to have handy.

Tip 1-1. Take Good Notes

This isn't required, but there's a *lot* of stuff in this book, and I would strongly suggest that you find some way to take some notes as you go. You can keep handwritten notes in a paper journal, or you can type up your notes in a digital file using Word, Pages, Google Docs, or something similar. Regardless of which way you go, here are some suggestions to consider:

- Break your notes down by chapter. Write down the chapter name and number at the top of each section.
- Write out the number and title of each tip in the chapter, with a big checkbox in front of it. Come up with some system for denoting whether you completed or skipped a given tip—like maybe a check mark ☒ for completion and an ☐ for skipping.
- As you work on each tip, keep notes on anything you learned, including anything you struggled with or need to come back to later. If you skipped the tip, write down why—it may be obvious now, but you might forget later.
- If you're using a paper journal, be sure to leave space between tips and chapters, in case you want to return later to add more notes.
- If you're editing a digital file, you can take screenshots and save them in your notes. This can be particularly helpful if you run into any problems. (If you don't know how to take screenshots, it's pretty easy these days—just do a web search on “how to take a screenshot on windows/macOS” using your particular operating system.)

- **Note:** If you're using a digital file, even if you aren't saving it to "the cloud" (we'll discuss this later), do NOT put any passwords in the file. If you're taking paper notes, it's fine to write down passwords as long as you don't leave it laying around where untrusted people might find it.

Tip 1-2. Determine Your Computer Type and Version

Many of the tips in this book will be broken down into subsections depending on what type of computer you have and what version of the operating system (OS) it's currently running.

If your computer is made by Apple, then you have a Macintosh ("Mac") of some variety: iMac, MacBook, Mac mini, etc. If your computer is made by HP, Dell, Lenovo, Asus, Acer, or basically any company other than Apple, then you probably have a Windows PC. (If you have a computer that runs Linux, this book doesn't cover that operating system. However, many of the tips in this book don't depend on your operating system.)

Now we need to determine which version of Windows or macOS your computer is currently running. See the following subsections for help figuring this out.

Note The techniques used here will be very helpful for other tips in this book. Specifically, it can be really hard to find settings on computers these days. It's almost always easiest to just search for them by name instead of trying to navigate through the various settings and system preferences to find them. I'll revisit these techniques in more detail in the checklist for Chapter 6 (computers) and in the checklist for Chapter 12 (mobile devices).

Tip 1-2a. Windows

If you have a PC, we need to figure out what version of Windows you're running. To find this out, we need to look at the system information. To search your Windows settings, open the search tool from the bottom of the screen. See the following figures to see what this looks like for Windows 10 (Figure 1-3) and Windows 11 (Figure 1-4).

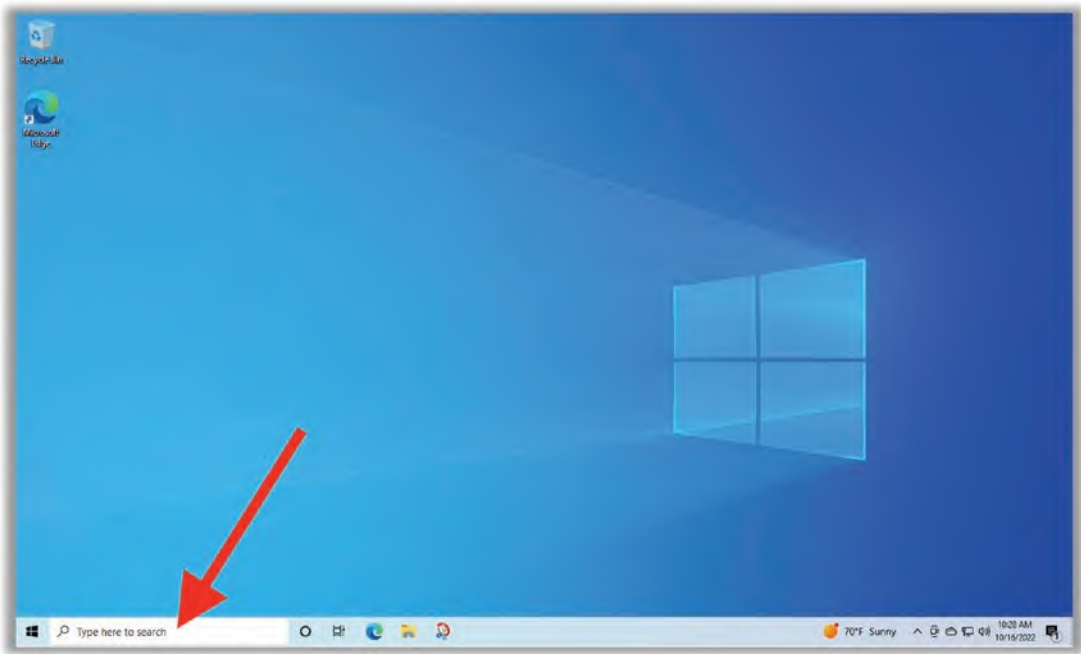


Figure 1-3. Windows 10 search tool

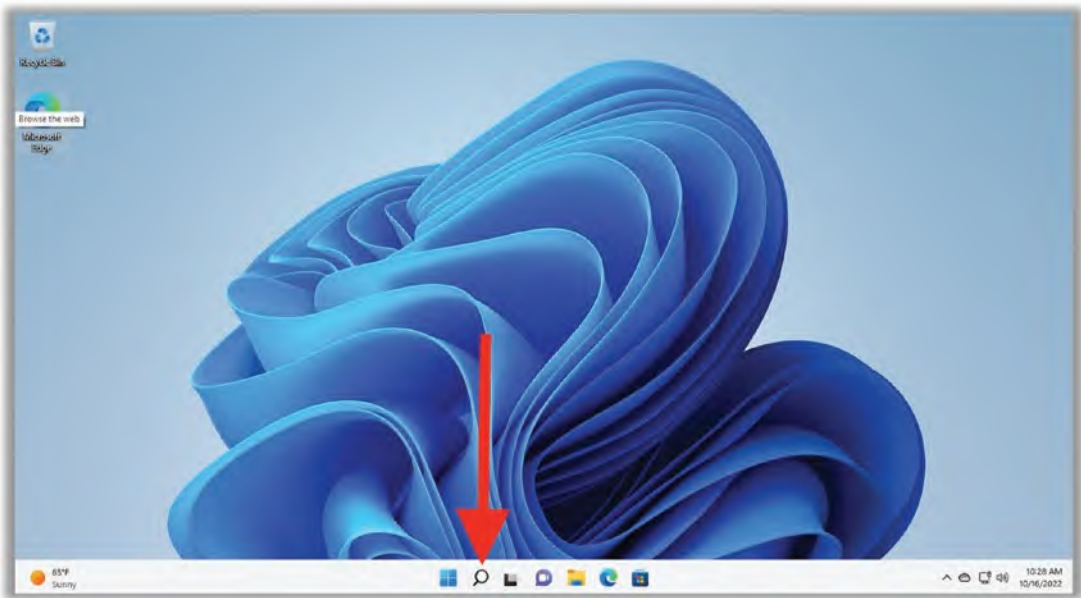


Figure 1-4. Windows 11 search tool

1. In Windows 10, you can just type your search text right in the text box. For Windows 11, you'll need to click the magnifying glass icon to open the search tool.
2. In either case, search for "about your PC." (Note that you will often see the search result you want before completely typing the entire text that I suggest. For example, you'll probably see "About your PC" as soon as you type the word "about." You can stop as soon as you see what you want.)
3. Click "About your PC" and scroll down to the "Windows specifications" section. There you will find the operating system version ("edition"). See Figure 1-5 for examples.

Windows specifications	
Edition	Windows 10 Home
Version	21H2
Installed on	8/24/2022
OS build	19044.2006

Windows specifications	
Edition	Windows 11 Home
Version	21H2
Installed on	8/24/2022
OS build	22000.1042

Figure 1-5. Windows specifications. Windows 10 (left) and Windows 11 (right)

Tip 1-2b. macOS

On an Apple computer, we need to figure out what version of macOS you're running. To find this out, we need to look at the system information. To do this, go to the Apple menu in the upper left of your screen. See Figure 1-6 to find it.

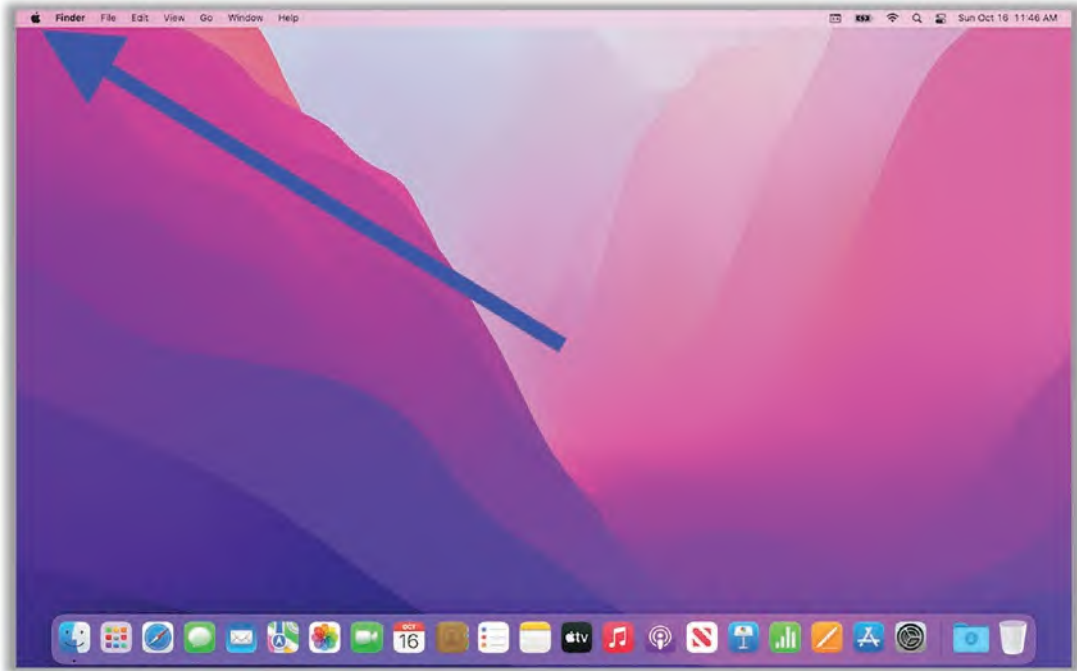


Figure 1-6. Apple menu location

From the Apple menu, select “About This Mac.” You should see something like Figure 1-7 in macOS Ventura and Figure 1-8 in macOS Monterey (and before). In Ventura, the macOS version is right above the “More info” button; in Monterey, the version name and number are at the top of the “Overview” section (click that tab if you don’t see it).



Figure 1-7. macOS Ventura About This Mac



Figure 1-8. macOS Monterey About This Mac

Tip 1-3. Determine Your Mobile Device Type and Version

Chapter 12 will focus on your smartphone and other smart mobile devices, like iPad and Surface tablets. As with our computers, it's important to know which version of the operating system they're running.

Tip 1-3a. Apple iOS

For any mobile Apple device (iPhone or iPad), you can determine the OS version as follows:

1. Go to Settings (the big gear icon).
2. Scroll down and click "General."
3. Click "About" at the top.
4. Look for "iOS Version." You only care about the first part (like "16.0.2")—the part in parentheses you can just ignore.

However, like with computers, there are so many settings on mobile devices that it's often just simpler to search for what you want. Try this method:

1. Go to Settings (the big gear icon).
2. At the very top is a search bar. If you don't see it, try scrolling up.
3. Type in "About" in the search bar. You should see an item in Settings called "General ► About." Click that to jump right to that setting.

Tip 1-3b. Android

There are many different Android devices. Each manufacturer and service provider can alter the look and feel. Because of this, in most cases I will simply describe what you need to do to find the right setting, as I do here:

1. Open your device's Settings app.
2. Near the bottom, click "About phone" or "About device" and then "Android version."
3. There you will find the "Android version" or "Software Information." You can ignore the "security update" and "build number."

However, like with computers, there are so many settings on mobile devices that it's often just simpler to search for what you want. Try this method:

1. Open your device's Settings app.
2. Click the search icon (looks like a magnifying glass).
3. Search for "software information" and tap the result.

CHAPTER 2

Privacy Matters

You can't talk about security without also talking about privacy. The two are inextricably linked. At a basic level, security enables privacy—for example, strong encryption helps us keep our data private. But privacy is fundamentally separate from security and is important in its own right. And unlike with security, we are often at odds with companies and government agencies when it comes to privacy. For this reason and others, I feel that privacy is the most important topic of this book. In this chapter, I'll explain why.

Privacy vs. Security

Let's start by dispelling a particularly insidious myth: to get more security, you need to give up some privacy. This is the subject of a poignant political cartoon that I often use in my class slides and speaking presentations, which you can see in Figure 2-1.

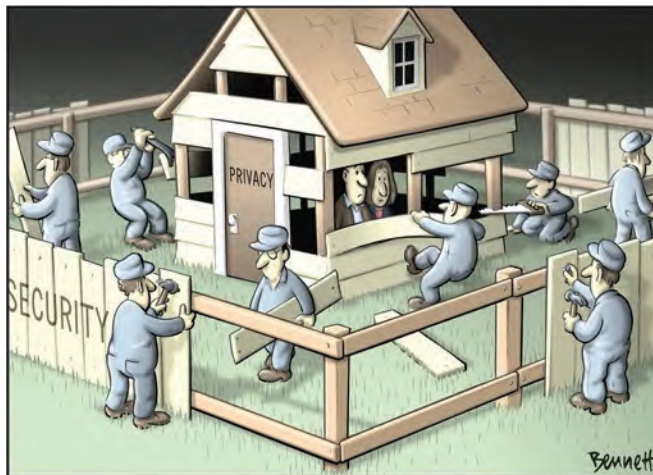


Figure 2-1. Credit: Clay Bennett, *The Christian Science Monitor*¹

¹ Clay Bennett, *The Christian Science Monitor*: [https://www.csmonitor.com/Photo-Galleries/CSM-Galleries/Clay-Bennett-Pulitzer-Prize-Cartoons/\(photo\)/231700](https://www.csmonitor.com/Photo-Galleries/CSM-Galleries/Clay-Bennett-Pulitzer-Prize-Cartoons/(photo)/231700) – see slide 7

There are those in law enforcement and intelligence agencies who will claim that in order to fully protect you, they need access to all of your private communications. Conversely, they claim that strong encryption is keeping them from stopping bad guys. James Comey, when he was the director of the Federal Bureau of Investigation (FBI), famously referred to this phenomenon as “going dark,” implying that they are losing the ability to surveil us (for our own good, of course). In reality, we are in the golden age of mass surveillance. There has never been a time in human history where law enforcement agencies have had so much information at their fingertips. This will be obvious by the time you finish reading this chapter—even more so by the time you finish the book.

However, when I say “privacy vs. security,” I’m not just referring to this false choice of giving up one to get the other. I’m saying that security and privacy are not the same thing, and security failures have different consequences than privacy failures.

Security threats have been around since humans have had possessions worth stealing. As long as you have something that someone else might want, you need to be thinking about how to prevent that thing from being taken for greed or maybe just destroyed for spite.

We’ve had privacy threats for a long time too. Examples are nosy neighbors and peeping Toms, who snoop for their own personal reasons. In more modern times, we have tabloid-style journalists who sell sordid stories and compromising photos of politicians and celebrities for profit.

Until very recently in human history, all of these threats required physical proximity. To steal something, you had to go get it. Spying on people meant following them around for days or even weeks at a time—snapping pictures with telephoto lenses, planting listening devices (“bugs”), rummaging through their garbage, and so on. This was a self-limiting activity due to logistics and available manpower.

That all changed shortly after the turn of the century with the advent of smartphones and broadband Internet. Not only have we managed to digitize all our most personal data, but we have also put that information on computerized devices that are connected to a global communication network every hour of every day. In fact, much of our data is actually now stored in “the cloud” and not even on devices in our possession or under our direct control. What could possibly go wrong?

But here’s a crucial difference between security and privacy: if someone steals your stuff, you can (at least theoretically) replace it; if someone steals *you*—your history, your

preferences, your relationships, your communications, your biometrics, your location history—you can't get that back. That knowledge can't be unlearned. Memories can't be erased. Put more simply: **security failures can be fixed; privacy failures cannot.**

Here's another important difference between security and privacy: corporations and governments are generally on your side when it comes to security—it hurts you both if something you entrusted to them is stolen or compromised. The same cannot be said for privacy. While corporations and governments will ardently proclaim their commitment to keeping your data private, what they usually mean is “private from everyone but us.” That is, they say that they will protect your data from the “bad guys,” but they don't include themselves in that category. The truth is that your data is supremely valuable to them for other reasons, which have little or no value for you. This creates an inherent conflict of interest. Furthermore, companies and governments are filled with human beings—fallible and sometimes malicious human beings.

Because of these conflicts of interest and the significant consequences of data breaches, privacy is a prime differentiating factor when it comes to evaluating products and services. It will have a significant influence on many of the suggestions in this book.

Therefore, I need to spend some time up front explaining why privacy is so fundamentally important. Even if you are a private person or feel that you value privacy in general, I'm guessing that there are still aspects to this topic that you haven't fully considered. So let's take a trip down the rabbit hole! (Fair warning: I'm about to climb up on a soapbox here and get a little philosophical. But please just indulge me here for a minute.)

Why Privacy Matters for You

Let's start by understanding what we mean by privacy. If I asked you to write a definition for that word, in the context of a person's privacy, what would you say? I've seen several definitions, but to me the most basic definition is that privacy is about having control over what information you share. A colorful way to say that is that privacy is about telling your story the way you wish it to be told.

Okay, so what does *that* mean? First, it means deciding what information about yourself that you wish to share, when you want to share it, and with whom. You may share different things at different times with different people. And that's your right. It's everyone's right. And because it's a right, it's not something you have to defend or justify.

It just is. For me, the right to privacy is just as much of a human right as is the right to liberty or freedom.²

However, in the context of computers and the Internet, we've developed a strange view of privacy. We think about privacy in terms of "data"—which makes it seem less personal. Privacy policies often talk about *personally identifiable information*, or PII. Again...it sounds so anodyne and innocuous. And yet, Google and Facebook—two of the most valuable tech companies on the planet³—derive the vast majority of their wealth from your data. Our personal information is worth hundreds of billions of dollars for them. We trade our personal data for "free" services all the time. As we will see later in Chapter 8, we are tracked mercilessly when we surf the Web. The amount of information gathered about us based on our online activity—what we search for, the sites we visit, the things we buy—is truly staggering. I've seen this expressed most succinctly as follows:

If the product is free, then you are the product.

Why do we allow this? I think some people believe that their data just isn't that interesting: boring text messages containing grocery lists, mundane emails about soccer games, inane social media posts with cat videos. "Who cares? I have nothing to hide."

Okay. But if I can learn enough about you, then I can use that information against you. For example, if I can convince your bank or credit card company that I am really you, I can steal your money or stick you with a massive bill—and maybe even ruin your credit. If I see that you're going on vacation by watching your social media posts, I can probably figure out where you live and take your stuff while you're away. If you want to get super creepy, I can also use pictures you post to find and stalk you or (worse yet) your kids.

But this information can also be used against us, for example, to influence us. While our data is ostensibly gathered to target us with "relevant" ads, it also creates a stunningly accurate profile of us, including gender, income range, political leanings, religious affiliation, medical conditions, sexual orientation, and even mental health issues. Because social media sites like TikTok, YouTube, and Facebook make money by showing you ads, they are laser focused on keeping you on their site or app for as long as humanly possible. They are expertly optimized to keep you "engaged." It's honestly not even a fair fight.

² Many people in the United States believe that the right to privacy is enshrined in the Constitution. It's not. The word "privacy" doesn't appear anywhere in that text, including the 27 Amendments. Is it implied? Legal scholars believe so, yes. But it's not explicitly codified.

³ As of July 2022, Alphabet (Google) is #3 and Meta (Facebook) is #6. <https://www.bankrate.com/investing/most-valuable-tech-companies/>

It's one thing to be coaxed into buying stuff. But this same information can also be used to manipulate much more consequential behavior. For example, these profiles are used to show you highly targeted political ads—not just on your phone, but in your mailbox. This can be used (and has been used) to influence the outcome of elections⁴—either by driving you toward one candidate, driving you away from another candidate, or even just convincing you not to vote at all.

This leads to an even bigger point: privacy isn't just personal.

Why Privacy Matters for All of Us

I've always been a fairly private person. It's not that I have stuff I want to actively hide, but I share different parts of my life with different people. How I act and what I discuss differs when I'm at work with my colleagues, at home with my kids, at a party with my friends, or at holiday gatherings with my extended family. I think everyone is like that to some degree. That's just being human.

But when Edward Snowden revealed the US National Security Agency's sprawling mass surveillance apparatus in the summer of 2013, it was a real awakening for me. It's one thing to vaguely believe that intelligence agencies like the NSA have the *capability* to spy on me personally. It's quite another to know that they're actively spying on all of us, all the time, without a warrant or even probable cause. It was this event that prompted me to write a book on security.

But it would still be several years (and at least two updates to this book) before I came to understand that privacy isn't just a “me” thing—it's also a “we” thing. In the summer of 2015, in a Reddit AMA (“ask me anything”), Snowden said the following⁵:

Arguing that you don't care about privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.

This implies at least two things. First, privacy is a right. You can choose not to exercise it yourself, but that does not (and cannot) preclude *my* right to exercise it. Second, privacy is bigger than just you. Privacy is a quality or aspect of a society in general—it's something we share and that affects us all.

⁴If you're skeptical (and you should always be skeptical), please watch the documentary called *The Great Hack* on Netflix. See the “Going Further” section at the end of the chapter.

⁵<https://www.motherjones.com/politics/2015/05/edward-snowden-reddit-nsa-ama/>

Before we get super deep, let's just look at this statement from a practical standpoint. When you give away your data, you're also giving away other people's data. Your privacy overlaps mine.

For example, when you post pictures on social media, they often include other people (not just you). Facial recognition technology can identify those people—and in fact, Facebook did just that. After much pushback, they stopped doing this without consent.⁶ But we also do it for them whenever we “tag” our friends and family in our photos and videos. Pictures taken on smartphones contain metadata that include the time and place a picture was taken (we will discuss this more in Chapter 10), which might show where your friends live or where their kids like to play.

Also, your friends list on Facebook and your address book on Google contain dozens if not hundreds of other people. The contact info may include email addresses, physical addresses, phone numbers, and birthdays. The friends lists and address books of those people almost certainly overlap, as well. Those connections create a “social graph,” which can divulge information not just about you but about them too. People with overlapping contact lists probably go to the same church, work for the same company, belong to the same political groups, belong to the same family, or have kids at the same school. Just like poor computer security on your part can put me at risk, poor privacy on your part can undermine mine.

But it's even bigger than that, which brings me to my final point on privacy.

Enter the Panopticon

Privacy isn't about having something to hide—it's about having something you simply don't wish to share with others.⁷ How often have you seen bumper stickers or T-shirts that say, “Dance like no one is watching”? And why do we only sing in the shower or when we're alone in the car? You might be tempted to say that you're just embarrassed to do those things in public. But what it really tells us is that we act differently when we know we're being watched.

⁶<https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/>

⁷This is a paraphrasing of a line from the movie *Anon*: “It is not that I have something to hide... I've got nothing I want you to see.” Again, see the “Going Further” section for more info.

In the eighteenth century, an English philosopher named Jeremy Bentham came up with a clever cylindrical prison concept that compelled behavioral conformance through implied mass surveillance. He called it a *panopticon*. The inmates lived in cells on the outer rim, and the cell openings faced the interior. A very small number of guards could be stationed in a watchtower at the center where they could see into all of the cells (see Figure 2-2). The genius of this design was that it was set up so that the people being watched (the inmates) couldn't see the people doing the watching (the guards). Therefore, the prisoners could never know for sure when they were being monitored. Even though a handful of watchmen couldn't possibly observe all the inmates simultaneously, each inmate had to *assume* that they were being watched at any given moment. This effectively forced all inmates into constant compliance.

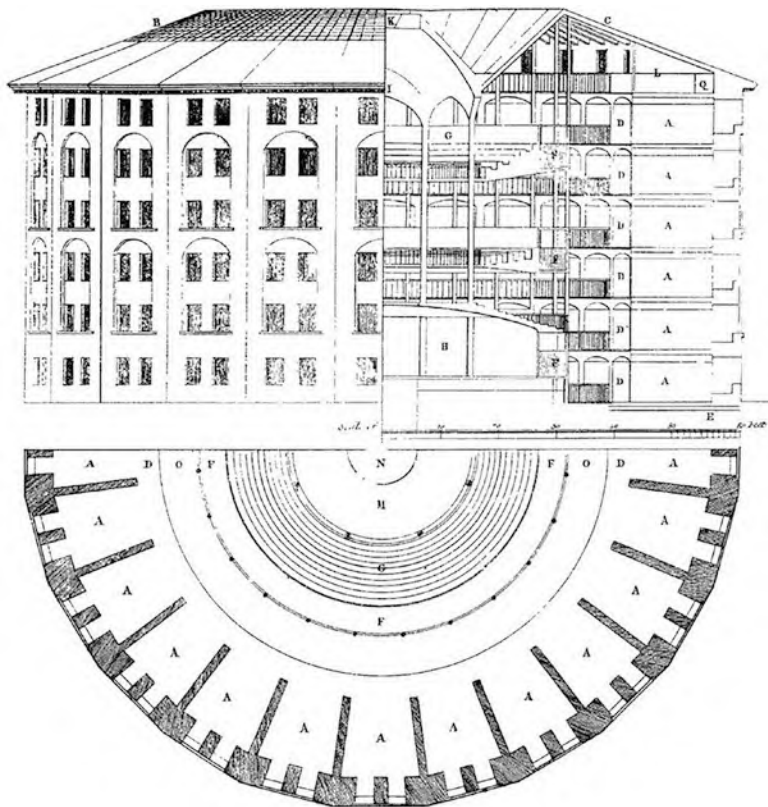


Figure 2-2. *Panopticon prison plan drawing*⁸

⁸ Plan of the Panopticon, 1843 (originally 1791), from the works of Jeremy Bentham vol. IV, 172–3. (Wikimedia commons): <https://commons.wikimedia.org/wiki/File:Panopticon.jpg>

Similarly, citizens will act differently when they feel their government is watching them. The classic depiction of this premise, of course, is the book *1984* by George Orwell. But even Orwell didn't contemplate that "telescreens" would be small enough to fit in your purse or pocket or that every citizen would happily and religiously carry these surveillance devices around 24/7, even when they went to the bathroom.

Mass surveillance undermines our collective privacy, whether it's done by corporations trying to sell us stuff or by law enforcement agencies trying to stop terrorists and child molesters.⁹ And it's crucial to understand that the former enable the latter. In most democratic countries, law enforcement agencies must obtain a warrant from a judge and demonstrate reasonable cause before they can spy on their citizens. But there's nothing that prevents them from just buying that information from a third party. (And by the way, hackers and foreign governments are also drawn to these treasure troves of data.)

For example, police often ask Google for lists of all people in a certain area at a certain time—this is called a *reverse location search warrant*.¹⁰ (Google has your location history because they own the Android mobile phone operating system, Google Maps, and Waze—all of which know where you are, by default.) They might be looking for a suspect or witnesses to a crime, but this same type of search query could also show who attended a protest or a political rally, who attended services at a place of worship, or who might have visited a clinic where abortions are performed. Police also have deals with Amazon that give them warrantless access to video recordings from Ring doorbell cameras.¹¹

Here's the bottom line. When we feel like someone is watching us, particularly someone in a position of power over us, we censor our own behavior. Consciously or unconsciously, we avoid doing things that might attract undue attention. This stifles self-expression and ultimately inhibits our freedom. Citizens of a healthy democratic society need to be able to express controversial viewpoints to close friends and explore nonmainstream subjects online. Citizens even sometimes need to be able to push legal boundaries without fear of retribution for a society to evolve. While targeted, warrant-based surveillance is a legitimate limitation on personal privacy for the greater good, warrantless mass surveillance is fundamentally wrong and bad for democracy.

⁹ These are two of the "Four Horsemen of the Infocalypse"—the bogeymen that are always brought up when demanding more access to our private data.

¹⁰ <https://slate.com/technology/2019/02/reverse-location-search-warrants-google-police.html>

¹¹ <https://theintercept.com/2022/07/13/amazon-ring-camera-footage-police-ed-markey/>

Okay. There's my speech on privacy. I'll get off that soapbox now! Thank you for listening.

Selling Privacy by the Pound

I just spent a lot of time talking about privacy in mostly abstract terms. To make this more real, let's talk about some specific threats to our privacy.

For starters, there's much more to privacy than what you knowingly and willingly give away. In fact, the truly scary part is what you're giving away every day without realizing it. Your credit cards and debit cards are convenient for making purchases, both online and at brick-and-mortar stores. It won't surprise you that Mastercard, Visa, and American Express know all about where you shop, what you buy, and how much you spend. It also shouldn't surprise you that major retailers also keep similar records.

After the Cambridge Analytica scandal, no one should be surprised at the amount of information social media companies like Facebook and LinkedIn have on you. You should probably also realize that Google has more than either of those companies. Google (who owns Gmail, the Chrome web browser, the Android mobile OS, YouTube, Waze, and much more) is an advertising company—period, full stop. More than 90 percent of its revenue is from selling ads. It can charge a premium for its ads because they're highly targeted. And they're highly targeted because they know unbelievable amounts of things about us. And they keep finding ways to learn more. In early 2021, Google bought Fitbit for over two billion dollars—not because they wanted to help people exercise, but because they wanted all that juicy health data on 25 million Fitbit customers.

Still not worrying you? How about this. A whistleblower recently exposed a secret arrangement between Google and Ascension (the United States' second-largest health system) to acquire access to 50 million patient records without obtaining patient consent. This effort, dubbed Project Nightingale, would seem to violate the 1996 Health Insurance Portability and Accountability Act (HIPAA). But there are loopholes in HIPAA for sharing data with third parties in order to improve health outcomes for patients or to optimize the overall health system.

Google and Facebook often claim that they never sell your data, and that's mostly true. For them, the data are the crown jewels, the goose that lays the golden eggs. They don't sell your data—they sell *access* to your data by selling ads that target you based on this data.

However, many smaller companies, app makers, and online services do gather and sell your data outright to shady third parties called *data brokers*. I've seen estimates that there are 2500–4000 data brokers in the United States alone.¹² These companies are almost entirely unregulated in the United States. You don't own your data, and in most cases, you can't even look at your data. Have you considered why grocery stores and pharmacies have “loyalty cards”? Whenever you present your card, you are allowing them to associate all your purchases with you. While they will almost certainly use this information to better target you with store promotions, they are probably also selling this information to third parties.

Want to know what info these companies have on you? It's not easy to do in most cases, but you have a few options (which will be discussed in the checklist at the end of this chapter). What you will find is that these companies have collected a treasure trove of information about you: income range, house and car value, marital status, number of children, education level, political party affiliation, types of products purchased, debt levels, household interests, and so on. But it also gets really personal too. These companies record things like religious affiliation, race, ethnicity, sexual orientation, known health issues, and even things like your propensity to gamble. And then there are all the correlations they can make by comparing several different sets of data and everyone they think you know. They may figure out that you have a sick child, a rich uncle, or a shopaholic spouse, for example.

Ads on the Web are sold sorta like ads on physical billboards. With outdoor billboards, you have a space to fill, so you rent that space out to advertisers, probably for weeks at a time. But on the Web, these ad spaces are rented out continuously via a process called real-time bidding. In the space of fractions of a second, websites will broadcast everything they know about you (which is considerable) to advertisers and take automated bids from companies trying to reach people like you. Given the wanton

¹² You can see a small sampling of the largest data brokers here: <https://privacyrights.org/data-brokers>

dissemination of personal information, this process has been called the biggest data breach in history and is the subject of ongoing litigation in Europe.¹³

Here's another classic story. One of the most lucrative consumers is a newly pregnant one. New parents spend tons of money, and locking in brand loyalty at this stage is paramount to product sellers. In February 2012, *Forbes* ran a story about how Target correctly predicted that a woman in a household was pregnant based on the types of products she was buying: unscented lotion and soap, large quantities of cotton balls, washcloths, and particular vitamin supplements. Based on a high "pregnancy prediction score," according to the story, Target took it upon themselves to send some unsolicited baby product coupons to the woman via the mail. Unfortunately, this particular woman was a teenage high school girl living with her parents, and she had not yet told them the good news.

This exact same premise was tested recently by a reporter for *The Atlantic* who tried very hard to keep her pregnancy a secret from marketers and ultimately failed. From the article¹⁴:

I didn't download "femtech" products that track ovulation, provide cat videos while confirming a pregnancy result, or give updates on a fetus's growth. [...] I bought prenatal vitamins and pregnancy tests in person with cash, without using rewards or loyalty programs. On the internet, I tried tactics such as using a VPN and non-tracking search engines. I was cautious when going to medical appointments. Knowing the link between location and health status, I turned off my phone's GPS or left it at home during appointments.

Yet, because of the lack of data privacy in the U.S., the day finally came when I lost my battle to keep my reproductive information private. I was sitting on my couch scrolling through social media when I saw it: an advertisement for diapers. It appeared the same week that we lost the pregnancy.

¹³ There's a link with more info in this chapter's "Going Further" section.

¹⁴ <https://www.theatlantic.com/ideas/archive/2022/10/can-you-hide-your-pregnancy-era-big-data/671692/>

And just to completely demoralize you, I must state one more fact. I earlier claimed that if the product is free, then you are the product. But unfortunately, the converse isn't true: just because the product isn't free doesn't mean that you are not also the product. That is, even if you do pay for a service, that doesn't guarantee that the company providing the service won't turn around and try to make extra money off your personal information, anyway.

It was revealed a few years back that both AT&T and Verizon were adding tracking information on all of their users' Internet traffic. Basically, any time you browsed the Web from your smartphone, AT&T and Verizon were tagging all of your requests with a marker (sometimes referred to as a *supercookie*), which could be seen by any website you visit. This marker changed rather frequently, but AT&T and Verizon kept lists of all of your IDs. This allowed AT&T and Verizon to basically sell subscriptions to your online activity. But even if websites don't pay for the mapping of this ID to your full identity, they can still use that unique ID to track your movement across websites. And if they can find some other way to independently figure out who you are, then it has the same effect of deanonymizing you. The only good news here is that this particular tracking happens only when using the cellular network for Internet access, and it works only on unencrypted web surfing. When you go to websites that support HTTPS (which most now do), the communication is protected, and no tracking IDs can be added.

After a consumer backlash, AT&T and Verizon eventually gave their users a way to opt out of this tracking. In fact, Verizon was fined \$1.3 million by the Federal Communications Commission (FCC) over this (which is a drop in the bucket to Verizon). But this just goes to show that even paying a lot of money for a service doesn't guarantee that the service provider won't sell your information to make more. Sadly, we had rules in place to prevent this practice back in 2016, but before the law could take effect, the new incoming presidential administration gutted the law in 2017. So at this point, all Internet service providers in the United States are totally free to collect as much info on you as they can to use and sell as they please—and they do.¹⁵

As a sidenote, a good bit of information about you is readily available to anyone who knows where to look. Even before the Internet, I could find out a lot about you by visiting

¹⁵<https://www.privacypolicies.com/blog/isp-tracking-you/>

your local county government offices. Property taxes, marriage licenses, divorce decrees, voting registrations, arrests, police reports, car accidents, and other public records can tell a lot about you. But with the advent of the Internet, you no longer need to show up in person to request this stuff—you can find most of it online now, and much of it is free to access (some require a small fee). All of this public personal data is collectively referred to as *Open Source Intelligence*, or OSINT. This is where people search sites like Spokeo, Whitepages, MyLife, and Intelius get much of their data. In the checklist for this chapter, I'll show you several free OSINT tools that you can try out.

Ever Feel Like You're Being Watched?

How often have you actually read the end-user license agreement (or EULA) that comes with all the software you install or the online services you use?¹⁶ Buried in there somewhere is language that allows the product maker to pretty much do whatever they want with your data. And it turns out that our smart devices are collecting a lot of it.

A 2014 story in *Salon* by Michael Price¹⁷ tells about a marvelous smart TV that he purchased to replace a failing, old dumb TV. This television came with all sorts of wonderful, built-in features like web browsing, email, social media, streaming TV services, apps, and games. Then he read the fine print:

I'm now afraid to use it. You would be too—if you read through the 46-page privacy policy. The amount of data this thing collects is staggering. It logs where, when, how and for how long you use the TV. It sets tracking cookies and beacons designed to detect “when you have viewed particular content or a particular email message.” It records “the apps you use, the web sites you visit, and how you interact with content.” It ignores “do-not-track” requests as a considered matter of policy.

It gets worse. This TV has a built-in microphone and camera that are used to provide face and voice recognition. The privacy policy actually states the following: “Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party.”

¹⁶ Check out this wonderful infographic showing the relative size of various companies' terms of service: <https://www.visualcapitalist.com/terms-of-service-visualizing-the-length-of-internet-agreements/>

¹⁷ https://www.salon.com/2014/10/30/im_terrified_of_my_new_tv_why_im_scared_to_turn_this_thing_on_and_you_d_be_too

Of course, we now live in the age of virtual assistants like Apple's Siri and Amazon's Alexa. We purposely buy products that listen to us all the time so that we can ask them for the news or the weather, buy stuff, set timers and alarms, and even turn lights off and on. While these devices are often thought of as constant eavesdroppers, the reality is a little more complicated than that. I'll say more about smart TVs and virtual assistants in Chapter 7.

But one of the scariest new(er) technologies is automated facial recognition. For decades, we've had CCTV security cameras in some public areas, recording grainy video on crappy VHS tapes, whose footage would eventually get overwritten. But now high-definition digital cameras are everywhere, they're connected to centralized monitoring services via the Internet, and data storage has become so incredibly cheap that footage can be saved for years or even decades. When coupled with a database of faces, this footage can now be used to automatically identify all the people caught in the video. A Belgian artist named Dries Depoorter recently posted a project called *The Follower* that managed to map Instagram photos from several influencers to public video footage showing them taking the picture. It was all completely automated.¹⁸

In early 2020, *The New York Times* reported on a small private company called Clearview AI that makes a cell phone app that can supposedly recognize almost anyone on the planet just by taking a picture of their face. The technology is based on a database of over ten billion photos that the company "scraped" from public social media sites like Facebook, LinkedIn, Venmo, and many others. As of earlier this year, the company claims to be collecting 1.5 billion new photos per month and is aiming to increase the size of their database to 100 billion photos.¹⁹ While Clearview claims that it only sells this technology to law enforcement agencies (which is already Orwellian enough), it has sold its services in the past to Macy's, Best Buy, Walmart, casinos, and even the National Basketball Association (NBA).²⁰ Currently, there are almost no legal restrictions on the use of face recognition technology, at least in the United States.

¹⁸ The footage has since been taken down, but he might post more: <https://driesdepoorter.be/thefollower/>

¹⁹ <https://www.washingtonpost.com/technology/2022/02/16/clearview-expansion-facial-recognition/>

²⁰ <https://www.vox.com/recode/2020/2/26/21154606/clearview-ai-data-breach>

This is the world we live in now, filled with smart devices, cameras, and sensors that track our every move. This data is collected, recorded, and sold to nebulous “third parties” and “partners.” These companies aggregate all of this data, correlate your information across these data sets, and then package it up for resale to advertisers and frankly just about anyone willing to pay for it.

You have no real control over the buying and selling of this data. You can attempt to “opt out,” but you’re relying on these unregulated companies to voluntarily comply with your wishes—not just now but forever. And frankly there is just no feasible way to opt out of all data collection, even if you could figure out the exhaustive list of companies that are collecting it. It’s logistically impossible for a mortal human to do. And trust me, they know this.

Solving the Privacy Problem

While I believe that we need much more transparency when it comes to the shadowy world of data brokers, transparency alone is not sufficient. Yes, people should be able to know what data is collected, how it’s being used, and with whom it’s being shared. But the “notice and consent” model of privacy—where people are given the option to opt out—is hopelessly flawed. Have you ever looked at the privacy settings for Google, Facebook, Twitter, and others? The sheer number of settings is overwhelming, and the descriptions of these options are very misleading. At a bare minimum, we need privacy as the default—opt-in instead of opt-out. And none of these companies will offer that willingly.

What we really need are regulations. I know that many people, particularly in the United States, will cringe at the very mention of that word. It’s become a highly politicized topic here. But there’s a reason why we don’t have to personally inspect the airplanes we fly on, the drugs we take, the food we buy at the grocery, or the safety features of the cars we drive. Our governments set minimum safety standards for these products and services and appoint agencies filled with experts to make sure companies adhere to them. That’s called regulation.

Some people believe that regulations stifle innovation and hurt competition. While poorly crafted laws can certainly do this, regulation in and of itself does not cause harm. In fact, I would argue that regulation can be the mother of invention. For example, without auto and factory emissions standards, many solutions for reducing pollution and increasing energy efficiency would never have been invented. Humans are problem solvers—without challenges, we get lazy. Without necessity, there’s no need for invention.

Even from a purely capitalistic perspective, regulations are just rules for the game—rules that everyone must follow in order to play and win. How fun is a game with no rules? Or unfair rules that benefit one player over others? Regulations, when done correctly, level the playing field and promote competition.

As consumers and as citizens, we need to compel our elected representatives to stand up for our privacy rights. Thankfully, some states in the United States are starting to step in where federal regulators have failed. The California Consumer Privacy Act (CCPA) and follow-on California Privacy Rights Act (CPRA), while far from perfect, give users the right to know who has collected their data, the right to view that data, and the right to ask that their data is not sold. There are loopholes, but it's a step in the right direction. And because California is so big, many companies will end up offering these same rights to people outside the state of California, as well—much as California auto emissions standards were adhered to throughout the United States.

Across the pond, the European Union enacted an even stricter and broader set of privacy regulations known as the General Data Protection Regulation, or GDPR. This is the source of all those stupid cookie consent pop-ups on web pages—so obviously it's not perfect, either. But laws and regulations are not written in stone. We try things, learn from our mistakes, and update the laws to reflect the new information. So the good news is that progress is being made. But we still have a long way to go.

Who Can You Trust?

There's one more aspect to all of this that we should stop to consider: who can you trust? That's a critical, fundamental question, and as a society, we need to be asking it a lot more than we are. Unfortunately, there's no easy answer. And if you think about this too hard, it's easy to spiral into tinfoil hat and black helicopter territory. But my job here is to try to simplify things for you, so let's look at this from a practical standpoint.

First, let's agree on what we mean by *trust*. Violating trust is not just about intentionally trying to do you harm. Online service providers and marketing firms are certainly not trying to harm their customers by gathering and selling mass quantities of “anonymized” personal data. In fact, they would (and do) argue that they're *helping* you by tailoring the ads you see on the Web to your specific interests. By better targeting the advertisements presented to you, they increase the likelihood that you will actually want to know about

the products and services for sale while simultaneously avoiding showing you ads for things you don't want to see. They view this as a win-win situation.

At the end of the day, you need to try to determine the motivations of the person, corporation, or entity behind the advice or service being offered. How do they make their money? Are you paying a fair price for what you're getting? If you're paying nothing or if the price is too good to be true, then you should think carefully about trusting the source—or at the very least, question whether your interests align with theirs. For example, many online review sites make their money by getting kickbacks when you click links on their site to visit the products they recommend. It should come as no surprise that many products that provide hefty referral fees often end up with top review scores and companies that don't provide kickbacks somehow don't make the list. (This is particularly true for VPN and antivirus review sites, by the way.)

Of course, these services are not free to produce and maintain. But people have come to expect free stuff on the Web. Unfortunately, the only business model we've managed to come up with to support free stuff is advertising. To be clear, I'm not against ads—I understand the need to make money. Watching ads is an ugly but viable option for monetizing your website; when I get upset is when those ads are watching me.

Of course, many sites and apps also make money off selling your information to interested third parties—which you probably agreed to when you signed up for the service, in cryptic language buried deep in the license agreement. Sadly, as we discussed earlier in this chapter, we also know that paying a fair value for a service does not mean you can trust the provider, but the odds are at least better.

Besides “following the money,” you also need to think about other motivations and ask deeper questions. Is it in this service provider's own best interest to be open, honest, and transparent with you? Or do they stand to gain more if they confuse, mislead, or scare you?²¹ Let's think about that one for a minute. Before the advent of the Internet and before 24-hour cable news networks came into being, most people got their news from newspapers and the nightly TV news. In the “old days” (like 30–40 years ago), TV news was not about making money—it was about providing a public service. (This wasn't out of the goodness of their hearts; it was actually mandated by the Federal Communications Commission under various “public interest” requirements for broadcast licensees.²²)

²¹ This is sometimes referred to as FUD: fear, uncertainty, and doubt.

²² https://benton.org/initiatives/obligations/charting_the_digital_broadcasting_future/sec2, reference 32. Amendments to Delegations of Authority, 59 FCC 2d 491, 493 (1976).

However, in the intervening years, as Nielsen ratings and advertising dollars have become the driving force in television, our “news” programs have become “infotainment.” The focus is not educational or informational; it’s about getting (and keeping) eyeballs. “Will watching the nightly news kill you? The answer will shock you! Tune in at 11!”

Similarly, the Internet economy is based on attention or “engagement.” Boring facts and uncontroversial topics don’t rivet people in their seats or keep them scrolling. The more sensational and urgent, the better. And by the way, that wasn’t the actual intent of a lot of these artificial intelligence algorithms that were used to decide what content to show you next. They were just told to figure out what would keep people scrolling, wanting more content.

So, bottom line, if reading or watching something provokes a strong emotional response—particularly fear or anger—be sure to double-check the story before you react. And triple-check it before you act on it or share it with others. I’ll give you some tips on how to do this in the checklist for this chapter.

Step Away from the Ledge

Okay...let’s take a collective deep breath here. Despite all the doom and gloom in this chapter, things are not all bad. And more to the point, they don’t have to be. We can have both security *and* privacy. In fact, I would argue you can’t have one without the other. And collection of personal data isn’t intrinsically evil, either. Let me explain.

Earlier in this chapter, I said that you can’t erase people’s memories. When your sensitive, private information is exposed, you can’t undo that. I’m sure many of you were thinking to yourselves: *It’s too late for me. I’ve already given up so much of my information.* The horse has left the barn, the genie is out of the bottle, the cat is out of the bag—pick your metaphor for “I’m screwed.” While humans can have long memories, the information that ad companies like Google and Facebook keep on you has a limited shelf life. They strongly prefer recent data. If you stop oversharing now, the data they’ve been hoarding all these years will eventually get stale and age out. In some areas of the world that have decent privacy laws, there are limits imposed on how long data can be retained. And when the rest of the world catches up, companies may be required to flush some or all of the data they have down the virtual toilet. Don’t throw in the towel. Taking action now *will* improve things down the line.

Note also that I'm not against saving lots of data, per se—not even personal data. We can learn a lot of extremely important and beneficial things by analyzing all the data we're generating. For example, by analyzing patient data, we can figure out how various drugs interact, in both positive and negative ways. When we analyze public wastewater, we get invaluable insights into the health of a local population. We can use real-time traffic data to help police and firefighters reach their destinations faster. We can use historical traffic data to decide where to spend precious tax dollars on infrastructure improvements. But we don't need to associate any of that data with a specific person for it to be helpful. We just need to aggregate and anonymize our data.

There is a lot of research being done on novel approaches to retain the usefulness of group data without compromising the privacy of any individual in the group. For example, *differential privacy* is a technique for methodically and randomly altering data from individuals in a group while maintaining the overall statistical characteristics of the group's data. This makes it harder to reidentify anonymous participants while preserving the analytical value of the data set. There's another technology called *homomorphic encryption* that allows data processing to be done on scrambled data—basically meaning you can do statistical analysis on a set of data while having direct visibility into the individual data records.

When you watch old sci-fi shows like *Star Trek*, the computers knew all about you—but they also used that information to help you and didn't share it with others. In the 2013 movie *Her*, Joaquin Phoenix's character shared every aspect of his life with his AI virtual assistant (voiced by Scarlett Johansson), and she used that information to counsel him. There was never any notion in this movie that she would ever reveal this information to others or use it for any purpose other than to help him. He eventually (spoiler alert) fell in love with her. In both of these cases, the receiver of the personal information strictly acted in the best interest of the person sharing the information. This is a concept called being a *data fiduciary*. Like doctors, lawyers, and some (not all) financial advisors, they are compelled by law to keep your data private and only use it in ways that benefit you, not themselves or anyone else. We have precedent for this already.

So it's not a lost cause. This game is not over yet. We can—and I believe we will—fix the privacy problem. And until such time as we decide as a society to outlaw the needless collection and misuse of personal data, there are still many things we can do as individuals to protect our private information. I will tell you every technique and trick I'm aware of in this book, and I know a lot of them.

Summary

- There's a lot more to privacy than most people think, and privacy is more important than many of us realize.
- Privacy is not just a "me" thing; it's very much a "we" thing too. Our photos, videos, social media posts, and contact lists contain information about dozens if not hundreds of other people. When you give away your information, you're giving away mine, as well.
- Privacy failures can be more impactful than security failures. While you can at least theoretically replace lost money and stolen goods, you can't erase people's memories.
- As humans, we act differently when we think we're being watched—we essentially self-censor. This is not just bad for us as individuals, but bad for all of us as a society.
- Consumers and corporations are generally on the same side when it comes to security. The same cannot be said for privacy. Corporations gather gobs of sensitive personal information to serve you hyper-targeted advertising. This creates an inherent conflict of interest.
- Similarly, governments will ask you to give up your privacy so they can protect you. But some governments (often foreign ones) will also use this information for political and social influence. You don't need to give up privacy to gain security—you can have both.
- Our data is being collected, shared, and sold constantly. The financial incentives for doing so are impossible for publicly traded companies to ignore. They have a fiscal responsibility to their shareholders to pick that money up off the table whenever and wherever it's available. Therefore, we need laws (a.k.a. regulations) to control the collection, storage, usage, and sharing of our personal data.
- It's not a lost cause. Personal data has a half-life, like nuclear waste: over time, it loses potency or value. If you stop oversharing now, the data you've already shared will eventually be thrown out.

- Data collection is not bad, in and of itself—as long as the data is properly aggregated and/or anonymized. This can be tricky to do, but it can be done. All of this collected data can and will be used to benefit society. We just need to stop the misuse of our data.

In the next chapter, we'll review some basic computer concepts and terminology and then dive into some heavier topics like encryption and cryptography! Don't worry. I have some fun ways to explain these topics.

Going Further

As you might suspect after reading this chapter, I'm pretty passionate about privacy. Over the years I have collected a ton of excellent resources I can recommend. If for some reason you are still not fully convinced about the importance of privacy for yourself personally and for all of us collectively, please follow these links to find some very compelling arguments from other people:

- *The Value of Privacy*: A great essay by Bruce Schneier, who literally wrote the book on cryptography. https://www.schneier.com/blog/archives/2006/05/the_value_of_pr.html
- *Why privacy matters*: A persuasive TED Talk by Glenn Greenwald, one of the journalists who Edward Snowden tapped to expose the NSA's mass surveillance program. https://www.ted.com/talks/glenn_greenwald_why_privacy_matters
- *Terms of Service Didn't Read*: You read the terms of service before clicking "Accept," right? Neither did anyone else. This site helpfully summarizes several popular sites' terms of service. <https://tosdr.org/>
- *Terms and Conditions May Apply*: A great documentary about how we all agreed to rampant data collection. <https://tacma.net/>
- *The Great Hack*: A must-see documentary that explains how Cambridge Analytica used Facebook data to influence voters in the 2016 US election, Brexit in the United Kingdom, and many other elections around the globe. <https://www.netflix.com/Title/80117542>

- *Anon*: As a dystopian sci-fi movie, it's so-so; but it serves as an insightful criticism of ubiquitous facial recognition systems. <https://www.netflix.com/Title/80195964>
- *Why encryption is important*: A nice summary of debunked privacy myths. <https://www.accessnow.org/why-encryption-is-important/>
- *Visualizing terms of service*: A fun infographic showing the relative lengths of the legal terms you agree to when using many popular services. <https://www.visualcapitalist.com/terms-of-service-visualizing-the-length-of-internet-agreements/>
- *What is Real Time Bidding?* A report by the Irish Council for Consumer Liberties on why online ad auctioning is effectively the biggest data breach in history. <https://www.iccl.ie/what-is-real-time-bidding/>
- *Snopes.com*: Before you forward that email or retweet that post, before you even let some article scare or upset you, check it for accuracy. This site is one of the best. <https://www.snopes.com/>

Checklist

While I will share several other specific recommendations on how to protect your privacy throughout this book, in this chapter I've collected a few more general tips and techniques.

Tip 2-1. Know What They Know

I've tried to explain how much data is being collected on you, but until you see it for yourself, you honestly can't imagine the literal magnitude of the problem. Many of the big online services have a way for you to download all of your information in one fell swoop—every email, every post, every picture, every “like,” every friend, every contact... You get the idea. I recommend you try this, if for no other reason than to understand the sheer quantity of information these companies have on you. Pay special attention to any marketing information—the ads they've picked for you, the demographics they've guessed for you, and so on.

The following are links that explain how to do this for each service. The general procedure will be to select all the data you want to download and then select how you want to receive that data. I would recommend asking for a simple download link to a “zip” file (or perhaps several zip files). A zip file is a compressed archive of a bunch of files and folders. Once you download this file, you can double-click the .zip file, and it will expand to a single folder that is full of other files and folders.

Note that it may take several hours or even several days for the service to collect this information. And it will probably take a while to download all of these massive files. Finally, it will probably also take you hours or days to look through it all. But I strongly encourage you to at least skim each and every bit of it so you know what's there. Once you've looked through all the files, you can delete them if you need to reclaim the hard drive space.

You have the European Union to thank for this, by the way. The General Data Protection Regulation (GDPR) mandated this capability for EU citizens, and most companies have made this available to anyone.

- *Google*: Note that Google owns the Chrome browser, the Android mobile operating system, YouTube, Waze, Gmail, and literally dozens of other services. When you see the full list, you'll be blown away. You can choose what to download here, and I suggest getting everything except maybe your emails. They take up a lot of space, and you should already have ready access to your emails. <https://takeout.google.com>
- *Meta (Facebook)*: Meta is the new name for Facebook. <https://www.facebook.com/help/405183566203254>
- *Instagram*: Note that Meta owns Instagram. <https://help.instagram.com/181231772500920>
- *Twitter*: <https://help.twitter.com/en/managing-your-account/how-to-download-your-twitter-archive>
- *LinkedIn*: <https://www.linkedin.com/help/linkedin/answer/50191/accessing-your-account-data>
- *Apple*: Again, like Google, you can probably skip downloading all of your emails here and just get the other stuff. <https://support.apple.com/en-us/HT208502>
- *TikTok*: <https://support.tiktok.com/en/account-and-privacy/personalized-ads-and-data/requesting-your-data>
- *Pinterest*: <https://help.pinterest.com/en/article/download-your-pinterest-data>

Tip 2-2. See What Your IP Address Reveals

Your unique Internet (or IP) address, because of the way these ranges of numbers are administered, can tell a lot about you—not only the name of your Internet service provider (ISP) but also where you are physically located (at least city and state). Every website you visit can see and therefore record your IP address—that's just how the Internet works (which I'll explain in Chapter 3). You can see this yourself:

<https://www.iplocation.net>

Note that some of the information shown here actually comes from your browser, not your IP address. We'll learn more about that in Chapter 8.

Tip 2-3. Opt Out Where You Can

While it's hard to truly opt out of all tracking, you should still take every legitimate opportunity to do so, if for no other reason than to register your disdain. Here are a few sites you can visit and tools you can use to reduce spam, phone calls, and regular post office junk mail:

- *This site has lots of great info:* <https://www.worldprivacyforum.org/2015/08/consumer-tips-top-ten-opt-outs>
- *Opting out of credit card offers:* <https://www.optoutprescreen.com>
- *Opting out of online tracking:* <https://optout.networkadvertising.org>
- *Opting out of Google "interest-based" ads:* <https://adssettings.google.com>
- *National "do not call" registry:* <https://www.donotcall.gov/>
- *Opting out of direct marketing mail and email:* <https://www.dmachoice.org/>
- *This site has a ton of information (probably too much) about what specific websites and real-world retailers collect and how to opt out:* <https://simpleoptout.com>

Tip 2-4. Investigate Your Own Public Information

If you're a normal adult, you probably have several public records containing personal information that are readily available online. This of course includes social media and search engine results, but also public records like property tax information, marriage and divorce filings, voter registration, and more. This is called Open Source Intelligence, or OSINT. This website has a gazillion online search tools to help you find this sort of information. Try some of them out:

<https://inteltechniques.com/tools/>

Removing yourself from people search sites is a daunting task. I'm frankly not sure it's possible today. But this article will explain more about how these sites work and give you detailed instructions for removing your data from some of the top sites:

- “Remove your personal info from the top 7 people search sites without charge” (Kim Komando, USA TODAY, October 2022):
<https://www.usatoday.com/story/tech/columnist/komando/2022/10/06/remove-personal-data-from-people-search-sites/8179864001/>

Tip 2-5. Get Your Stories Straight

We've all gotten those emails about dying children wanting to get emails from around the world, Disney giving away free passes, or urgent COVID-19 health information. There are many hoaxes and “fake news” stories out there that sound very real. Furthermore, we have technologies today that can manufacture very believable pictures, audio clips, and even videos that are completely fictitious called *deep fakes*. Many of these stories intentionally play on your emotions. When you start to get worked up about something, this should be a signal to verify the source before reading more—and certainly before you even think about sharing it with others.

How do you do that? You can always just search the Web using a key phrase from your email (maybe the subject line) plus the word “hoax.” Or you can just go to Snopes, whose whole purpose is to document these sorts of things. Some of them are even true. They do the homework for you. I trust them:

<https://www.snopes.com/>

Tip 2-6. Operate on a Need-to-Know Basis

Many websites, apps, and retailers will “require” you to give them personal information for various dumb reasons. Always challenge this assertion and ask if there is an alternative. Information like your email address, cell phone number, birthday, full name, and home address can be used to track you or even steal your identity. Here are a few ideas to consider:

- If you can't avoid giving out personal information, you can often just lie. If you know you'll never need to interact with this person or business again, just give them false information where possible. I often do this with my birthday. I just choose a reasonable date. Obviously, if they need to call you or ship you something, you probably need to give them a valid answer.
- You can still lie to companies that you'll interact with again, as long as the lies don't really matter (like your birthday). However, you should carefully note down your lies somewhere in case you need to lie again later. For example, let's say you're having trouble with your account and the support person asks you to confirm your birthday as part of an account verification process. You'll need to know the lie that you told them when you signed up.
- Here's a fun workaround to avoiding tracking at the grocery store or pharmacy. If the store allows you to find your loyalty account using your phone number, try your local area code plus 867-5309. If you were a 1980s teenager, you'll recognize this as the telephone number for "Jenny" from the one-hit-wonder song by Tommy Tutone. Apparently, people often give this number out, so it may already be in the system.
- If some website requires you to upload a picture of your face and you don't care if it's wrong, then upload a fake picture. Now, I don't mean "upload someone else's picture." I mean "upload a picture of a nonexistent person." This website will generate fake faces on demand. Reload the page to get a new face:
<https://thispersondoesnotexist.com/>

CHAPTER 3

Castle Guard Certification

Before we can begin to discuss security, we really have to define some key terms and concepts. You do *not* have to memorize this stuff, and it's okay if you don't follow everything here. But for the rest of this book to make sense, I need to get you up to speed on the basics of how computers and the Internet work. I've thrown in some fun little tidbits that will help to keep things interesting. There will be a wide range of people reading this book, and I just can't take the time to fully explain everything. But in this chapter, I'll give you a solid base to work from.

I'm trying to cover all the bases here, so if you see a topic you already understand, feel free to skip it or just skim it. There's a glossary at the end of this book that you can refer to for quick help, or you can return here if you want to refresh your memory.

Castle Guard in Training

Let's revisit our castle analogy—but now you're not the lord of the castle; you're a bright young castle denizen who has applied for a job on the elite castle guard detail. However, in order to land this prestigious position, you must complete the Castle Guard Certification Program. After all, you need to know a portcullis from a parapet, a battlement from a barbican, and a mace from a morning star. Upon successful completion of your training, you will receive a fancy scroll, signed by the castellan of the keep. Surely something you would brag about on whatever the equivalent of medieval social media would be.

To defend your lord's castle proficiently, you must understand the layout of the castle and how its defenses work—not just individually, but in concert. You will need to study your likely enemies and their preferred methods of attack. And finally, as you will sometimes be tasked with conveying secret missives between the lord and the king, you must also be trained in the art of secure message delivery.

So, returning to modern parlance, to fully understand the security and privacy advice I'm going to give throughout this book, you need to be familiar with some basic computer and Internet stuff. This may sound boring or maybe even intimidating, but I'm going to do my level best to make it entertaining and easy to understand. Let's start with how computers work. This may be a review for some of you, but I'll bet even tech-savvy people will learn something new here.

Computer Lingo

Computers are everywhere. I don't just mean desktop computers and laptops, either. Just about every piece of modern electronics has some sort of computer chip in it, running some sort of software. We're entering the era where all of these computers are interconnected: appliances, thermostats, TVs, doorbells, security cameras, cars, and even toasters and light bulbs. Despite their ubiquity, computers are not well understood—and for good reason: they're phenomenally intricate pieces of engineering! My first computer was a Texas Instruments TI-99/4A (see [Figure 3-1](#)).



Figure 3-1. *Texas Instruments TI-99/4A personal computer (circa 1981)*

This computer had only 16KB of memory. My daughter's first iPod had more than 250,000 times as much memory! A guy named Gordon Moore (cofounder of Intel) wrote a paper in 1965 that predicted that computing power would double about every two years. This prediction turned out to be pretty accurate and was later dubbed Moore's law. The act of doubling is deceptively powerful. Let me give you a classic example. Let's say I gave you a penny on January 1, and I offered to double its value every day for the rest of the month. So on January 2 you'd have two cents. A week later you'd have a whopping \$0.64. Two weeks later you'd be up to \$81.92. Now we're getting somewhere, but it still doesn't seem like much. By the third week, however, the value of your stash would be more than \$10,000, and by the end of the month, after 31 days of doubling, you would have a whopping *\$11 million dollars*! That's the power of doubling. Using Moore's law, we can estimate that desktop computers today are more than a million times as mighty as my little TI-99/4A.

Entire books have been written about how computers work,¹ but for our purposes here, I just want to cover the essential ideas at a very high level. Remember, you do not have to remember all of this; I'm just trying to get you familiar with some terms and concepts. Check the glossary if you need a quick note to jog your memory.

Hardware and Software

You can't talk about computers without talking about *hardware* and *software*. Hardware refers to the physical computer and all its parts—basically the things you can see and touch. This includes not only the computer itself but the things attached to it, as well. We generally refer to these attached devices as *peripherals*, and they include the mouse, keyboard, monitor, printer, disk drives, and so on.

Software is the computer code that runs on the hardware—the complex set of instructions telling the hardware what to do in every possible situation the programmer could think of, including (and often especially) when bad things happen. The prime piece of software that runs the computer itself is the *operating system* (OS). Software *applications* are smaller, more-focused pieces of software that are meant to do specific things, like help you edit a document, listen to music, or surf the Web. The operating system handles things like starting and stopping applications, managing the computer

¹ One of the best books on how computers work for the layman is *Code* by Charles Petzold. I was fortunate enough to interview him on my podcast: <https://www.charlespetzold.com/books/>

files, connecting you to the network, and taking input from or sending output to the peripheral devices like your mouse, keyboard, monitor, and printer. The OS is a special software application that must be there for the computer to run; applications are optional add-ons that perform specific tasks.

For most PCs, the operating system is Microsoft Windows; for Apple's Macintosh computers, the operating system is called macOS (previously "Mac OS"). Examples of applications include Microsoft Word, Adobe Photoshop, Google Chrome, and Apple's FaceTime.

You can sort of think of hardware and software in terms of a stage play. The hardware is the stage, set, curtains, lights, and sound system. The operating system is like a combination of a script, director, and stage crew—the OS controls the overall flow of the show, making sure the actors follow their lines and setting up the environment for the scene (props, costumes, lighting, sound effects). Finally, the actors are sort of like the applications, performing specific roles based on the script and interacting with the props (data and peripherals).

File Manager

When you're sitting at your computer and you want to look at the list of files stored on it, you do this with the *file manager*. In Windows, this is called File Explorer; on a Mac, it's called the Finder. When you double-click a folder on your desktop or open This PC or Macintosh HD, you are launching the file manager. This may seem trivial, but some people aren't used to giving it a name.

Bits and Bytes

All the data on your computer—every document, every image, and every movie and song—is stored as bits and bytes. By the way, this includes all of your software applications and even the operating system itself. Bits and bytes are the building blocks of digital things. A *bit* is the smallest piece of information on a computer. A bit has two possible values—0 or 1. A bit, therefore, is binary. That's just a fancy way of saying that it can have only two possible values (*bi* means "two"). In fact, "bit" is just shorthand for "binary digit." We abbreviate bit with a lowercase *b*.

To build bigger things—like larger numbers, alphabetic characters, and those fun little emoji icons—we need more than a single bit. The next largest chunk of digital data is the *byte*,² which we abbreviate with a capital *B*. There are eight bits in a byte. So, since each of those 8 bits has 2 possible values, if you do the math, there are 256 possible combinations of 8 bits: 00000000, 00000001, 00000010, 00000011, and so on, till you get to 11111111.

We use various patterns of these bits to represent meaningful pieces of information—this is called *encoding*. There are a gazillion ways to encode things, mostly because you can do it any way you want as long as you spell it out clearly so that someone else knows how to *decode* it. One common example of encoding is ASCII (pronounced “ass-key”). ASCII is used to encode characters—letters, numbers, and other symbols that you would find on a computer keyboard. For example, the letter *A* is encoded as 01000001 in ASCII. Because we want to tell the difference between uppercase and lowercase, we need an encoding for both. Lowercase *a* is encoded as 01100001. Basically, anything you can type using a computer keyboard has an ASCII representation. So, using ASCII mapping, “Hello” would look like this:

01001000 01100101 01101100 01101100 01101111

The first eight bits, 01001000, represent the letter *H*, and so on. It looks ugly and complicated to you as a human, but this is the language that computers speak, day in and day out.

Now, let’s talk about bigger data. One byte might be enough to encode a single key from the keyboard, but that’s not terribly useful. To encode entire documents, images, movies, and so on, we need lots of bytes. And just like we have shortcuts for large decimal numbers (thousand, million, billion, etc.), we have shortcuts to describe lots of bytes. These terms are based on standard metric prefixes: kilo (thousand), mega (million), giga (billion), tera (trillion), and so on. So, a kilobyte (KB) is a thousand bytes, a megabyte (MB) is a million bytes, a gigabyte is a billion bytes, and a terabyte (TB) is a trillion bytes.³

²Okay, historically, the next largest grouping of bits is called a *nibble*; believe it or not. That’s 4 bits. No one uses this anymore.

³Almost. Because computers are so tied to binary counting, they count things based on the powers of 2. You frankly will probably never need to know this, but if some smart-ass tells you that 1KB is not really a thousand bytes, they’re right... it’s technically 1024 bytes. Why? Because. Just trust me. For most purposes, you can just call it a thousand and be done with it. The same is true for the others (MB, GB, TB)—just go with thousand, million, billion, and trillion. It’s close enough.

Storage

For your computer to store and process all these bits and bytes, it needs somewhere to keep them. There are all sorts of sophisticated levels of storage space on your computer, but the two most important ones are *random access memory* (RAM) and the hard drive. When you buy your computer, these are two of the most prominent specs you'll see on the box.

The best analogy I've come across for understanding how computer memory works is comparing your computer to a workshop. Your workshop holds all your tools and materials. You use the tools to work on the materials. You either make new things or modify old things. But you don't simultaneously use every tool and all your materials—you generally use one at a time, or a few at most. When it's time for you to work on a project, you fetch the specific tool and materials that you need for the moment and bring them to your workbench. When you're done, you put the tool and remaining materials back. If you try to work on too many things at once, you'll find that your workbench is full—you literally cannot use all your tools and materials at once; you have to choose. Maybe you can try to just move some to the floor nearby and swap them with something else when you need it again, but this is not very efficient.

Your computer works in a similar way. Your hard drive is like your workshop—it holds all your data and all your apps, ready for you to use. When you launch a particular application or open a file, the data for the file and the application are copied from your hard drive into RAM where the computer can work with them directly and most efficiently. When you close the app, the data is copied back from RAM to the hard drive. That's why the hard drive is so much larger than your RAM. The hard drive has to hold everything, whether you're working on it right now or not; the RAM only needs to hold what you're actively working on. The more RAM you have, the more you can work on at one time—like having a bigger workbench. When you fill up your RAM, your computer actually moves things back to the hard drive to make room, trying to swap things back when you need it. That's why your computer becomes really sluggish if you try to open too many applications or big files at the same time.

If you have too much crap in your workshop, you have two options: build a bigger workshop or get some sort of external extra storage space, like a rented storage room or maybe a shed in the backyard. Similarly, if you want to work on more things at one time, you need a bigger workbench. When this happens on your computer, you have similar

choices. When you want to hold more data, you get a bigger internal hard drive or buy an external hard drive. When you want to work on more things at once, you need to buy more RAM.

Networks (Wired and Wireless)

When computers talk to one another, they do it over a *network*. Put another way, a network is a set of connected computers that are all communicating using a common computer communication language, or *protocol*. Most computer networks today use a communication language called the Internet Protocol (IP). Networks vary wildly in size but come in two primary forms: public and private. The public network we all know and love is the massive, globe-spanning network called the Internet (originally from the term *internetwork*).

However, there are countless small, private (or semiprivate) networks that are attached to the Internet. These are usually referred to as *local area networks* (LANs). You might think of corporations being the primary owners of LANs, but if you have a router at home with more than one computer or device on it, then you have a LAN too.

Networks can be wired or wireless or (often) both. Computers that are wired to the LAN use Ethernet cables (they look like phone cables with a wider plastic clip at each end). Computers that are wirelessly connected to the LAN use Wi-Fi.⁴

Figure 3-2 shows a picture of a standard Ethernet cable (wired connection) and the internationally recognized symbol for Wi-Fi (wireless connection).



Figure 3-2. *Ethernet cable (left) and Wi-Fi logos (right)*

⁴The term Wi-Fi is just a marketing term someone made up. It was meant to sound like Hi-Fi but doesn't really stand for "wireless fidelity." It's just a lot catchier than 802.11, which is the technical specification name.

You can't talk about cybersecurity without understanding some basic things about how computers communicate. I've devoted a whole section to this topic later in this chapter. But I think one of the more elegant analogies I've ever heard when explaining computer topics came from an online class I took during the pandemic.⁵ The instructor compared computer languages and communication protocols to the spoken languages. You construct languages using words and grammar. While these words may share a common alphabet, the words may be unique or have different meanings—just as communication protocols all use bits and bytes, but you must understand the protocol and the encoding to interpret them properly. Like many modern computer communication protocols, human communication is built in layers—from alphabetic characters, to words and paragraphs, to chapters, to whole documents. At even higher layers, we add formatting rules for specific applications—from food recipes to Haiku. We even have two primary methods for conveying information with languages: spoken (“wireless”) and written (“wired”).

Bandwidth

When we move data around, we like to know how fast it can go. We measure this in “bits per second,” usually megabits per second (Mbps) or gigabits per second (Gbps). This measurement is referred to as *bandwidth*. Most people run into this value in two places: when they're signing up for service from an *Internet service provider* (ISP) and when they're looking at networking products like Wi-Fi routers.

The useful way to think about bandwidth is moving water through a pipe. You can move more water, faster, through a bigger pipe. The Internet is often referred to as a series of pipes (or tubes), and that's because of the water analogy. If you think about how water gets to your house from your town's main water source, that's similar to data moving on the Internet, at least in terms of speed (see the next section for the routing part). There are big pipes at the source that take lots of water to your neighborhood, then there are smaller (slower) pipes that come to your home, and finally there are much smaller pipes that take the water to your sink, shower, and so on.

⁵The class came from a fabulous New York-based outfit called the Tech Learning Collective. They specialize in teaching computer classes for nontechnical people, with a focus on practice skills. Their primary goal is teaching cyber self-defense to at-risk groups, but they welcome any and all students: <https://techlearningcollective.com/>

It's much the same with your Internet service. The connections within your house are the slowest (the smallest pipes). The connection from your house to the neighborhood junction box is a good bit faster. The connection from the junction box to your cable provider is faster yet. And the connection between your service provider and the next service provider is the fastest—the biggest “pipe.” These superfast connections are often referred to as the “Internet backbone.”

Bluetooth

Bluetooth is the funny name of a very handy wireless connection technology.⁶ Its main purpose is to remove the need for pesky wires. Originally this was used mainly to connect peripheral devices (like mice and keyboards) to your computer over short distances. But it's gained a lot of popularity for sending and receiving digital audio. Examples include hands-free car connections to your mobile phone, portable speakers, and, of course, wireless headphones. It is also used in some modern remote controls because it doesn't require line of sight like the more common infrared (IR) remotes. Figure 3-3 shows the official Bluetooth symbol, so you'll recognize it when you see it.



Figure 3-3. Bluetooth logo

Computer and Internet Buzzwords

We're almost done, but there are a handful of other marketing and techie terms we should touch on before we move on to cybersecurity stuff.

⁶The name has an even funnier origin. It's named after a Viking king, Harald “Bluetooth”, who had a dead tooth that was blueish gray. The Bluetooth symbol is a juxtaposition of the Norse runes for “H” and “B”. <https://brianklaas.substack.com/p/the-bluetooth-viking-and-the-scattered>

Clients and Servers

When two computers talk to each other, one of them is usually asking the other one to do something. The requester is called the *client*, and the responder is called the *server*. While it's possible for one computer to be a client in some cases and a server in other cases, in today's Internet age, almost all requests originate on your computer (client) and terminate at some big computer out on the public Internet (server). Example requests might include "show me the video with the cat playing piano" or "find all the websites with pictures of Scarlett Johansson" or "post this totally cool photo of me for all my friends to see."

The Cloud

This must be one of the most overused (and abused) terms in modern computer lingo. So, what is it? When someone refers to *the cloud*, all they really mean is that it exists or is happening somewhere out in the Internet. The common industry joke is that "the cloud" just means "someone else's computer."

When engineers draw diagrams of computer networks, they often use a picture of a cloud to represent some vague grouping of things "out there"—we can't really see what's in there and don't really care (or don't wish to show it). Things enter one part of this nebulous fog and they emerge somewhere else. Sometimes they change in there and sometimes they just come out the same. Sorta like the Internet, eh? I'm convinced that this is the origin of "the cloud," though I'm not sure we'll ever know for sure.

Today all of our computers and devices are connected via the Internet, and the connections have become so fast that we can actually send our data to some remote server for processing instead of doing it all locally on your computer. When you send your data to the Internet for something out there to work on it, we call it *cloud computing*. An example of this would be Google Docs: instead of running Microsoft Word locally on your computer (modifying a file on your hard drive), you edit your document in a web browser, and all of this is happening on a faraway computer owned by Google. When you store copies of your data using a service like Dropbox or Google Drive, this is *cloud storage*—while the files exist on your local hard drive, they also exist on the Dropbox or Google server.

Net Neutrality

Another term that has gotten a lot of buzz and is often misunderstood is *net neutrality*. In recent years, you may have heard politicians and corporate spokespeople screaming about why it's going to destroy the Internet and ecommerce...or why it will save it. So, which is it?

Net neutrality, as a concept, means that no person or company on the Internet should be allowed to have preferential treatment. The Internet should be a level playing field. When you define it like that, it sounds pretty good, right? So, let's look at a real-world example and see how this definition holds.

Netflix is a very popular movie-streaming service—so popular that by some estimates it accounts for over a third of all Internet traffic during peak hours! (And during the coronavirus “social distancing,” it was even higher.) As you might expect, slinging all those bits around can seriously tax the servers on the Internet. If an ISP has to buy more equipment to handle all that demand, shouldn't Netflix have to pay them some more money to help cover the costs⁷?

It's tempting to say yes, they should. But it's a slippery slope. The bottom line is that Internet service providers are selling a service, and if they can't deliver what they've promised, then they need to invest some money in their infrastructure. If that requires raising costs for the service, then that's what they need to do, perhaps creating tiers of service so that only the people using the most bandwidth pay the most money. But we can't be asking the companies providing popular services to foot the bill or it will turn into a money grab, and the only companies that will be allowed to play are the ones who can pay. The reason Netflix and other startups flourished in the first place was because they could compete on an even playing field. The little guys always want regulation to keep things fair because otherwise they could never compete with the deep-pocketed incumbent powerhouse corporations. But once you become a powerhouse corporation, you want to get rid of these regulations, so you can tilt things in your favor and keep out the competition.

Net neutrality is not new. It's what we had all along, at least in the beginning of the Internet era. We need to preserve it so that the next Google, Netflix, or Facebook can come into being. Unfortunately, in 2018, the US government rolled back regulations that

⁷ South Korean Internet service provider SK Broadband sued Netflix recently because the hit show *Squid Game* was so popular, their network was swamped trying to stream it. Netflix lost, but appeals are ongoing.

would have ensured a fair playing field. Since the repeal, Verizon throttled the Internet usage of firefighters who were battling some of the worst forest fires in history. When AT&T bought HBO, it allowed its cellular customers to watch it without the streaming data counting against their data usage. Sounds nice, but it's the opposite of the Netflix problem: no startup streaming companies can compete with free, giving HBO an unfair advantage. These companies are basically unregulated now.

The Internet of Things (IoT)

The term *Internet of Things* refers to the current push to add Internet connectivity to everyday devices: toys, appliances, water meters, thermostats, you name it. This allows you to control these devices from your smartphone or computer, even from outside the house. Of course, this means that others may be able to control them, as well, if they can find a bug in the software to exploit (or if you pick really crappy passwords and/or reuse a password that was hacked in a data breach).

These devices are almost always tied to some sort of cloud service. These devices are constantly “phoning home” to the manufacturer or third parties to provide those cool Internet-connected features. They're probably also sharing data about what you do with those devices. The Amazon Echo products are often brought up when discussing IoT—small Internet-connected devices that respond when you say the phrase “Alexa” (this is referred to as the *wake word*). You can ask for the weather forecast, get the latest news, order products from Amazon, and even control other IoT devices in your house. However, this also raises some obvious questions about privacy. I'll cover that later in the book.

Know Your Enemy

Understanding the castle and its defenses is just the first part of your training, and probably the easiest part. Now you need to study your potential adversaries. These can be spies from neighboring regions, thieves from criminal organizations, or even armies from rival nations. Understanding their motivations and resources is above your pay grade. But you need to be able to recognize the weapons and tactics that may be used against you, so that you can make the best use of the castle defenses and even just understand what your boss is talking about at the daily guard meeting.

While I'm guessing you've at least heard most of the terms from the previous section, I'm guessing several of the terms in this section will be new to you. There are a handful of cybersecurity terms that get thrown around quite a bit in news stories, but they're rarely defined clearly or correctly. So, let's take a minute to define some common cybersecurity terms and phrases.

Zero-Day Exploit

Exploit is the general term for some sort of chink in your cybersecurity armor—a flaw or vulnerability that will allow bad things in. Exploits are usually software bugs in your operating system or an application like a web browser, PDF reader, or browser plug-in. A bug is just a mistake in the code—some software engineer (like me) screwed up and missed something. It's actually quite easy to do, even for seasoned software writers, which is part of the reason we have so many problems with malware these days.

A *zero-day exploit* is one that was previously unknown to the general public, particularly to the creator of the software containing the vulnerability. Essentially it means that the bad guys found it before the good guys did—the good guys have had zero days to fix the problem. It's important to note that many bugs go unnoticed for years before they're discovered, by either side. The vulnerability dubbed Shellshock, announced in September 2014, is one of the worst zero-day bugs ever found—and it was lurking in the software since 1989!

Malware

Malware is short for “malicious software,” and it's a catchall term for software that intentionally does bad things. As you might imagine, there are many different varieties of malware out there. And it's actually common for bad guys to use multiple types of malware in a given attack, often deployed in stages. The dynamics favor the bad guys: while the defenders have to be successful every time, the attackers only need to succeed once. So, let's review the main flavors of malware.

Virus: A computer virus is probably the first thing that popped into your mind when you read the definition of malware. A *virus* is a piece of malware that is usually spread via infected computer programs. It requires a human to activate, usually by running the infected program. Like biological viruses, computer viruses can self-replicate, infecting other files and applications on your computer. Viruses can even “mutate,” making slight changes in themselves to try to avoid detection. Before the advent of ubiquitous

networking, bad guys counted on people sharing these infected files on portable storage media (like floppy disks or thumb drives). Today these infected files are usually transmitted via email attachments or infected file downloads.

Worm: A *worm* is a special kind of virus that can spread autonomously to other computers over the network. That is, it doesn't require a human to activate it in order to propagate itself. This makes worms much more dangerous. Worms replicate by exploiting bugs in network services that computers use to talk to one another or sometimes just emailing themselves as file attachments to people in your address book. Once it starts to propagate, it can infect several computers very quickly—particularly in companies that have many computers running the exact same versions of the same software and therefore have the exact same vulnerabilities.

Trojan: A *Trojan* is malware disguised or hidden inside “legitimate” software. The name comes, of course, from the classic tale of the Trojan horse that the Greeks used to sack the city of Troy. The Greeks hid a select group of troops inside a large, hollow wooden horse statue (Figure 3-4). They left the horse at the gates of the city as a trophy and then sailed away in apparent defeat. The people of Troy brought the horse into the city gates, and when night fell, the troops came out of the statue and opened the gates from the inside. The Greek army, which had returned under cover of night, was then able to enter the city and take it.

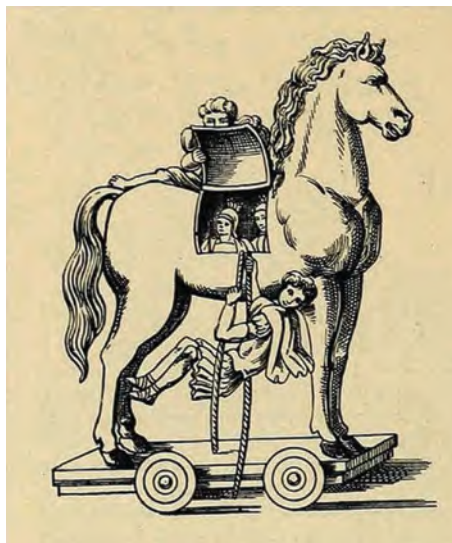


Figure 3-4. Classic image of the famed Trojan horse⁸

⁸Image source: *Histoire des jouets* by Henry René d'Allemagne (1902).

A Trojan application or document works much the same way. You're presented with what appears to be a legitimate application or document, but the malware is hidden inside it. When you launch the app or open the document, the malware program runs and infects your computer. Unlike viruses, trojans do not self-replicate.

Ransomware: With the rise of digital currencies like Bitcoin, we've seen an explosion in a specific type of malware called *ransomware*. Crooks infect your machine with software that effectively steals your data and holds it for ransom. The malware surreptitiously encrypts your hard drives, making the data completely unreadable—but also completely recoverable with a simple decryption key. It would be like crooks sneaking into your house, putting all your valuables in a vault on your living room floor, and then leaving you a note that says, "If you want the combination, you must deposit \$10,000 in my Swiss bank account." You technically still have all of your stuff...you just can't use it. Clever, eh? If you pay the fee, they give you the keys to decrypt and recover your data.⁹

You might be thinking to yourself: can I really trust them to give me the decryption key when I pay? Turns out, even crooks have reputations to protect. It's in their best interest to give you your files back. If they don't, word will get around and future victims won't pay up. This particular type of malware has become so profitable and so popular that criminal cyber gangs actually rent out ransomware tools to less technically savvy crooks ("ransomware as a service"), providing tech support to them and even to the victims.

Scareware: Sometimes the bad guys take the direct approach to getting your money. This type of malware might surreptitiously do something bad to your computer and then offer to fix it (for a fee). Sometimes this type of malware disguises itself as a free antivirus scanner or something, and in reality this software is *causing* the problem and then offering to undo the damage. In other cases, the malware watches your online habits, waiting for you to do something potentially embarrassing, such as visiting porn sites or illegal gambling sites. At this point they pop up some sort of fake law enforcement warning, threatening to arrest you unless you pay a fine.

⁹I'll talk in Chapter 6 about how you can encrypt your hard drive to prevent someone from accessing your files if they were to steal your laptop or hard drive. However, encrypting your hard drive will not prevent ransomware... there's nothing preventing a file from being encrypted twice!

It's worth noting that a very popular email scam involves bad guys claiming that they have infected your computer and recorded you doing naughty things and then offering to delete this evidence if you pay them off. Sometimes they will even use personal information gleaned from online data breaches, such as old passwords, to try to convince you that they really have hacked your computer. They're lying. Just delete the email.

Spyware: This is malware that is designed to look for sensitive information on your computer and then relay what it learns to the bad guys. This might include things like account passwords, contact lists, or personal information that would allow the watcher to impersonate you (identity theft) or hijack your computer or online accounts. A popular type of spyware that records everything you type on your keyboard, called a keylogger, looks for passwords, credit card numbers, cryptocurrency wallet IDs, and other sensitive info. Public computers, like those at libraries, cybercafes, and hotel business centers, are prime targets of keyloggers.

Potentially unwanted program (PUP): This is probably the most innocuous form of malware, though it can still be quite annoying and frustrating. This sort of malware commonly accompanies “free” software you download from the Web—you download the free app, but one or more PUPs come along for the ride. The original software vendor makes money from the third-party vendors for installing their unwanted crap on your computer. Some apps will tell you about the “bonus” software, if you dig deep enough into the installer options, but they don't make it easy to find. Assuming you find the installer configuration that shows you the extra software, you can usually deselect the additional, unwanted junk.

A more insidious type of PUP is called *adware*. Once installed, this malware will pop up advertisements in some form or another. For every ad shown or clicked, a referral is paid, which is how they make their money. Sometimes adware will collect information from your computer, as well, to be sold to marketers.

Bot: A bot (short for “robot”) is a piece of software that automates something that a human would normally do. Bots are not always bad. For example, bots are used by search engines like Google to “crawl the Web” looking for new and interesting websites to provide in their search results. (These particular bots are also called spiders or web crawlers.) Other bots might be used for slightly less benevolent things like beating real humans at online games, registering for online contests, or creating bogus email accounts from which to send junk email (or *spam*).

That's why many websites force you to look at a seriously distorted picture of some letters and numbers and then ask you to enter what you see. (Those annoying tests are called CAPTCHAs.¹⁰ See Figure 3-5.) Others ask you to identify elements of a picture on a grid ("click all the squares containing buses").



Figure 3-5. Example of a web CAPTCHA form

In both cases, they're trying to prevent bots from automatically doing whatever it is that you're trying to do. They specifically create problems that they believe are easy for humans to solve but hard for computer programs to figure out.

However, in the context of malware, bots can be used to do things that you would *not* normally do—like send emails to everyone you know advertising pills for male genital enlargement. Some bad guys actually try to build up large networks of infected computers to form a *botnet*. A botnet is essentially an army of remote-controlled computers, all pretending to be the owner of the computer but actually working for someone else. And remember that computers today aren't just desktops and laptops—when it comes to bots, any Internet-connected computerized device will do. It's actually more common today for botnets to be composed of IoT devices. Because of this, it's quite likely you'll never know that your devices have been conscripted into a botnet because they will continue to perform their normal functions too.

One common use for botnets is to simultaneously slam some specific website with requests in an attempt to bring their servers down. This is called a *distributed denial of service*, or DDoS, attack. They do this because either they don't like the owner of the website or maybe they're trying to extort protection money from them.

¹⁰ An acronym for Completely Automated Public Turing test to tell Computers and Humans Apart. A Turing test, named for famed mathematician and computer scientist Alan Turing, is a test that attempts to verify that you are communicating with a real human and not a computer.

Cryptomining: With the meteoric rise of “cryptocurrencies” like Bitcoin, there’s been a sort of digital gold rush to “mine” it. Bitcoins are mined by performing some very hard, very taxing computer operations. And as time goes on, these digital currencies are designed to be harder and harder to mine in order to control the supply. It didn’t take long for the bad guys to turn their botnets into massive, networked mining rigs. Thankfully, the only real impact on you and your devices is a higher electric bill. Cranking up your computer’s brain to work on these complex operations requires significant power.

Rootkit: This is a particularly nasty bit of malware that often attacks the operating system. It’s specifically designed to hide from you and from malware detection software like antivirus programs. Sometimes the rootkit actually disables or breaks your security software, preventing it from working. To make matters worse, rootkits can find ways to hide copies of their code so that even if you do find the running copy and remove it, it just replaces itself and runs again.

HACKERS

I want to take a minute to examine a term that we throw around a little too loosely: *hacker*. Many people equate the term hacker with criminal. While it’s true that cybercriminals are often hackers, hacking and hackers are not always bad. Think of a hacker as a tinkerer. Hackers are insanely curious and industrious people who like to deeply understand how something works and then use that knowledge to make it do something else. Almost every inventor in history can be thought of as a hacker. TV characters like The Professor on *Gilligan’s Island* or MacGyver are basically hackers—figuring out how to take every day common things and making them do something extraordinary. When I was a kid, I took apart many of my toys and put them back together in funky ways. That’s a form of hacking. When people talk about “life hacks,” they’re talking about inventive ways to do useful things.

Hackers actually have a term they use for people who do illegal hacking—they refer to them as *black hat* hackers. The term comes from old cowboy movies where the bad guys stereotypically wear black clothes including a black hat. Similarly, hackers who hack for good are called *white hat* hackers. How does one hack for good, you might ask? Because all software has bugs and it’s hard to “grade your own homework” objectively, many companies will hire professional cybersecurity experts to try to hack their products—that is, to try to

find the vulnerabilities before the bad guys do. The companies will pay a “bug bounty” to the hackers who find bugs, with the value of the bounty being based on the severity of the vulnerability (among other factors).

Furthermore, it’s not uncommon for black hat hackers to be converted to white hat hackers as part of their rehabilitation. You can argue that Frank Abagnale (the subject of the wonderful movie *Catch Me If You Can*) was a sort of black hat hacker who used his cleverness to commit check fraud and ended up working for the FBI after he was caught to help banks improve their antifraud techniques. Kevin Mitnick was a cybercriminal who went on to write several best-selling books and found a cybersecurity consulting firm after he was caught and did five years in prison.

Hardware Bugs

In recent years, a new class of threat has become popular: hardware hacking. Instead of finding bugs in the operating system, web browser, or other applications, hackers have managed to cleverly exploit vulnerabilities in the computer’s processing chips, called the *central processing unit* (CPU).

Two bugs that garnered a lot of media attention several years ago were dubbed Spectre and Meltdown, but there have been other variants in recent years. In an effort to eke every last ounce of processing power out of our computer chips, CPU manufacturers AMD and Intel devised techniques to optimize certain computations. Specifically, they designed their chips to precalculate various possible outcomes ahead of time and, when a particular course is chosen, have the answer ready and waiting. This involved prefetching all the necessary data to make these decisions. It turns out that this mechanism wasn’t properly locked down and a rogue application could actually peek at this data without proper permission, and so this information leaked. And if that information contained private data, it could be harvested and used for nefarious purposes.

If that sounds complicated, that’s because it is. These vulnerabilities and the hacks required to exploit them were devilishly crafty. But because AMD and Intel make the brains for just about every computer on the planet, it meant that just about everyone was vulnerable—Mac, PC, and even Linux (which is the dominant operating system for most big-time computer servers on the Internet). In this case, it was actually possible to patch the bugs with low-level software changes (usually at the expense of those clever

computer efficiency gains). But the day will surely come when a software fix won't cut it, and in that case, your only choice will be to throw your computer out and get a new one. Computer chips take many months to design, manufacture, and integrate into computer systems, so if this type of bug were to be found, it could be a long time before computers with fixed CPU chips would be available for purchase. The silver lining for you, though, is that most of these types of attacks are only valuable on big-time cloud computers that serve multiple accounts—not home computers.

Cryptic Codes and Confidential Communications

Okay, folks... everything we've learned up to this point in the chapter has been necessary, but kind of mundane. I did my best to make it interesting for you, but at the end of the day, it's just a bunch of techno terms. The time has come to venture into new frontiers! This is where we turn magic into science, pulling back the curtain to reveal the man working the levers!¹¹

The rest of this chapter will be devoted to exploring two important and truly fascinating technical topics: how the Internet works and how encryption works. These are incredibly complex topics, but I'm only going to focus on a few crucial concepts. We have tons of data that we need to protect. That data flows over the Internet and we protect it with encryption—both in motion and at rest. These concepts are essential for understanding private communications, passwords, VPNs, safe web browsing, and so much more. Never fear—I've got some simple analogies that will make it all crystal clear.

All right—let's do this!

How the Internet Works

The Internet is a fascinating piece of technology (actually many different technologies, playing together more or less nicely). Entire books are devoted to explaining this stuff, but I want to focus here on how the data moves—because it's important to understand these concepts before talking about the things we do to protect the data as it moves.

¹¹ That's a *Wizard of Oz* reference. We're going to explicitly pay attention to the man behind the curtain.

When you surf the Web,¹² send an email, upload a video to YouTube, or stream a movie on Netflix, you are transferring data between your computer and some other entity on the Internet. This entity is often a big server owned by the likes of Amazon, Google, or Netflix but sometimes another computer like yours (e.g., if you’re doing a Zoom meeting at work or a FaceTime session with a friend).

Data can travel in two directions, and we like to label these directions so we can talk about it. When data goes toward the Internet, we call that direction *up*; when data moves toward your computer, we call that direction *down*. So, when you are pushing a video file to YouTube, we call that *uploading*; when you stream a song from Spotify to your computer or smartphone, you are *downloading*. If you think of the Internet as “the cloud,” then you can remember this by thinking that clouds are up.

But how does that really work? As I said earlier, data is made up of bits and bytes. If you make a perfect copy of the bits, then you make a perfect copy of the data. To get data from one computer to another computer, you just have to find some way to reproduce the same bits, in the same order, on the other person’s computer. Let’s say you want to send someone a Microsoft Word file. You don’t physically send your bits to someone else—you send *copies* of the bits. When you’re done, the file exists on both your computer and on their computer, and the two files are 100 percent identical.

So, how do we do that exactly? Again, it would take an entire book to tell you the real deal here, so we’re going to simplify things considerably.

The Internet works a lot like the US Postal Service’s first-class mail system. The USPS is in charge of getting letters from point A to point B, and it does so using a vast array of methods and technologies—most of which you never see or know about. All you know is that if you put your letter in the mailbox, with the recipient’s address on it and a stamp, they’ll take care of the rest! If you want that other person to send something back, then you need to also include a valid return address. As far as you know, it’s just magic—it somehow leaves your mailbox and ends up in the other person’s mailbox, right?

Well, let’s take a look at what really happens behind the scenes after you put that letter in the mailbox. Every so often, usually once a day, a mail carrier comes by to check your mailbox. If the mail carrier finds a letter in the mailbox, they take it and throw it in their

¹² The “World Wide Web” is a subset of the broader Internet—but it’s the part we’re most familiar with.

pile of outgoing mail. At the end of the day, the mail carrier takes the pile of outgoing mail to a sorting facility that looks at all the “to” addresses and starts separating the mail into bins based on destination. Local mail may go right back out the next day with the same mail carrier, whereas mail to another state will likely be put on a truck or plane and sent to another post office for local delivery at the far end. They may split that pile up and send it in different ways, even to the same destination. How they split this up might depend on how full the truck or plane is, on whether a particular truck or plane is out of commission, or even on the fluctuating costs of fuel. The route taken and the method of transport will also vary based on what type of service the user paid for (bulk mail, first-class mail, or express delivery). There may be multiple stops along the way and multiple methods of transport. Again, as the sender, you don’t know or care how it gets there—only that it does get there and in a reasonable amount of time.

Internet routing works very much the same way. Every computer on the Internet has a unique address. It’s called an *Internet Protocol address*, or IP address for short. An IP address is set of four numbers separated by periods like 74.125.228.46 or 72.21.211.176. You’ve run across these numbers if you’ve ever gone poking around in your network settings on your computer or smart devices.

FUN FACT

Each one of those four numbers in an IP address ranges from 0 to 255. So, if you add up all the possibilities, that’s more than four billion possible unique addresses... and, believe it or not, we’re already running out! There’s an expanded addressing scheme that’s been around for years but is only slowly being adopted called *IPv6* (which stands for Internet Protocol version 6, which will replace the current *IPv4*). IPv6 has a truly stupefying number of unique addresses:

340,282,366,920,938,463,463,374,607,431,768,211,456

Yeah, that’s one number. It’s been said that every single atom on the surface of planet Earth could have its own IPv6 address...and there would still be enough left over for 100 more Earths!¹³

We’ll revisit these topics in Chapter 7.

¹³ <https://www.edn.com/ipv6-how-many-ip-addresses-can-dance-on-the-head-of-a-pin/>

To make those numbers easier for humans to remember, we give them aliases like “google.com” or “amazon.com”—we call those aliases *domain names*. When your web browser or email application is told to use one of these aliases, your computer invokes a service called the *Domain Name Service* (DNS) to convert the alias to an IP address. DNS is like the phonebook for the Internet: you use the name to look up the number. But with domains, the names are guaranteed to be globally unique. And because DNS is global, lookups are done in stages to keep the lookup tables at a manageable size. Sorta like looking up the country, then the state, and finally the city.

So, when you tell your computer to send some data across the Internet, it packages that data up, slaps on the destination IP address, and puts the data in a sort of digital mailbox, waiting to be picked up. Your return IP address is automatically added so that the computer at the other end can send you a reply. Once the data is picked up for delivery, it’s dispatched through a series of special computers called *routers* that figure out how to get your info from here to there. The exact route it takes may be different each time, based on how busy the routers are, the costs charged by the various carriers, and any special handling that your computer may have requested (more on that in a minute).

Now, as fancy as the Internet is, it doesn’t have the notion of shipping large things in a single package—like shipping a big box full of stuff at the post office. Basically, everything is letter-sized. Why is that? Well, when you’re dealing with bits and bytes, you can deconstruct anything into small pieces and reconstruct them perfectly at the other end! (It’s sorta like that scene in *Willy Wonka* where Mike Teavee is transported across the room in chunks.) Since the individual pieces may take different routes, they may actually arrive out of order at the far end. So, how do we fix that problem? As you chop up the big thing into little pieces, you assign each piece a number, sequentially. At the other end, they can use the numbers to put everything in the proper order when reassembling the data.

To think about this, let’s go back to our analogy of the post office. Let’s say you want to ship a copy of the *Oxford Dictionary* to someone across the country but you can ship it only one page at a time. How would you do that? Well, first you’d have to copy all the pages and stuff each one into its own envelope. Every one of those envelopes would need to have the recipient’s address on it. The pages are already numbered, so if they arrive out of order, your friend will be able to put them back in the proper order.

However, now you realize that your mailbox isn't actually big enough to hold all of these letters at once. Now what? Well, you just have to do it in batches, maybe 100 letters at a time. Once the mail carrier empties your mailbox, you can put in 100 more. The person at the other end opens all the envelopes and reassembles them in order (using the page numbers). When the last letter arrives, they will have the complete book!

Now, the US mail service isn't perfect... sometimes letters get lost. Turns out that this happens on the Internet too. So, how do you handle that? Well, you ask the person at the other end to send a letter back every so often telling you what they've received so far. If they find that some pages are missing, they can ask you to resend them.

That—in a nutshell—is how data is sent across the Internet. But instead of taking days or weeks, it takes fractions of a second! Your computer breaks the file or email or whatever into small chunks called *packets*. Each packet is labeled with a “from” IP address and a “to” IP address. Those packets are then numbered so that the computer on the receiving end will (a) know in what order to reassemble them and (b) know if any packets are missing and need to be resent. See, it's not that hard!

Why do you need to know all of that? I'll explain in later chapters. We'll revisit this analogy when we talk about privacy, authentication, and encryption.

How Encryption Works

Now that we've reviewed the basics of computers and we've learned the fundamental operation of the Internet, it's time to turn to the *really* cool stuff: encryption! Okay, I will stipulate here and now that normal people may not share my deep-seated fascination for the mechanics of cryptography. But I'm going to do my best to win you over. One of the important takeaways from this book is that you can trust the math. The media and pop culture like to make it look easy to hack into secure systems, cracking passwords and breaking encryption with ease. In reality, modern computer security algorithms are extremely robust and nearly impossible to crack, if implemented properly (which turns out to be a crucial “if”). Despite the billions of dollars spent on supercomputers at places like the NSA and GCHQ,¹⁴ the tools that cryptographers have created hold up surprisingly (and thankfully) well.

¹⁴ Britain's version of the NSA, which is called Government Communications Headquarters.

For the rest of this chapter, we’re going to discuss the processes and tools that allow us to shop and bank online securely, as well as communicate privately and keep our computer data from being read by others, and much more. Having a basic understanding of crypto¹⁵ will give you a huge leg up later in the book (and in life) when you’re evaluating basically anything involving securing your devices and your data. Plus, it’ll make you sound really smart at your next cocktail party!

Encryption

Cybersecurity experts break the concept of security into three parts: confidentiality, integrity, and availability. This is referred to as the *CIA Triad*. The first part, confidentiality, refers to keeping data private or secret. Integrity is concerned with making sure that data can’t be altered or deleted—that what was sent was exactly what was received or that what was saved was exactly what was written. And availability refers to the data being accessible. If your computer is broken or stolen or unable to process requests, then it doesn’t really matter if the data on it is kept private and intact. In the rest of this section, we’re going to focus on the first two: confidentiality and integrity. It turns out that both of these can be solved using *encryption*.

Let’s start by considering the classic case of a personal diary. You would like to be able to write some thoughts down and save them in such a way that only you will ever be able to read them—that is, you want them to be confidential. You could just hide this journal somewhere and hope no one finds it. This is a form of *security by obscurity*, something that is secure only because its existence isn’t known. It’s like hiding a key under your doormat. In the realm of cryptography, this is never sufficient, at least not as the primary means of security. No, what you really want is some sort of mechanism by which we can render the words completely incomprehensible to a third party, even if they steal the journal—and yet somehow be fully readable by you.

¹⁵ By the way, cybersecurity professionals hate that Bitcoin bros have co-opted the term “crypto” to refer to cryptocurrency. Crypto is short for cryptography—don’t let anyone tell you otherwise.

SECURITY BY OBSCURITY FAIL

Security by obscurity is used way more often in the real world than it should be. For anything important, it should simply never be used. Here's a real-life example of how the implementation of security is just as important as the underlying technical aspects. A tech startup company debuted a new Wi-Fi-controlled "smart" light bulb. They designed the bulbs so that once you set up your first bulb (where you must give it your Wi-Fi credentials so it can connect to your home network), any added bulbs would talk to the "master" light bulb and automatically connect to your Wi-Fi network. How convenient! These amazing little devices had a special private "mesh" network that allowed them to talk to one another. Since wireless communications are broadcast over the airwaves, hackers can easily eavesdrop on the signal. Well, the engineers at this company understood this, so they used "military-grade" encryption to prevent eavesdroppers from tapping into these communications. Unfortunately, the encryption key they used—the lynchpin for any successful encryption—was a fixed, hard-coded value! That is, *there was only one key for all of their products*. But they hid this key away inside the memory on their light bulbs...who would ever figure out how to extract it? Hackers, of course. They were able to take one of these light bulbs, hook up some wires to the computer chip inside, and pull out the universal encryption key. All a hacker needs to do is come close enough to your house to "hear" the light bulbs talking to each other, and they can decrypt the transmissions and see your household Wi-Fi login ID and password. The company counted on no one bothering to poke around in their devices to find the encryption key—security by obscurity. Once this key is made public (i.e., no longer obscure), the jig is up for all customers who bought these bulbs. The company updated its software with a fix, but it still requires the customers to get around to updating their light bulbs to remove the vulnerability...which is not very likely.

As you may have guessed, what we need here is encryption. We need to somehow transform our words into something that appears to be pure gibberish to anyone else. In cryptography, the original text is referred to as the *plain text*, and the garbled output is called the *cipher text*. We call it that because to convert the plain text to cipher text, we run the plain text through a *cipher*. A cipher is a secret code or algorithm that maps letters in the plain text to letters, numbers, or symbols in the cipher text. The simplest types of these ciphers are referred to as *substitution ciphers* because you substitute each letter of the regular alphabet with one character from a cipher "alphabet."

This is the classic “secret decoder ring” from bygone years. If you’re not familiar with the secret decoder ring concept, it’s basically two wheels, side by side, connected together on a common hub. Each wheel has a sequence inscribed on its edge so that if you rotate the wheels, you can align the letters or numbers in multiple ways. When the letter ordering is the same on both wheels, we call this a *rotational cipher*. (Again...don’t worry about remembering all this terminology... there will be no quiz on this. It’s just informational.)

Let’s say that each wheel just lists the characters from the English alphabet, in the proper order, so that if you align the letter *A* on one wheel with the letter *A* on the other wheel, then they are in perfect alignment all the way around...*B* on the first wheel maps to *B* on the second wheel, all the way to *Z* mapping to *Z*. That’s a crappy cipher, so let’s give the wheel a spin... let’s say now that *A* maps to *N*. That would mean that *B* would map to *O*, *C* would map to *P*, and so on. Because the wheels are round, when you get to *Z*, the next letter is *A*, and it continues. This is actually a special rotational cipher referred to as *ROT13*, which is short for “rotate 13 places”—because the letter *N* is 13 places away from the letter *A* in the alphabet. Since the English alphabet contains 26 characters, if you run ROT13 encoding on something *twice*, you end up back where you started (because $13 + 13 = 26$).

Figure 3-6 is an example of this. You can see the entire alphabet mapping and also see how the word *Hello* would be encoded using this scheme.

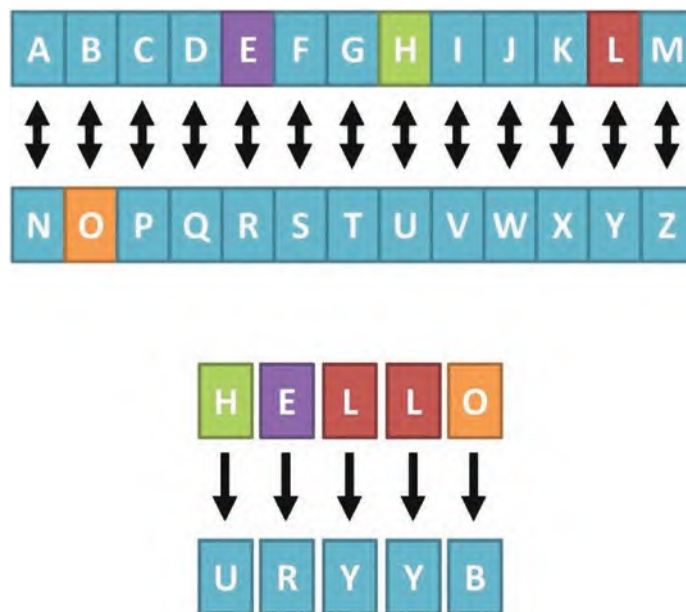


Figure 3-6. Alphabet character mappings for the ROT13 rotational cipher

My favorite pop culture example of the secret decoder ring comes from the classic movie *A Christmas Story*. The primary character, Ralphie Parker, has just received his Little Orphan Annie secret decoder pin in the mail, and now he's part of the Little Orphan Annie "Secret Circle." At the end of each radio broadcast of the classic adventure series, announcer Pierre Andre would read off a secret, ciphered message that only kids with the decoder could interpret. In this case, the cipher mapped letters to numbers, so one wheel had the alphabet while the other wheel had numbers. (See Figure 3-7.¹⁶)



Figure 3-7. *Little Orphan Annie decoder pin from A Christmas Story*

To decode the message, you needed to know how to align the two wheels—and Pierre informed his listeners to set the dials to B-2. In other words, turn the wheels on the pin so that the letter *B* mapped to the number 2. This is the simplest conversion possible because *B* is the second letter of the alphabet. Therefore, *A* is 1 and *Z* is 26. Ralphie's first message as part of the Secret Circle was as follows:¹⁷

2-5-19-21-18-5-20-15-4-18-9-14-11-25-15-21-18-15-22-1-12-20-9-14-5

¹⁶ This is my personal decoder pin, obtained from the A Christmas Story House and Museum in Cleveland, Ohio. If you're a fan of the movie, it's a must-see (<https://www.achristmasstoryhouse.com>)!

¹⁷ As you can see in the figure, the actual decoder pin wasn't a true rotational cipher. But I've simplified it here for the purposes of our example.

Using his decoder pin, Ralphie painstakingly decoded the message. We know that 2 maps to *B*, so the first letter is *B*. The fifth letter of the alphabet is *E*, so that's the second letter of the message. The 19th letter is *S*, and so on, until we ultimately get this:

B-E-S-U-R-E-T-O-D-R-I-N-K-Y-O-U-R-O-V-A-L-T-I-N-E

At this point, Ralphie slowly reads the message, figuring out where the word boundaries are... "Be sure... to drink... your... Ovaltine. Ovaltine? A crummy commercial?!?"

Cryptanalysis

Now let's flip this whole process on its head... let's play the bad guy now! You have intercepted this secret message and you want to know what it says. How would you go about trying to break the cipher? The process of trying to break a cipher is called *cryptanalysis*. Modern cryptography is performed by computers, and these ciphers are beyond the capability of a mere mortal to break unassisted. But in the olden days, ciphers were performed by hand and broken by hand.

So, let's begin our cryptanalysis by taking a close look at the cipher text. First, we need to make some assumptions. We will assume that the plain text is in English. We will also assume that each symbol in the cipher text maps to a single letter in the English alphabet. Those assumptions may be wrong, but one of the most powerful tools in a code breaker's arsenal is to know as much about the input as possible. Having prior knowledge, even if it's just a lucky guess, can significantly reduce the effort required to decrypt a piece of cipher text.

Next, we need to study the cipher text and look for patterns or clues. We see numbers ranging from 1 to 25. Given that the English language has 26 characters, we will assume that this cipher is a simple substitution cipher that maps letters (*A* to *Z*) to numbers (1 to 26).

Here's where things get interesting. Since we've assumed that the plain text is in English, then we can use our knowledge of the English language to help us crack the cipher. It turns out that the most used character in the English language (by a healthy margin) is the letter *E*. How do we know that? Well, most people would have no reason to know this, but it's a code breaker's job to know these sorts of statistics. So, if you were to take a rather large block of cipher text that came from an English plain text, you could be pretty sure that the most common symbol would map to the letter *E*. The next three most

common letters in the English language, in order, are *T*, *A*, and *O*. Counting the use of symbols in cipher text and trying to map them to common letters are called *frequency analysis*—using the frequency of the symbol in the cipher text (i.e., how often that symbol appears, relative to other symbols) to guess the associated English character in the plain text.

Our cipher text is pretty short here, but let's give frequency analysis a shot. If you count the number of times each number is used here, you will see that three numbers are used the most: 5, 15, and 18. Each one of these numbers appears three times. So, let's assume that one of these symbols maps to the letter *E*. We will try each one to see whether it works. Let's first guess that the number 15 maps to *E*. Now we're going to make another assumption, just to see if we can get lucky: let's hope that whoever created this cipher wasn't trying very hard and they just mapped the letters to numbers in order. So, if $E=15$, then $F=16$, $G=17$, and so on. Using that mapping, the code breaker substitutes all the letters and gets the following guess at the original plain text:

R-U-I-K-H-U-J-E-T-H-Y-D-A-O-E-K-H-E-L-Q-B-J-Y-D-U

Hmm. That doesn't look right. So, at least one of our assumptions was wrong. But since we're lazy, let's stick with the assumptions we have and just try another mapping. After all, there were three symbols that all showed up three times in our cipher text, so if 15 wasn't right, maybe 5 or 18 will do the trick.

If we try $E=5$, keeping our other assumptions, we get the following:

B-E-S-U-R-E-T-O-D-R-I-N-K-Y-O-U-R-O-V-A-L-T-I-N-E

Bingo! We've just decrypted the message! Woo-hoo!

If the cipher text was helpful enough to contain spaces, marking the boundaries of words, we could have used other statistics to help us decipher the message. The most common single-letter words in the English language are *I* and *a*. The most common three-letter word is *the*. The most common first letter of a word in English is the letter *S*. So, just knowing where the word boundaries are would have given us a lot more information that we could exploit to guess the mapping and break the code.

Obviously, cryptanalysis in the modern world is a lot more complicated—today we use computers and much more complicated algorithms to encrypt our data. But the previous exercise gives a glimpse into how an attacker might try to break a code. One of

the most famous acts of code breaking occurred during World War II where Englishman Alan Turing, with his colleagues at Bletchley Park, cracked the Enigma machine ciphers (Figure 3-8) used by Nazi Germany (improving on techniques originally pioneered by the Polish). However, code makers and code breakers have played significant roles throughout history, dating back to at least 1500BC in Mesopotamia.¹⁸



Figure 3-8. German WWII Enigma machine (photo by Karsten Sperling)

Modern Cryptography

Modern ciphers revolve around the notion of a secret key. You take your plain text, plus some sort of text key (much like a password), and run it through an *encryption algorithm*.¹⁹ The resulting output looks like complete gibberish. Unlike our simple substitution cipher previously, the output may not have a direct character-for-character mapping—it might well not even be representable as English characters at all. But, if you take the same secret key and apply the algorithm in reverse (the *decryption algorithm*),

¹⁸ Turing's work has been wonderfully captured in the Academy Award-winning movie *The Imitation Game*. And if you find the history of cryptanalysis as fascinating as I do, I highly recommend you read *The Code Book* by Simon Singh.

¹⁹ An algorithm is just a fancy name for a process or technique—a set of steps to complete a specific task.

you get the original plain text back. This sort of cipher is called a *symmetric cipher* because the same key is used to both encrypt and decrypt (see Figure 3-9).



Figure 3-9. *Symmetric encryption flow diagram*

It's crucial to note here that the encryption and decryption algorithms themselves are public and well known. That is, the process for mangling and unmangling (demangling?) the text is *not secret*. In the past, people have argued that we would be more secure if the algorithms themselves were secret. That sort of sounds intuitively correct—like a magician not telling how his tricks are done. But that's exactly the point—it's not really magic if there's a trick to it. If I could break your encryption just by knowing how you did it, then the entire process is dependent on that secret process never being leaked or discovered—not just for one person but for everyone who ever used that algorithm—and therefore, every message or file ever encoded with that algorithm. In today's world, that's just not good enough. Any encryption scheme worth using must be secure even if the detailed mechanics of that scheme are well known. This also allows the algorithm to be exhaustively tested and scrutinized by crypto experts.

If you're just using a cipher to encrypt personal data, like your diary, the symmetric cipher works quite well. You choose a password, commit it to memory, and use it as the secret key to encrypt the text of your diary. As long as you picked a strong password and a decent encryption algorithm, that diary is completely unreadable by anyone but you (i.e., the only person who knows the secret key). But again, you have to notice the caveat I slipped in there... you must choose a strong password for this to work. We'll discuss this in-depth in Chapter 5, but for now just realize that computers are so powerful that they can guess millions or even billions of passwords per second in an attempt to crack your diary open—so choosing your granddaughter's name or favorite football team is not going to cut it.

You can think of symmetric encryption as a treasure chest with a strong lock—you have the key, and only you can open the lock. It doesn't matter if people have the trunk in their possession—unless they have the key, they can't access the diary kept inside. It

shouldn't even matter if they know how the locking mechanism was made. For this analogy to compare well to modern cryptography, we must assert that the trunk would be completely impregnable, and the lock would be effectively impossible to pick. The crucial element then is the key for the lock. As long as you have the key in your possession and there are no other copies of the key, then only you can open the lock, and therefore only you can access the contents.

Having the ability to lock up your diary is a good thing, but there are other situations in the real world that require security. In cryptographic parlance, we've covered the case of *data at rest*, but what about *data in motion*? That is, what about communications? In this new scenario, we've crucially increased the number of people who need to be able to access the information from one to more than one.²⁰ We've also added the requirement that we need to be able to send this data across some distance, in the hands of third parties who we can't necessarily trust. To use a symmetric cipher for this purpose, you must now share your secret key with the intended recipient. But how will you do that securely? You can't just send it to them—someone might intercept it along the way. You might tell them over the phone, but what if your phone or their phone is being tapped? You would have to meet them in person and whisper it in their ear. And yet, that's not always practical or even possible.

Thankfully, some very clever researchers devised a radical new approach to encryption in the mid-1970s that revolutionized secure communications and encryption in general. They essentially invented a lock with two keys: a public key that is used to close the lock and a private key that opens the lock. This is referred to as *asymmetric encryption* because different keys are used to encrypt and decrypt. In this scheme, copies of the public key are given away freely and indiscriminately, while only the owner holds the private key. Anyone wanting to send a message will use the recipient's public key to lock the message, and the recipient will use their private key to unlock it. What a brilliant and elegant solution! With this technique, it is now possible for two people to communicate securely without ever having to physically exchange a single, shared key. They can exchange private messages at a distance without ever having to meet in person first.

You can think of it like this. Let's say Alice wants to send some highly confidential documents to a colleague across the country, Bob.²¹ While Alice could get on a plane

²⁰ Benjamin Franklin famously said: three may keep a secret, if two of them are dead.

²¹ Alice and Bob are well known in the cryptographic world. These are the names used when describing communication scenarios in lieu of saying "Party A" and "Party B."

and hand them off in person to Bob, that's way too expensive and inconvenient—she wants to just ship them via US mail. Alice has a nice little box that she can secure with a lock, but she can't just send Bob a copy of the key in the mail—after all, anyone along the way could make their own copy of that key. Being a smart woman, she knows that she doesn't have to rely on a symmetric locking mechanism—she can use an asymmetric method. To accomplish this, Alice tells Bob to send her an open padlock. She then takes Bob's padlock and fastens it on the box. She didn't need Bob's key to close it—anyone can close the lock simply by clicking it shut. However, only Bob can open the padlock because only he has the key. If Alice was thinking ahead, she could even include one of her own padlocks with the box when she ships it so that Bob could return the documents to her using the same technique.

So, how does all of this apply to you and your computer? As we discussed earlier in this chapter, whenever we send an email, watch a video on YouTube, shop at amazon.com, pay bills using our online bank account, or just surf the Web, we're sending data to and receiving data from the Internet. That data is chopped up into bite-size pieces called packets, and those packets make their way from your computer to some other computer. Along the way, those packets go through potentially dozens of other computers, routers, switches, and servers. The key thing to remember here is that those digital missives are a lot more like postcards than letters. That is, any person (or computer) along the way who takes the time to look at them can see whatever they contain.

For some of what we do on the Internet, that may be acceptable. But obviously there are many situations—like banking and shopping—that will require a secure, private connection. The communication protocol used by the Internet is Hypertext Transfer Protocol (HTTP).²² You've seen this many times when looking at web addresses like <http://yahoo.com>. If you are observant, you may have noticed that often times it's not http but https. That extra *S* stands for “secure.” When your web browser is communicating via HTTPS, you should see some sort of indicator like a padlock icon that indicates that your communications with that website are secure. That means that no matter how all your packets are bouncing around the Internet, only the computer at the far end can actually decipher them.²³

²² I don't know why it's not HyperText or Hyper Text. And since it's neither of those things, you'd think the abbreviation would be HTP not HTTP. But that's the way it is.

²³ Note that HTTPS, by itself, does not say anything meaningful about the *identity* of the service you're communicating with—only that the communications are private.

Authentication and Message Integrity

Hurray! We have asymmetric encryption! Problem solved, right? Not quite. It's not sufficient just to prevent someone from seeing the contents of your communication. Let's go back to our document shipping analogy with Alice and Bob to see why. How did Alice know that she was actually shipping the documents to Bob? If I were a crafty spy, say Mallory, I could try to insert myself between Alice and Bob—pretending to each of them to be the other party. This is called a *man-in-the-middle attack*.²⁴

The crucial step here is to intercept communications between Alice and Bob. Let's say that Mallory infiltrates the US mail service so that she has access to all the correspondence between Alice and Bob. When Bob sends one of his open padlocks to Alice, Mallory intercepts the package and replaces Bob's open lock with her own open lock. She doesn't have Bob's key, but she also doesn't need it. When Alice sends the classified documents to Bob in the locked container, she has unwittingly locked it with Mallory's padlock, not Bob's. Mallory intercepts the package, opens the padlock using her key, and accesses the contents—thereby violating the confidentiality of the communication. If she wants to be really sneaky, she can simply copy the contents and relock the box with Bob's lock (which she saved). Bob receives the package, unlocks the padlock using his key, and wrongly assumes that the contents have not been viewed by anyone else.

As a man (or, in this case, woman) in the middle, Mallory can create all sorts of mischief. For example, not only could she copy the contents of the messages and packages, but she could also *change* them. That is, she could violate the integrity of the transaction. Let's say Bob's message to Alice is "please send me \$10,000 in cash." Since Mallory has intercepted this communication, she could alter the message to say \$20,000 instead. When Alice sends the \$20,000, Mallory can remove half the money and send the remaining \$10,000 to Bob. Bob then receives exactly what he asked for and would therefore suspect that nothing was amiss.

Cryptographic Hashing

So, how do we solve this problem? We now need to come up with some way for Alice to convince Bob, beyond a shadow of a doubt, that not only was she the only person who could have sent this package but also that the contents of the package have in no way

²⁴ Actually, there's a push now to refer to this as a "manipulator" in the middle, to make it gender neutral.

been altered. To solve this problem, we need to not only use asymmetric encryption, but we need to introduce a new tool called a *cryptographic hashing function*. (I know... it sounds super technical... just hang with me on this. This is the final step and it's a very important one.)

First of all, for simplicity, let's just talk about sending a document from Alice to Bob. Alice has a set of pages that she needs to send to Bob securely, with complete confidence that no one has altered or intercepted them along the way. What sort of tool would we need here?

Let's say there exists a document X-ray machine that can effectively squash multiple pages into one. It stacks up all the pages and shoots a magic ray through them all, capturing what is essentially a shadow of all the text on the pages, merged into a single composite "X-ray" image. We'll call this machine a *Dox-Ray machine*!

To see how this marvelous Dox-Ray machine works, let's use a simple example. Figure 3-10 shows six sentences of about the same length.

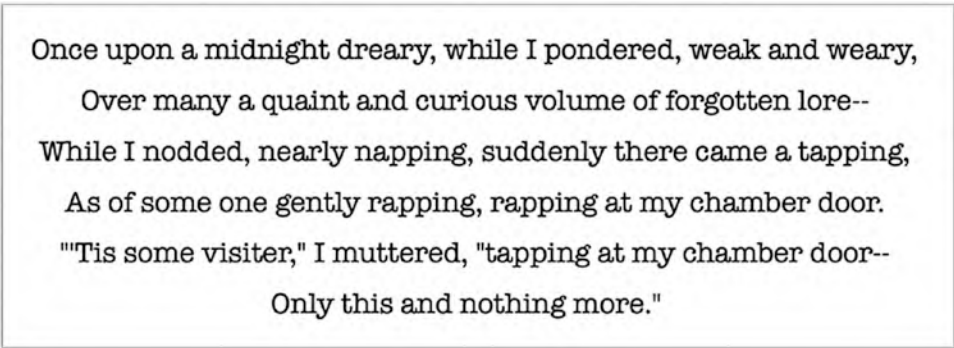


Figure 3-10. Five phrases

Now let's cut this up, line by line, and stack each sentence or phrase on top of each other. If we could see through them all, perhaps with a bright light underneath, it might look something like Figure 3-11.

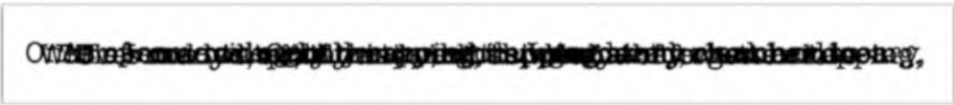


Figure 3-11. Five phrases stacked on top of one another

This is the Dox-Ray image of all six phrases: the merging of all the lines, one on top of the other.

This Dox-Ray image has some very interesting properties. First, it's completely unique and predictable, based on the input. The one and only way to get this *exact* Dox-Ray image is to use these exact same words, in the exact same order. If you changed, added, or deleted even a single character, the image would also change.

Second, there is no way for you to get the original six phrases back from this Dox-Ray image. This is a “lossy” conversion: information is lost in creating it. It's therefore a one-way conversion. Given the input (the six phrases), you can always reproduce the output (the Dox-Ray image); but given the output, you cannot retrieve the original input.

Finally, this process produces something small and a fixed size. If you imagine that we run this X-ray process on a set of pages of a book, the output will be the size of a single page, regardless of how many pages are in the original book. You're basically squashing the entire tome into a single sheet of paper.

So, our Dox-Ray machine can take a set of document pages and produce a unique image of all those pages—a single page that represents dozens or even hundreds of input pages.

Message Integrity

Are you with me so far? Here's where the rubber meets the road. We're going to take this new Dox-Ray technology, along with an improved locking mechanism, to solve our private communication problem once and for all!

So, let's give this Dox-Ray machine to Alice and Bob. With this nifty device, Alice could take an X-ray of her documents and include that image with the package. When Bob receives the package, he could use his own Dox-Ray machine to create an image of the documents he received. He can then compare his image with the one sent by Alice. If they're identical, then Bob can be assured that the document hasn't been altered. If Mallory attempted to alter the document in any way—removed a page, used Wite-Out correction fluid, replaced a page with different text, or tried to add a new page—the Dox-Ray machine would produce a different image. So, even if Mallory could intercept and inspect the package, she can't alter the document in any way without being detected.

This is essentially how a cryptographic hashing function works. You put in a bunch of text and out comes a short value. If you alter just one letter of that input text, the output value changes *completely*. It's also effectively impossible to find another set of words that

will end up with the same hashing result. Hash functions are sometimes called trap-door functions: easy to go one way and nearly impossible to go the other way, like falling through a trap door in the floor.

Let's test that theory, just to prove the point. Using a popular crypto hash function called SHA-256, here is the hash output using this entire 400+ page book as input:

```
4a939d318741a70f67af9e3fbb28d5f2ebeccc799c0ee6bf0de59628bbcc7178
```

Now here's the hash of this book after altering just a *single character*:

```
1fd4094a7780cdc18c54c339bc4011669656455e7a64a32b4769aafa6516e6b7
```

Do you see any similarities in those two numbers? Nope. They're completely and utterly different. So, this is even better than our Dox-Ray machine—one tiny change in the input creates a massive change to the output. And obviously, there's no possible way to reproduce the entire contents of this book from that short output value.

Asymmetric Locks

If I've managed to make you properly paranoid, you might realize that there's still a problem here. If Mallory can access the contents of the box, then she can also access the included Dox-Ray image. She could alter the documents, recreate the X-ray with the new documents, and include *that* image in the package. This is where the public key (asymmetric) crypto comes back into play. Basically, we're going to need a more sophisticated padlock.

Let's imagine a different sort of lock, one that doesn't exist in the real world—let's call it a *SuperLock*. This lock has two key slots: one to lock it and one to unlock it. The keys for this special lock always come in pairs. One is a public key, which is copied and given out to anyone who wants to have one; the other is a private key, which is never copied and held only by the owner. Either key can be used to close the lock, but once locked, only the other matching key can open it. The same key cannot do both things—one key locks it and the other key must be used to unlock it. Any two keys will work, which is the beauty of the SuperLock—but the keys have to be a *matched* pair. With me so far?

SuperLocks are available in fine stores everywhere, but to have a pair of matched keys made, you must go to a very special locksmith—a SuperLocksmith, naturally. This locksmith will create a pair of matched keys, one public and one private. The locksmith

will keep a copy of your public key and make a duplicate for anyone who asks, free of charge. Finally, this locksmith will also vouch for the fact that he made the lock for you, specifically, and can prove that he gave the single, private key directly to you. Basically, the SuperLocksmith is vouching for your identity.

Given this clever design, we can now say two very powerful things. First, if I lock a SuperLock with someone's public key, then that someone is the only person on the entire planet who can open that lock (because they are the only person who has the private key). That is to say that I know for a fact that if I were to lock this special lock with one of Alice's public keys (which I could pick up for free from the locksmith), then I can be sure that Alice, and only Alice, could unlock it.

But the second thing we can say here is just as important and not as obvious. If I were to receive something with a SuperLock on it and Alice's public key could open that lock, then it must have been Alice who locked it (with her private key). And therefore, I can guarantee that whatever is in the locked box did in fact come from Alice.²⁵

We now have all the tools we need to resolve our dilemma. We're in the home stretch here! Hang with me just a bit longer.

Putting It All Together

Let's start from the top again and see how this works with our new tools. Alice wants to send Bob some confidential papers. She wants to make sure that no one else will be able to read these documents, even if they were to intercept them in transit. She also wants to make sure that Bob will know beyond a shadow of a doubt that Alice was the one who sent them. Finally, just to be safe, Alice wants to also give Bob the means to verify that the documents have not been altered in any way.

So, Alice and Bob each buy a Dox-Ray machine from their neighborhood big-box electronics store. They also each buy a SuperLock from a local SuperLocksmith, who creates a pair of matched keys for each lock. Alice and Bob take home their private keys and put them somewhere safe. They also pick up a free copy of the other person's public key at their local SuperLocksmith chain store.

²⁵ This provides something called *nonrepudiation*. That's a fancy legal term that basically means Alice can't plausibly deny that something digitally "signed" with her private key came from someone else.

Alice is ready to send some private documents to Bob. Alice puts the papers in a secure box. Then she takes out her Dox-Ray machine and scans the documents. She puts the resulting Dox-Ray image into another, smaller box. She then locks this smaller box with one of her own SuperLocks using her private key. Since the box was locked with Alice's private key, anyone can open it using one of Alice's freely available public keys. The point in this case is not to protect the contents (the X-ray image)—the point is to declare that Alice was the one who X-rayed the documents and therefore the one that sent the package.

Now Alice puts the little box containing the Dox-Ray image inside the big box, along with the confidential papers. She then locks the big box with another SuperLock, this time using Bob's public key. At this point, the only person who can unlock that big box is Bob. Alice confidently hands her package to her new and rather shady-looking mail carrier, Mallory, who dutifully delivers the box to Bob.

Bob takes the locked box from Mallory, who seems to be grumpy today for some reason. He unlocks the SuperLock on the outer box with his private key. He then removes the smaller box that contains the X-ray image. Using Alice's public key, he opens the smaller box and removes Alice's X-ray image. Because the SuperLock opened using Alice's public key, he knows that Alice was the one who could have locked it. He then whips out his Dox-Ray machine and takes his own image of the documents he received. The image exactly matches the one Alice sent! Now he knows that even if the box had somehow been compromised, the contents have not been altered.

And there you have it! With a little ingenuity, we have transmitted sensitive data with confidentiality and integrity! The only part of the CIA Triad we didn't address was availability. Mallory could have thrown the box in the ocean or simply never delivered it to Bob. But that's outside the scope of our little story.

At a base level, these are the same mechanisms used to secure just about all communication on the Internet today. There are many different algorithms and complex combinations of these mechanisms, but the fundamental principles are the same. The public and private key pairs are negotiated behind the scenes by your computer (the client) and the far-end computer (the server). While you could actually create a public/private key pair and register them with a formal key authority (the locksmith in our analogy), most average people have no need for this. You prove your identity when you first set up your online account, and from then on you use a combination of user ID and password to authenticate. Your computer or smartphone does the rest.

Newer Isn't Always Better

In the realms of security, there is a constant struggle between using the latest and greatest technology while at the same time not trusting anything until it has been proven using the test of time. Let's say you were in a castle with an angry horde outside your gates and I came to you with a new-fangled magical force field that I guarantee will be stronger than any stone wall you could build. Would you tear down your walls and install the force field based on my say so? Probably not. What if I showed you reams of laboratory data where I tested my force field against a stone wall with simulated attacks? If you were properly worried about your safety, this would still not be sufficient. Yet, if this product were truly better than what you have now, you'd be wrong to ignore it. So, what would you do?

Well, you'd probably deploy the new force field *in addition to* your existing walls and see how it held up during some actual assaults by actual adversaries. And you would probably do this for some time before you decided it was safe to replace your walls with the newer tech. Stone walls are something you know and trust. You know how they're built; you know how to build them well because you've gone through many iterations of building them. You know their weaknesses, and you've figured out how to shore them up. But this new force field thing... it's never been used. You really have no idea how it will perform in the real world. What if the designer missed something crucial? What if it works great in the lab where you can control everything but works poorly in the real world where there are many variables outside your control (like having unfailing and unlimited access to magical energy)?

The same is true for security. New encryption schemes, new authentication systems, and new security processes are generally avoided until they've been around for at least a few years. This gives independent security teams a chance to kick the tires, take it for a spin, and see how it performs in the real world. It's all well and good to come up with a new encryption algorithm that's mathematically sound on paper, but it's quite another to actually implement this algorithm in software and hardware.

Quantum Computing

There's one new technology that's starting to get more attention in the mainstream press: *quantum computing*. Specifically, this technology is touted as being able to cut through modern encryption techniques like butter. There is some truth to this, but the reality is not nearly as grim as many news stories make it out to be.

Public key cryptography is based on some heavy-duty math, but the basic idea is that the encryption uses math problems that are very easy to perform in one direction but are extremely hard to reverse or undo—even with supercomputers. For example, many crypto algorithms rely on multiplying large prime numbers, which is relatively easy to do. To break the encryption, you would need to undo this multiplication (in math terms, you need to factor the product into the original two prime numbers), which is extremely difficult to do...for a normal computer.

Quantum computers are weird. They can sort of do multiple math operations all at once, where a regular computer would need to do them sequentially. It's hard to explain, but the upshot is that they are much better at factoring large numbers than normal computers. Theoretically, they could be used to break encryption that is based on the prime number factorization problem in much less time than a regular computer.

But never fear; all is not lost. First, practical quantum computers are still several years away. They are very much still in the experimental stage of development. But more importantly, cryptographers saw this coming a long time ago. They have been diligently working for many years now on newer encryption techniques (dubbed *post-quantum cryptography*, or PQC) that rely on different difficult math problems that are not so easy for quantum computers to tackle, such as *elliptic curve cryptography*. By the time quantum computers are viable, we'll have technology in place that will be resistant to their abilities.

Graduation Ceremony

Congratulations! You have successfully completed your Castle Guard Certification Program! The castellan of the keep has bestowed upon you a nifty scroll with fancy writing. Way to go! Seriously, though, this last part about encryption was the trickiest part of the entire book. You don't have to understand it, but it will definitely give you a leg up with understanding the recommendations throughout the book.

Summary

- Computers have been around for decades, but there are still lots of basic terms and concepts that aren't well understood. Hopefully this chapter cleared a lot of that up for you.
- We also learned a bunch of cybersecurity terms. If you forget something, remember to turn to the glossary for quick help or you can return to this chapter as needed.
- Hackers are not always criminals, any more than engineers or scientists are. Hackers are just computer tinkerers, studying how they work and figuring out how to make them do new things. We need "white hat" hackers to help us find and fix the chinks in our cyber armor before the actual cybercriminals do.
- Our digital photos, movies, music, and documents are all made up of bits and bytes. That data is sent and received over the Internet in chunks called packets. And those packets are delivered much the same way letters are delivered by the postal service.
- Encryption is a marvelous tool that allows us to keep our data safe and secure—both on our hard drives and as it traverses the public Internet. I explained how we use encryption and other cryptographic tools like hashing functions to protect the integrity and confidentiality of that data.
- Quantum computing is coming, and it will require that we update our encryption techniques, but we'll have everything in place when the time comes—probably well before we need it.

Now you're ready to start taking some action! In the next chapter, you'll take the first steps on your quest by backing up your important data and reducing your security and privacy footprint.

Going Further

There are so many fun and useful things you can do with a computer that many people—even people who use computers on a daily basis—aren't aware of. There are also lots of shortcuts and cool tricks that can save you a lot of time and frustration. If you use a computer regularly, I would strongly suggest buying a book or taking a class on how to use it.

- *Code: The Hidden Language of Computer Hardware and Software* (Charles Petzold, Microsoft Press, Aug 2022) is a marvelous book that explains how computers work from first principles. The style is engaging and the explanations are understandable by anyone. I was fortunate enough to interview Charles about the second edition: <https://podcast.firewallsdontstopdragons.com/2022/09/12/decoding-computers-software/>
- For the Macintosh or Windows PC, look at a recent edition of one of the *Teach Yourself VISUALLY* book series, like *MacBook Pro & MacBook Air* or *Windows 11*.
- Also, the *...for Dummies* series of books are usually pretty good. Try *macOS Ventura for Dummies* or *Windows 11 for Dummies*. There are also *for Dummies for Seniors* versions, if you think that makes more sense for you (and it honestly isn't a matter of how old you are).
- If you're interested in the history of cryptography, *The Code Book* (Simon Singh) is a great book.
- If you want to learn more about history of computer hacking, the seminal book on the subject is called *Hackers: Heroes of the Computer Revolution* (Steven Levy, O'Reilly Media, May 2010). You might also try watching the documentary *Code 2600*.

Checklist

Tip 3-1. ★ Don't Click Links, If Possible

Links can be faked or tweaked ever so slightly so that a human might not notice. For example, out1look.com instead of outlook.com or tvvitter.com instead of twitter.com... did you catch the difference? It may depend on the font you're using to view this book.

Whenever possible, leave the link be and go straight to the source in your web browser. For example, if you get a suspicious email or text message from your bank that says "click here to verify your account," just log in to your bank directly and check your account for any notices (or call them). Note that it doesn't really matter if the email or text comes from someone or some company you trust—the sender name can be forged or their account could have been compromised.

The main rule here is: don't click any links that you didn't ask for. For example, if you just reset your password, then you would expect an email shortly thereafter with a link to click. But if you get an email out of the blue saying "your account has been hacked, click here to set a new password," you should not click that link. Log in to the affected account by typing in the address or using a bookmark/favorite, and then look for notifications.

If you're worried about a link or button that you really need to click, you can try testing it on this website first. Right-click the web address link and copy it, and then paste it on this website:

<https://www.virustotal.com/gui/home/url>

Tip 3-2. Watch Out for Shortened URLs

The formal name for a web address is a *Uniform Resource Locator*, or URL. Because web addresses can get pretty ugly, there are several services that will allow you to create shortened versions that are easier to type and/or remember. The service takes the short version and then automatically forwards your web browser to the original destination. Unfortunately, this also has the effect of hiding the ultimate destination of the link.

There are several websites that will let you expand a shortened URL without actually visiting the website, but I like this one. It will even attempt to give you an image of what the site looks like.

<https://checkshorturl.com/>

Tip 3-3. ★ Don't Open Email Attachments, If Possible

While images are usually safe, things like Microsoft Office documents (Word, Excel, and PowerPoint files), PDF files, executable files, installer files, or compressed files (like zip files) should be avoided—or any file with an extension you don't recognize. At work, follow whatever policies your company specifies. You can't get very far if you don't trust email from your coworkers. But at home, you should be very wary about opening any attachment that you didn't explicitly ask for. If you're not sure, contact the sender first (via phone or some other means) to make sure they did actually send it.

CHAPTER 4

Get Your Castle in Order

With the key background knowledge from the previous chapter, we're ready to start taking some truly important steps to being more secure. If you do nothing else but follow the tips at the end of this chapter, you will be miles ahead of most people.

Backups

What if you had a time traveling device...Doctor Who's TARDIS, Hermione's Time Turner necklace, Doc Brown's DeLorean, or the classic HG Wells contraption? Then you really wouldn't have to worry about security, right? If something bad happened, you could just go back in time, before it happened, and then avoid it the second time around. Short of maybe death, there would be really nothing from which you couldn't recover. You would have the wondrous power of the Do-Over!

This is the same principle behind backing up your data. If you keep regular backups of your data, then you can never lose anything. While backing up your data can't prevent someone from copying and abusing your data (e.g., identity theft), it can at least prevent you from losing your data to ransomware or a crashed hard drive or even a natural disaster. Backing up your data is one of the best techniques for mitigating the damage from an attack or random stroke of bad luck. Luckily, in today's world, it's fairly easy to do. It does, however, cost money. Think of it as insurance—and investment in your data security.

A common guideline for data backups is the *3-2-1 Rule*: for any important file, you should have *three* copies, on at least *two* different types of storage, and *one* copy should be offsite. When I say “three copies,” functionally that means the original plus two backup copies. The original will be on your computer's hard drive. If you have two backup copies and one of those backups is stored in the cloud somewhere, then that meets the other two criteria.

So let's look at your three main options for backing up your data:

1. A local, external hard drive
2. A cloud backup service
3. A cloud drive (file synchronization) service

External Hard Drive Method

Let's look at the local external backup hard drive option first. As we discussed in the previous chapter, all your data—your files, documents, digital photos, downloaded music, and home movies—live on your computer's hard drive. Unlike all the crap in your garage, you can create perfect and free copies of all of this data anytime you want. Keeping a backup copy of this data is as easy as buying an external hard drive, plugging it into your computer, and then telling your computer to use this drive for backup.

Both Windows and Macintosh computers come with software built-in for this purpose. This software is even smart enough to keep multiple backups. It's not just a single copy of your data—it's a rolling copy of your data as it changes. The first backup will obviously need to make a copy of every single file, but subsequent backups only need to make copies of the files that have changed. These backup services will even allow you to restore older *versions* of files. This is helpful in cases where you somehow messed up a file or just want to undo a bunch of changes you made. Having a full backup of your entire hard drive, with multiple versions, is really just like having a time machine (and in fact, Apple cleverly dubbed its backup software Time Machine). You can return your computer data to just about any point in time—on a per-file basis, if necessary. You can even completely restore all your files and data to a new computer if your current computer bites the dust.

Sounds pretty foolproof, right? The external hard drive option is a solid solution for most people. However, there are at least two problems with it. First, it doesn't protect you from natural disasters. If your house burns down or floods with water, the hard drive sitting right next to your computer is going to suffer the same fate as the hard drive that's inside your computer. Second, malware can mess up an attached external backup drive just as easily as they can mess up the drive inside your computer. However, external drives are still excellent protection against computer hard drive crashes, accidental file deletion, or any problem that affects only the main computer. They also tend to be the cheapest solution over time because they require only a one-time cost (buying the external hard drive).

Cloud Backup Method

Now let's look at the second option: online backup (also called cloud backup). This includes services such as iDrive, Backblaze, Carbonite, and many others. You sign up for the service, you download their application, and you tell it to start backing up your stuff. That's it. The cost varies from service to service and even varies over time for a given service because of competition and falling costs of storage. (At the other end of your Internet connection, they have a hard drive with your name on it, basically—so effectively you just paid them to buy the external drive and keep it off-site for you.) Unlike the fixed cost of buying your own external hard drive, these services make money by charging you an ongoing fee to keep your data for you. So over time, this option is going to cost more than the external drive option.

Online backups solve the natural disaster problem because the data is stored outside your home. It also usually solves the malware problem because there is no direct access to the cloud data from your computer.

But the online backup solution has its drawbacks. First, there's just the problem of logistics. Let's do the math. (Don't worry, *I'll* do the math; you just follow along.) Let's say you have a one-terabyte hard drive, which is fairly common. Let's also assume you have a modest Internet connection that allows you to upload ten megabits per second.¹ That means when everything is working perfectly, under absolutely ideal conditions, you can upload ten megabits of data to your online backup service every second. How long would it take you to copy your entire hard drive to the online backup provider? First, note that your drive is one *terabyte*, but your upload speed is measured in *megabits*. If you recall from the previous chapter, there are eight bits in a byte—so one terabyte is eight terabits. If you divide eight terabits (eight trillion bits) by ten megabits (ten million bits) per second, you will see that it will take 800,000 seconds to transfer all of this data... which is more than nine days! Recall that this assumes ideal conditions, which will never happen for nine straight days. If you have faster broadband service, you can cut that time down quite a bit. But the point of this math exercise is just to show that it may take quite a while for that first backup to complete.

¹ Note that we're talking *upload* speeds here, not *download* speeds. Most times you care about download speeds, which is the speed most ISPs tout. Often the upload speed is much slower than the download speed.

So, why would anyone bother with an online backup solution? First, you're probably not going to upload your entire hard drive to the cloud. For example, you don't really need to back up your operating system or applications, which take up a lot of space and are easily replaceable. You might not even need to back up your music, if you use a streaming service like Spotify or Apple Music. This could greatly reduce the amount of data you actually need to back up. Most people really only *need* to back up the files that they simply cannot replace—documents (which are usually very small), personal photos, and maybe home movies. Second, you only need to upload *everything* one time. It will take a while, but once it's done, you only need to upload new files and files that have changed. So, while it may take a week or more for that initial backup, it will be much faster after that. Finally, your hard drive is probably not 100 percent full. Our calculations were based on the worst-case scenario.

The main issue with cloud backups is privacy (or lack thereof). You're giving all your data to a bunch of complete strangers...those embarrassing spring break pics, "love letters" from that special someone, your tax returns, and even things like your browsing history and emails. If you back up your cell phone data to your computer, you could be exposing your text messages, contacts, and location history too. But wait, surely all your data is encrypted, right? Yes... but who holds the key? Any service worth considering will encrypt your data during transit (from your computer's drive to their off-site drive), which will prevent someone like your Internet service provider from seeing any of the data as it flies by (data in motion). And most services will encrypt your data on their hard drives too (data at rest). If they do this properly (and that's a very important "if"), this would protect your data from any unauthorized access, including hacking. However, if served a warrant² from the police or FBI or a National Security Letter from the US government, they would be required by law to decrypt your data and hand it over (and probably also be strictly prohibited from telling you that they did it). And if they're able to decrypt it for legal reasons, then they can decrypt it for any reason—meaning that employees of the company may also be able to look through your stored data. However, most companies now allow you (and only you) to hold the encryption key, though it's almost never the default option. I will tell you how to do this, of course.

²Thanks to the CLOUD Act, passed in early 2018, they may not even need a warrant.

Cloud Drive Method

There is one more option to consider, which is sort of a minimalist version of the full cloud backup. If you don't have a lot of files to back up and you can keep those files in a single folder, then you could just use a cloud drive or file synchronization service like Dropbox to back them up. These services allow you to designate a single special folder on your computer that is synchronized across all of your devices through the cloud. Any changes to files in this folder are magically changed in the special folder on all your other devices, as well—almost instantaneously. If you add a file to this folder, it appears on your other devices. And if you delete a file from this folder, it disappears from the synchronized folder on your other devices. Furthermore, in most cases, these synchronization services maintain historical versions of all the files in this folder, meaning that you can recover files even after they've been deleted or get back older versions of the file (for a limited amount of time). Therefore, you could use this service as a sort of offsite backup.

However, there are drawbacks to this method. First of all, if you use a third-party solution like Dropbox, it will not be easy to backup certain types of files like music or photos if you want to use the built-in music and photo apps that come with your operating system. Second, like cloud backup services, the files are encrypted but the service provider usually holds the keys.

Apple, Microsoft, and Google have created their own “cloud drive” solutions: iCloud, OneDrive, and Google Drive, respectively. They are tightly integrated with their operating systems (macOS, Windows, Android, and Chrome OS) and are actually extremely difficult to avoid using these days. These services come with a minimal amount of free storage space, but you will almost surely need to pay for more if you want to use them to store all of your personal documents.

I'll discuss iCloud and OneDrive in more detail in Chapter 10. I will also discuss some solutions that are much more private because they give you full control over the file encryption.

Choosing Your Best Backup Solution

So...which option is the best? Honestly, if you can afford it, I recommend you do both an external hard drive and a full cloud backup. They each solve the same problem but in slightly different ways, with different pros and cons. If you do both, you get the best of both and address the shortcomings of each. This technique will also meet the 3-2-1 Rule criteria.

However, if cost is a problem, I recommend using an external hard drive. It's quicker, it's cheaper over the long run, and it keeps your data under your own control. Most cloud sync services give you five to ten gigabytes of file storage for free, so you could use that to back a handful of important files to the cloud. If you want to go the extra mile to protect against natural disasters or anything that could destroy both your computer and your external hard drive at the same time, then use *two* external hard drives: swap them once a month and keep one drive offsite somewhere (like at work). This is what I used to do before cloud backup costs came down.

If the computer you're backing up is a laptop, having an external hard drive that is always connected isn't terribly practical. You could get in the habit of plugging the external drive in every night, however. If you don't mind paying an ongoing fee and want to know that your data will always be safely held offsite, then using a cloud backup solution is probably your best option for a laptop.

If you truly want to ensure your privacy when using a cloud backup, you should choose a service that allows you to choose and manage your own encryption key.³ This means that all the cloud storage company will see is an indecipherable blob of bits. However, this also means that if you lose that encryption key, your data is effectively gone; even though the online service technically still has your information, neither you nor they can recover it in usable form. However, this isn't as scary as it sounds—I'll help you do this.

If you find that convenience is really worth more to you than privacy, then using iCloud or OneDrive is by far the easiest way to back up your most important data to the cloud—and it's probably enabled already. Microsoft and Apple have made it hard to avoid.

Keeping the Lights On

I would like to make one further recommendation. Computers need electricity to run. If that power source is abruptly cut off, it can cause serious problems for your computer, including corrupting your data. It doesn't have to be a complete power outage, either—just a flicker or “brownout” can cause your desktop computer to shut down abruptly.⁴ For this

³ As this book was being published, Apple announced that they would now support user-encrypted iCloud backups. This is a really big deal, though it still has some limitations. You can read more about it here: <https://support.apple.com/en-us/HT202303>

⁴ If you have a laptop, it has a built-in battery. Power interruptions are only an issue for desktop computers.

reason, if you have a desktop computer, I strongly suggest buying an *uninterruptible power supply* (UPS). This is basically a big battery that can be used to power your computer if the power to your house goes out, however briefly. You plug this battery into the wall and then plug your computer into the battery box. When the power goes out, the box will supply power to your computer for a limited amount of time—the bigger the battery you buy, the longer it will let your computer run. But all you really need is enough power to give your computer time to properly and gracefully shut down. Most of these UPS boxes have a data connection to your computer that allows the UPS to tell the computer when it should shut down. This means it will work without you being there to monitor it.

Minimization: Less Is More

One of the most effective techniques for increasing security is decreasing your exposure to threats. For castle builders, this might involve limiting the number and size of the entrances—that is, to reduce the number of places you need to defend. In the cybersecurity biz, this is referred to as reducing your *attack surface*.

For example, every single piece of software you have installed—every application, utility, plug-in, and extension—is just one more place that an attacker can probe for vulnerabilities. All software has bugs. Adding more software adds more bugs, and bad people can exploit those bugs.⁵ Worst yet, old software may no longer be getting important security updates—they may be riddled with known vulnerabilities that will never get fixed. Therefore, you should take every opportunity to close the gaps, reduce the number of vulnerabilities, and lower the risk of bad guys getting in.

Castle lords can also reduce their risk and likelihood of attack by simply having less valuables to protect. The same is true of personal data. *The only data that can't be stolen or abused is data that doesn't exist.* We call this data minimization. Privacy advocates implore companies to only collect the data they absolutely need and only store it for as long as it's needed. Data should really be treated like nuclear waste instead of “the new oil.” As we've already discussed in Chapter 2, without laws to restrict this behavior, we should assume the worst. And therefore, we need to take matters into our own hands wherever possible.

⁵ Note that this also implies that you shouldn't install lots of apps willy-nilly, either. Some people install tons of free and trial apps and then forget to remove them—particularly mobile apps.

Spring Cleaning

Spring cleaning isn't just for physical stuff—you need to periodically purge the apps you don't need or don't use. If the software in question was downloaded (as almost all software is today), then you can just reinstall it if you find later that you need it. Also, you have a complete backup of your system (right?), so in the absolute worst case, you can always jump in your digital time machine and return things to an earlier state.

There are other good reasons to clean up your system. First, those extra apps take up space on your hard drive. Just like crap cluttering up your garage, every so often you just need to purge old stuff to make way for new stuff. Second, many applications and utilities have components that run in the background all the time, whether you're actively using them or not. That chews up memory resources (RAM) but may also slow down your computer or your Internet traffic. Finally, many of these utilities and extensions are started automatically every time you boot your computer, which can significantly increase the time it takes to start up. Have you felt like your system has been running more slowly than it used to? Do you find it slower to surf the Web? Does your computer take forever to restart? Getting rid of the junk might very well speed things up.

If all of that isn't enough, here's another reason to remove unneeded software: these applications (particularly free ones) may be spying on you. It's sadly not uncommon these days for applications to sell your data to marketing companies and data brokers.

In the tips at the end of this chapter, I'll help you find and remove software applications you no longer need or use.

Data Minimization

If you followed the advice in the previous chapter and downloaded your data from Google, Facebook, and others, then you may worry that the task of reducing that mountain of information will be Herculean (or perhaps even Sisyphean). But thanks to privacy regulations in places like California and the EU, companies have been forced to give you free and simple online tools that allow you to delete some or all of your data.

You should strongly consider deleting some of your online accounts, as well—particularly social media accounts, if you can summon the courage to do so. For any account you decide you can live without, you should first download your data (see [Tip 1-1](#)), then delete your data, and lastly, delete your account altogether.

Last but not least, you should purge any files you no longer need—both physical (paper) documents and digital documents.

I will actually cover most of these tasks later in the book, alongside similar topics that deal with computer security (Chapter 6) and social media (Chapter 10).

Update All the Things

Once you’ve backed up all the important stuff and you’ve gotten rid of all the excess cruft, then the last thing you need to do before we proceed is to update whatever software is left after the dust settles.

It’s *extremely* important to keep your software applications and utilities up to date—particularly your operating system, web browser, and popular apps like Microsoft Office. New bugs, exploits, and other vulnerabilities are found in software *all the time, every day...24/7/365*. The bad guys are plentiful and highly motivated, and they don’t honor business hours or national holidays.⁶ Mature and responsible software companies are diligently patching these holes and making updates available as soon as they can.

But even when software makers release updates with bug fixes, the bad guys know that people are slow to patch the vulnerable software. As soon as the fixes are announced, cybercriminals reverse engineer the updated software to figure out what was fixed and then immediately (often within hours) create hacking tools to exploit the vulnerability.

At this point, I need to differentiate between the two types of software updates: major and minor. Most modern software has a multipart version number of the form X.Y or X.Y.Z, where X, Y, and Z are integer numbers—for example, version 10.3 or version 1.0.4. Minor updates are sometimes called “dot updates” or “point updates” because the major version number (the “X” here) stays the same, and only the numbers after the dot or decimal point go up (the “Y” or “Z” value). So, going from 10.3 to 10.4 or from 1.0.4 to 1.0.5 or even to 1.1.0 would be considered a minor update. Going from 10.3 to 11.0 or 1.0.4 to 2.0.0 would be a major update.

⁶Cybercriminals are known for striking over long holiday weekends. Hacking big companies can take time, so bad guys strike when most people are out of the office and have better things to do than think about work.

Major Software Updates

Major updates usually involve fancy new features or major changes to the look and feel. These major updates are often referred to as “upgrades” because of these feature changes, and it’s not uncommon for software vendors to charge money for upgrades. Despite the moniker “major,” these updates are not as critical from a security standpoint. They’re not really about bug fixes, though operating system upgrades (as opposed to just regular software application upgrades) often do contain new and desirable security and privacy features. Regardless, you don’t have to rush to install these major updates. In fact, I almost always wait at least a week to install them, even if they’re free, just to make sure there are no nasty problems with the new features.

Note that major updates or upgrades are usually not automatically installed, even if you have your settings configured for automatic updates. That’s another thing that makes major updates different from minor ones. Many times this is because major updates cost money but also because they tend to be purely feature updates and not security updates.

Upgrades to software applications are mostly a matter of choice. If you want the new features and are willing to pay for them, great—go ahead and upgrade. If not, you can stay on the current major version. My advice is different for minor updates, but we’ll discuss that in the next section.

For the remainder of this section, I’ll focus specifically on operating system (OS) upgrades.

Apple stopped charging for its OS updates a long time ago, mostly because Apple makes their money off of hardware, not software. There’s frankly no reason not to upgrade your Mac computers to the latest version of macOS that it will support. From a security and privacy standpoint, newer is definitely better for macOS. Apple’s update process is easy and safe too.

Microsoft, on the other hand, still charges for some Windows upgrades... frankly, it’s rather confusing. This is partly because Windows has several different flavors, as we mentioned in Chapter 1—they not only offer Home and Pro, but also Enterprise, SE, and Education. See what I mean? Confusing. But most regular people have the Windows Home flavor installed on their personal computers, so that’s what we’ll focus on for this book.

If your computer is new enough and has the right hardware features, you can upgrade from Windows 10 to Windows 11 for free in many cases. If your PC supports Windows 11, it has undoubtedly made you aware of this fact, pushing you to upgrade. There are some nice security features in Windows 11, so if your PC can handle it, I would upgrade to Windows 11.

I will say this, however...if your Mac or PC is so old that it cannot be upgraded to the latest version of the macOS or Windows operating system, then you should start thinking about getting a new computer, say in the next year or two. I say this because eventually Apple and Microsoft will stop providing even minor updates for older computers, meaning that you won't be getting crucial security fixes. It's also pretty obvious that they release fixes for the latest OS before fixing the older ones.

Upgrading your operating system is outside the scope of this book. So, if you decide to do this and you have any reservations about doing it yourself, you might want to find a tech-savvy friend or relative to help you. *Before you upgrade, be sure to perform a full system back up!* See this chapter's checklist for instructions.

Minor Software Updates

Despite the implication of the name, minor updates are the most important. They quite often include security fixes—and when they do, you want to install those fixes ASAP.

Both Microsoft and Apple have thankfully made keeping your operating system up to date easier over the years—even making it the default, which is great. If you turn on the right options (and I'll show you how), your computer will install critical security fixes automatically. These updates will usually be installed overnight if you leave your computer turned on.⁷

Apple and Microsoft have also managed to provide a mechanism to keep regular applications up to date automatically, as well—even software from third parties. If you get an app through the Apple App Store or Microsoft Store, the operating system can be configured to keep that application up to date for you. As an added bonus, Apple and Microsoft do some basic level of automated testing on the apps in their app stores, looking for shady practices or obvious security problems. They don't catch everything, but it's way better than nothing. This also allows them to remove a rogue app from the store at any time.

Applications that you've installed from a browser download or from some sort of external storage device cannot be updated using the app store updating system. These applications may have their own proprietary update mechanism, which will usually

⁷I almost never turn my computers off. There's little reason to do so today, even to save energy—most computers will enter a low-power “sleep” mode after some amount of time. However, sometimes it's helpful to restart your computer. I'll cover that in Chapter 6.

pop up a dialog when there are updates available. In some cases, you have to explicitly find the “Check for updates” menu option or even check directly with the software maker (usually on their website) to determine if there’s a newer version available. Some applications can be installed both via the official Apple/Microsoft app store and via direct download—for all the reasons given here, you should install via the app store if you have the choice (even though it may cost more).

If you don’t want to turn on automatic updates, then you will need to periodically run through all your software and update it manually. I recommend at least once a month for most applications and weekly for your operating system and crucial applications like your web browser, email program, and any “office suite” software (word processing, spreadsheet, or presentation software). You can see how that would be painful and error prone. So, you might want to reconsider turning on automatic updates.

What both Apple and Microsoft need is something that the Linux operating system has had for a long time now: a package manager. A package manager’s whole job is managing your software: installing, removing, and updating. It even handles dependencies between different software packages, whether they come from the same vendor or not. Windows actually does have a package manager—it’s called WinGet. However, it’s not for the faint of heart because it’s a command-line tool (i.e., there is no graphical user interface). There are also third-party tools for managing your installed applications, but I don’t feel comfortable recommending them. This is a function that should be built into your operating system, in my view. I would only trust Apple and Microsoft to do this properly.

Summary

- One of the best ways to insure yourself against catastrophic loss is to make full backups of all your files, or at least the truly irreplaceable ones. You can do this using an external hard drive or using a cloud backup service (or both).
- You should follow the 3-2-1 Rule for important, irreplaceable data: three total copies, on two different types of storage, one of which should be offsite.
- The only data that can't be stolen or abused is data that doesn't exist. A close second to nonexistent data is data that no longer exists. Deleting your data from online services, particularly social media, can significantly reduce your exposure.
- Once you've backed everything up, you should take some time to clean up your hard drive—remove unused applications and utilities. Every piece of software has bugs, so if you're not using something, it's safest to just get rid of it. You can always reinstall it later.
- You need to keep your operating system and key applications up to date. Software bugs and security holes are discovered all the time and keeping up to date will mitigate your risk. You should take advantage of automatic updates wherever possible.

In the next chapter, we'll ask the question: who are you, really? Notice that this question really asks two things: what is your identity and can you prove it? Turns out those are pretty fundamental questions. The answer impacts both security and privacy.

Going Further

- *Trust No One*: In this blog article, I talk about several privacy and security issues related to data minimization. All of the suggestions here will be covered by tips in this book, but you still might find it interesting to read: <https://firewallsdontstopdragons.com/trust-no-one/>
- *Deleting Your Way to Better Security*: This article talks about deleting unused or unneeded software. Again, this book will cover all these tips: <https://firewallsdontstopdragons.com/deleting-your-way-to-better-security/>
- *7 Steps to Tidying Your Digital Life* (*New York Times*, *Wirecutter*, Jan 2021): In the spirit of providing second opinions, you'll see that the *New York Times* has similar feelings on minimization. I believe I cover all their recommendations in this book, as well: <https://www.nytimes.com/wirecutter/blog/tidying-your-digital-life/>

Checklist

We're finally ready to start making real changes! It's crucial that you back up your computer and update your existing software before you make major changes, so *please* don't skip those steps. This checklist will tell you how to do both.

Tip 4-1. How to Change Computer Settings

This is the first checklist where we really start getting into making changes on your computer. Many of the tips in this book will ask you to alter general computer configuration settings. So, let's take a minute to talk about how to find and change any given system setting on Windows and macOS. (We briefly covered this in [Tip 1-2](#).)

The short version is that finding settings on your computer has gotten difficult. There are a crazy amount of switches, dials, and knobs you can fiddle with. And for some unknown reason, Apple and Microsoft like to keep moving them around. Thankfully, they have given us the ability to just search for them by name, and that's the technique we will use in this book. Let me show you how to do this.

Tip 4-1a. Microsoft Windows 11

First, find the search tool for Windows. See [Figure 4-1](#).

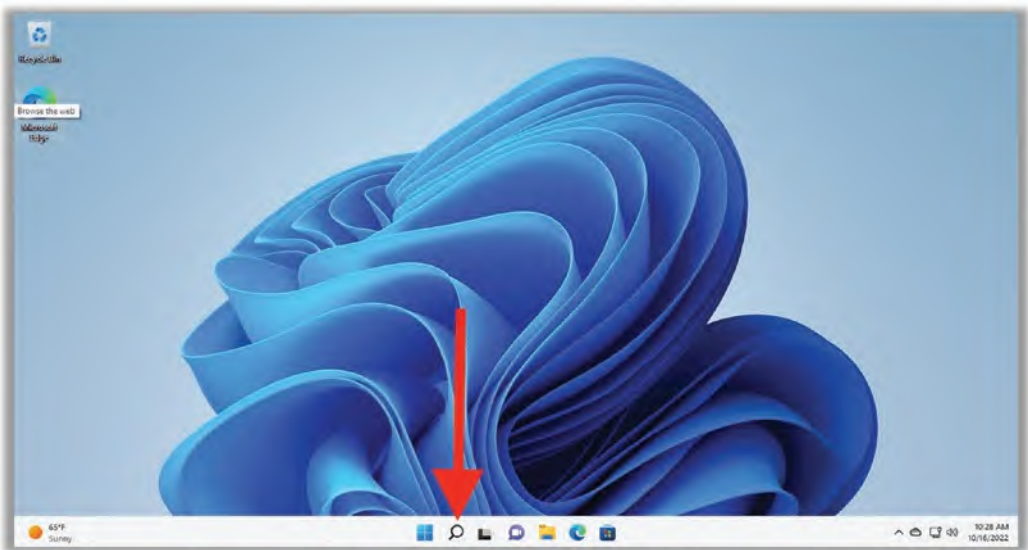


Figure 4-1. Windows 11 Search tool location

Click the magnifying glass icon to bring up the search tool. Try a simple search, like “update” (Figure 4-2).

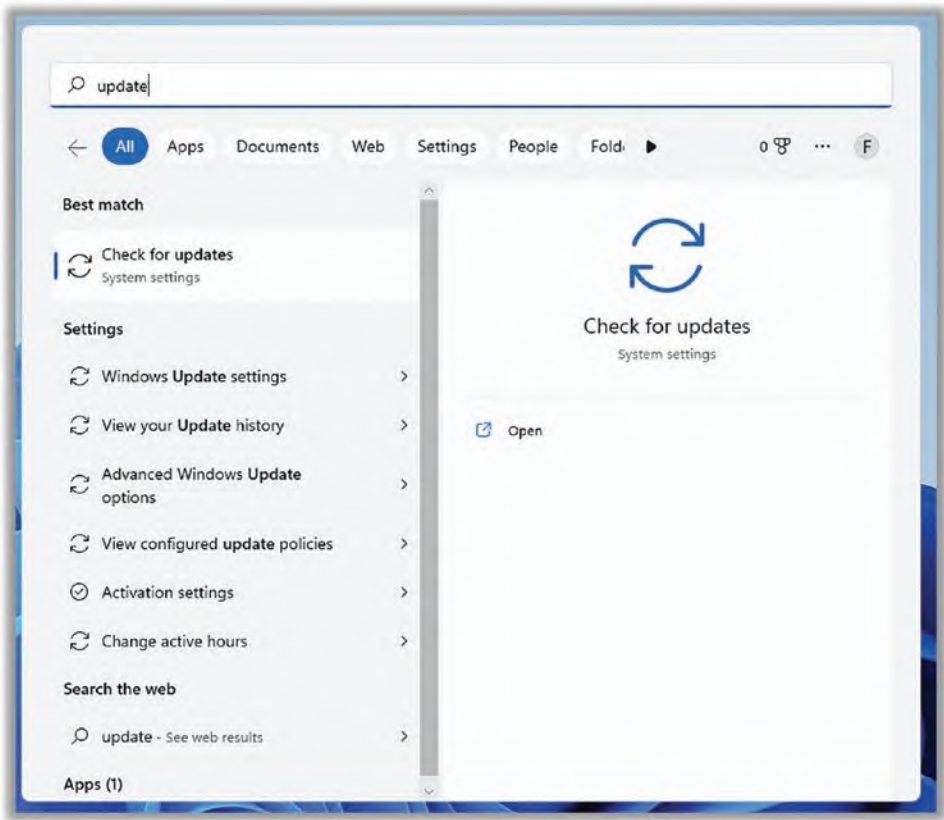


Figure 4-2. Windows 11 Search for update

You can see that this finds several settings, including “Check for Updates” as the best match, but also several others, including “Windows Update Settings.” Just click the one you want to bring up the proper settings window.

Tip 4-1b. Microsoft Windows 10

The Windows 10 search tool is always there for you in the taskbar at the bottom (Figure 4-3).

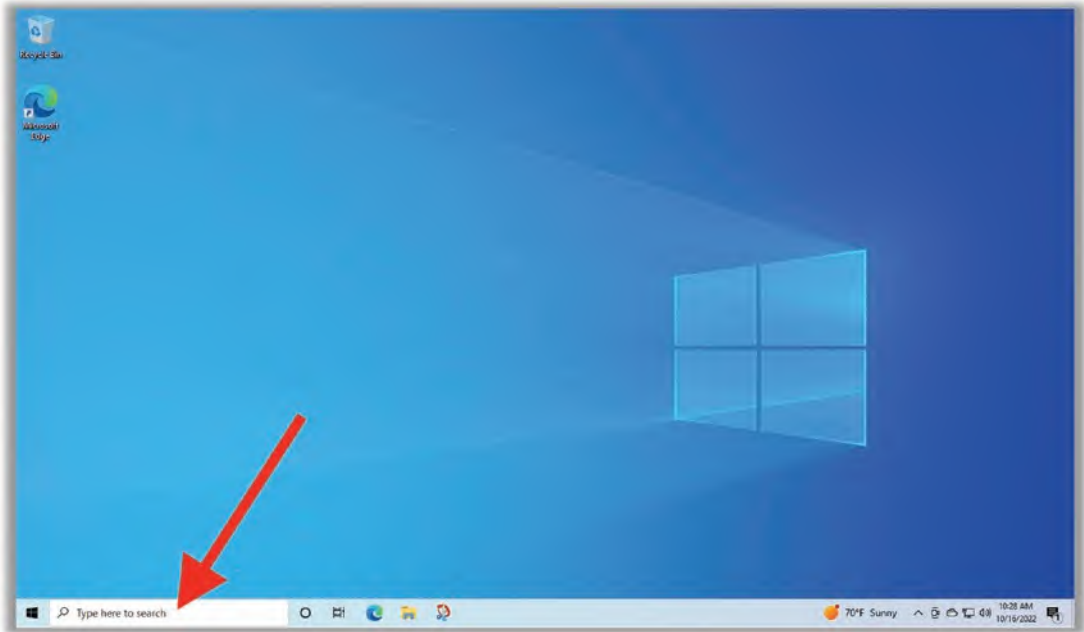


Figure 4-3. Windows 10 Search tool location

In this text box, try at simple search, like “update” (Figure 4-4).

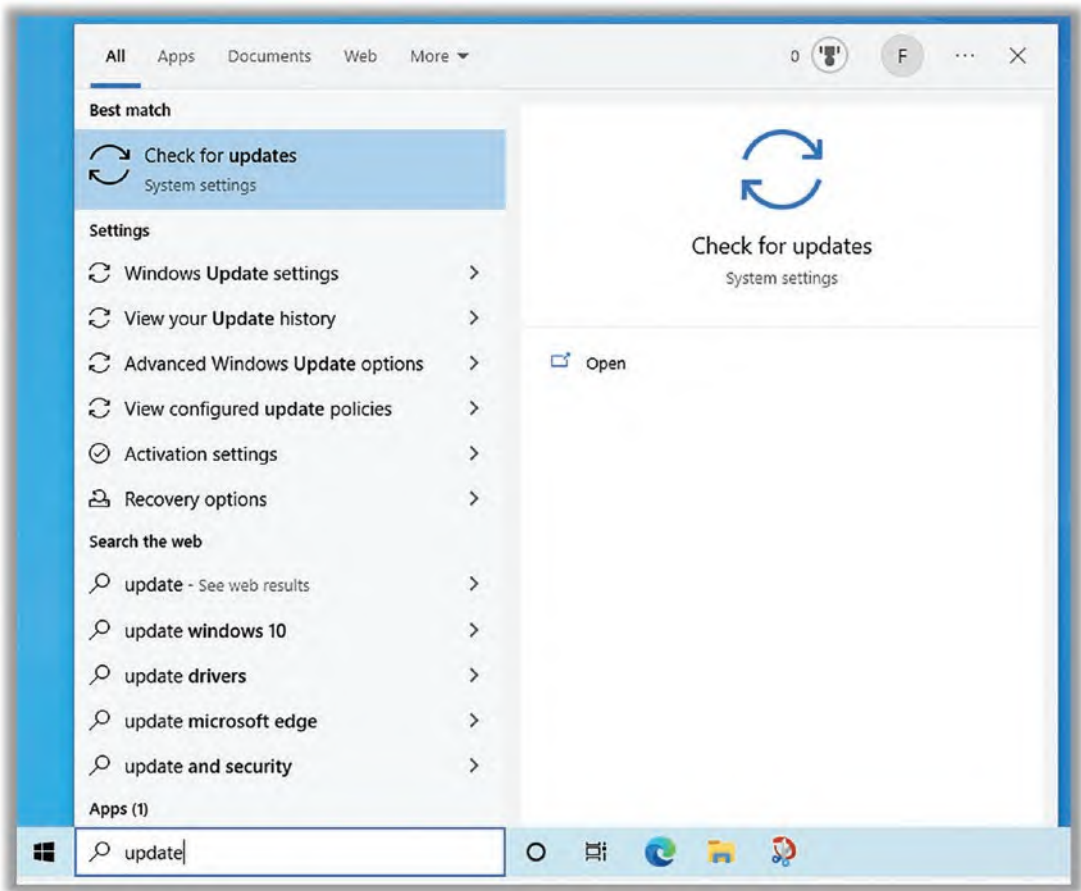


Figure 4-4. Windows 10 Search for update

You can see that this finds several settings, including “Check for Updates” as the best match, but also several others, including “Windows Update Settings.” Just click the one you want to bring up the proper settings window.

Tip 4-1c. macOS Ventura

Apple radically changed the system configuration look and feel with Ventura. I can't say I'm a fan and I'm not alone. They may yet change this back. In Ventura, your macOS settings are called System Settings (it was previously called System Preferences), and they look more like the settings on your iPhone. This was an intentional change—Apple is trying to make iOS and macOS work similarly.

To make system changes, go to the Apple menu in the upper-left corner of your screen (Figure 4-5).



Figure 4-5. *macOS Ventura Apple menu location*

From this menu, select “System Settings” (Figure 4-6).

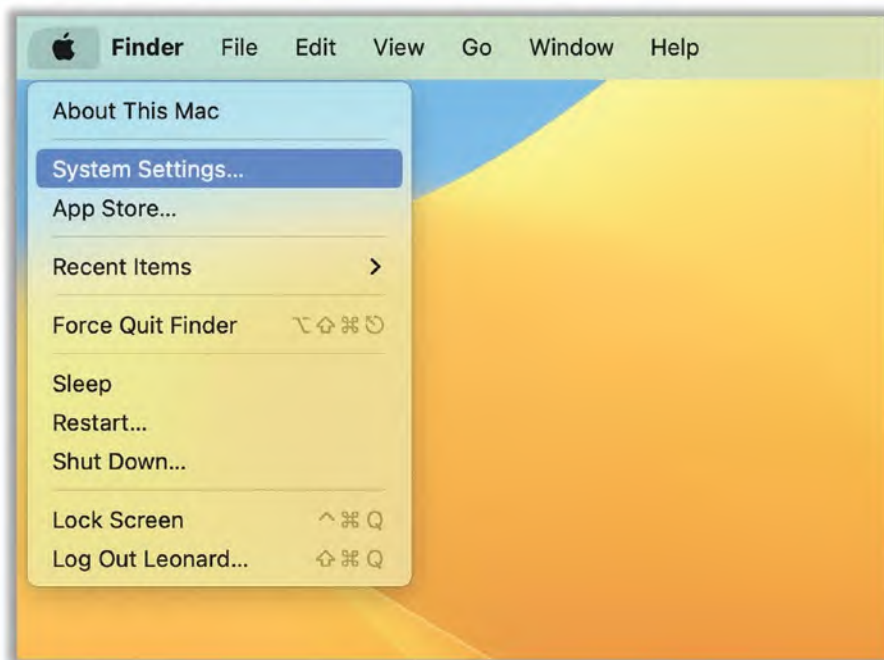


Figure 4-6. *macOS Ventura System Settings under Apple menu*

This will bring up the System Settings dialog (Figure 4-7). This one dialog contains all the system settings that we’ll be tweaking in this book. It looks very different from macOS Monterey, but very similar to iOS.

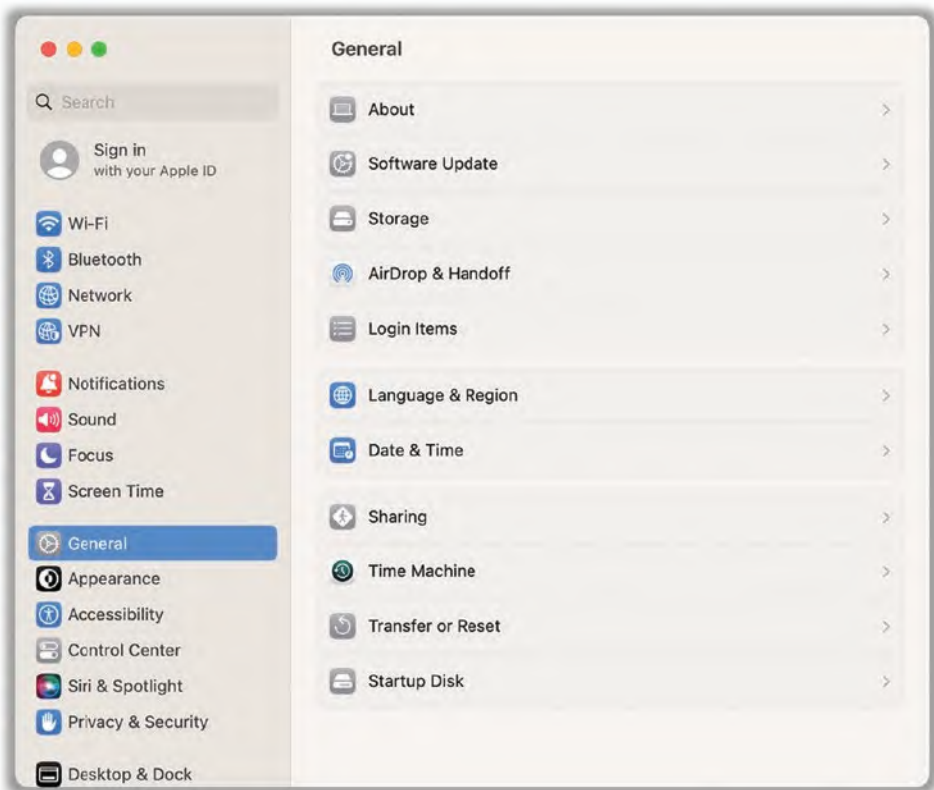


Figure 4-7. *macOS Ventura System settings*

Because it can be difficult to find a specific setting, in this book I'll have you find settings using the search bar here. Try searching for "security." You should see something like Figure 4-8.

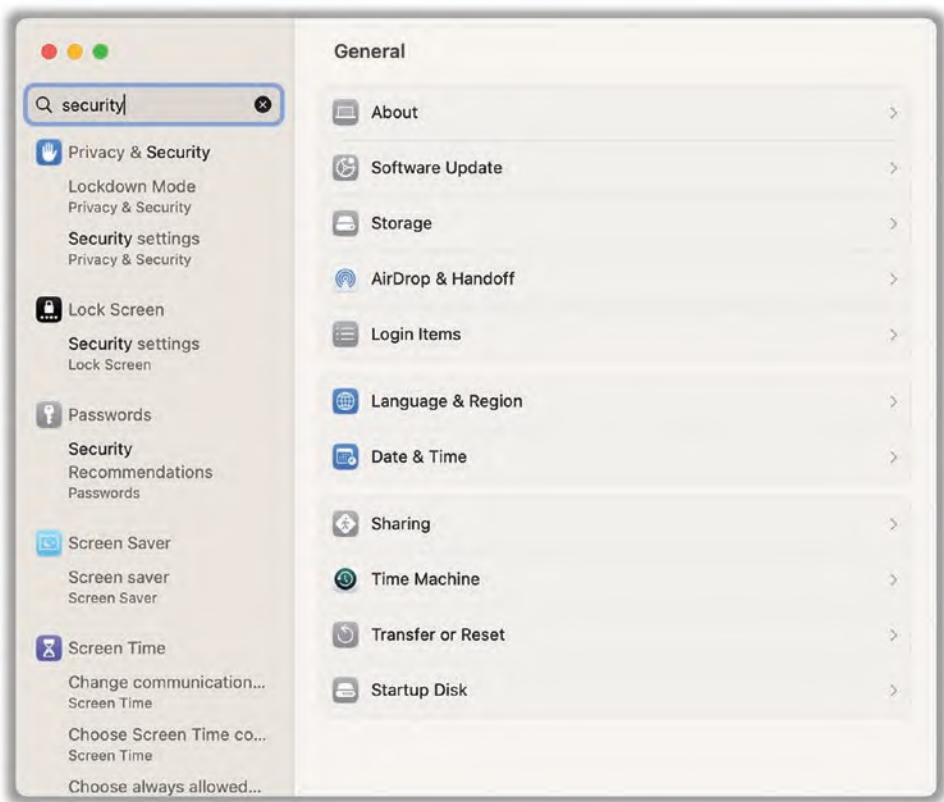


Figure 4-8. macOS Ventura System settings search

You’ll see that there are several results just below the search bar. Just click the search result in the list that you want. I will always attempt to give you the exact search term you need, resulting in the top result being the one you want. As you start typing, as soon as you see the text I specify, you can select it in the list to jump right to this setting.

Tip 4-1d. macOS Monterey

In macOS Monterey and earlier, all Mac system configuration is contained in the System Preferences. To make system changes, go to the Apple menu in the upper-left corner of your screen (Figure 4-9).



Figure 4-9. macOS Monterey Apple menu location

From this menu, select “System Preferences” (Figure 4-10).

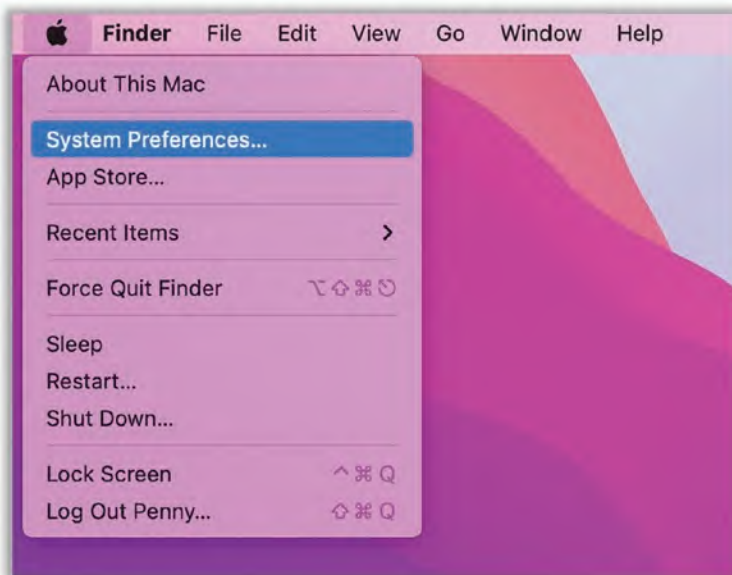


Figure 4-10. macOS Monterey System Preferences under Apple menu

This will bring up the System Preferences dialog (Figure 4-11). This one dialog contains all the system settings that we’ll be tweaking in this book.

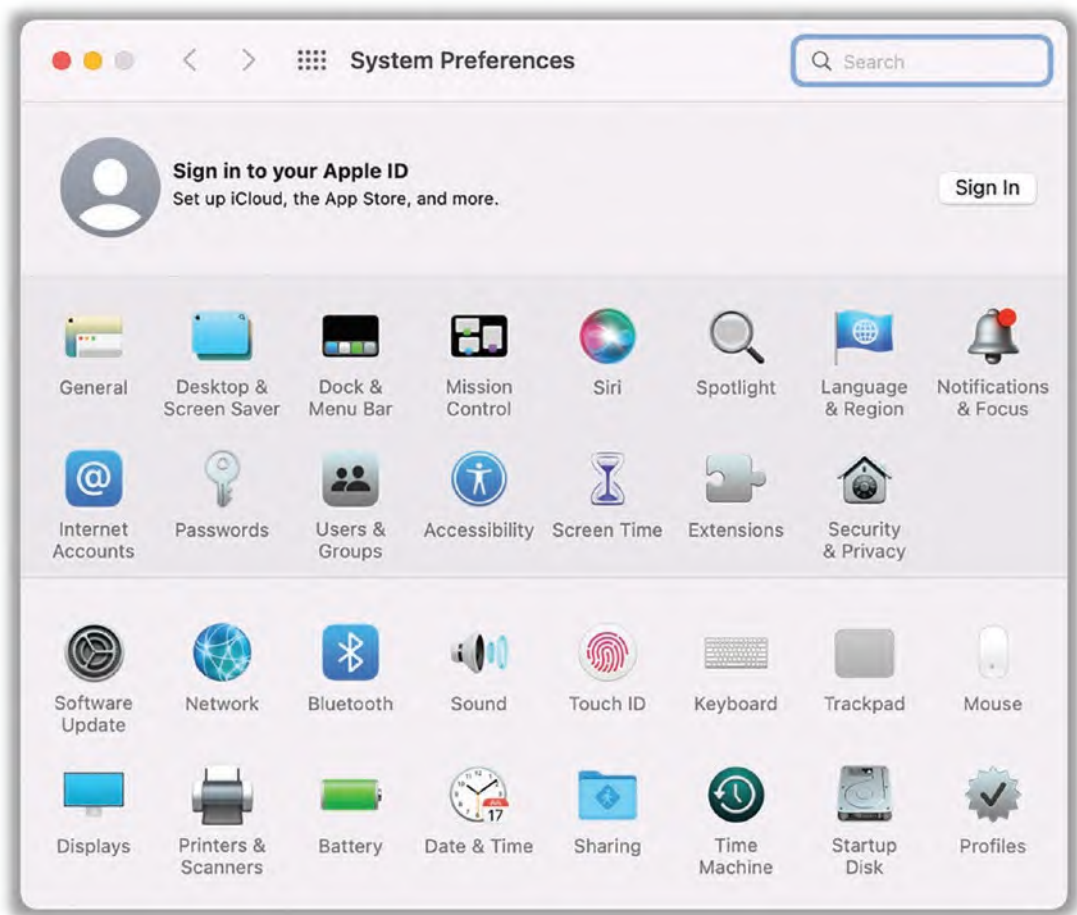


Figure 4-11. *macOS Monterey System Preferences*

Each of these icons represents several more settings, grouped by type. Because it can be difficult to find a specific setting, in this book I’ll have you find settings using the search bar here. Try searching for “account.” You should see something like Figure 4-12.

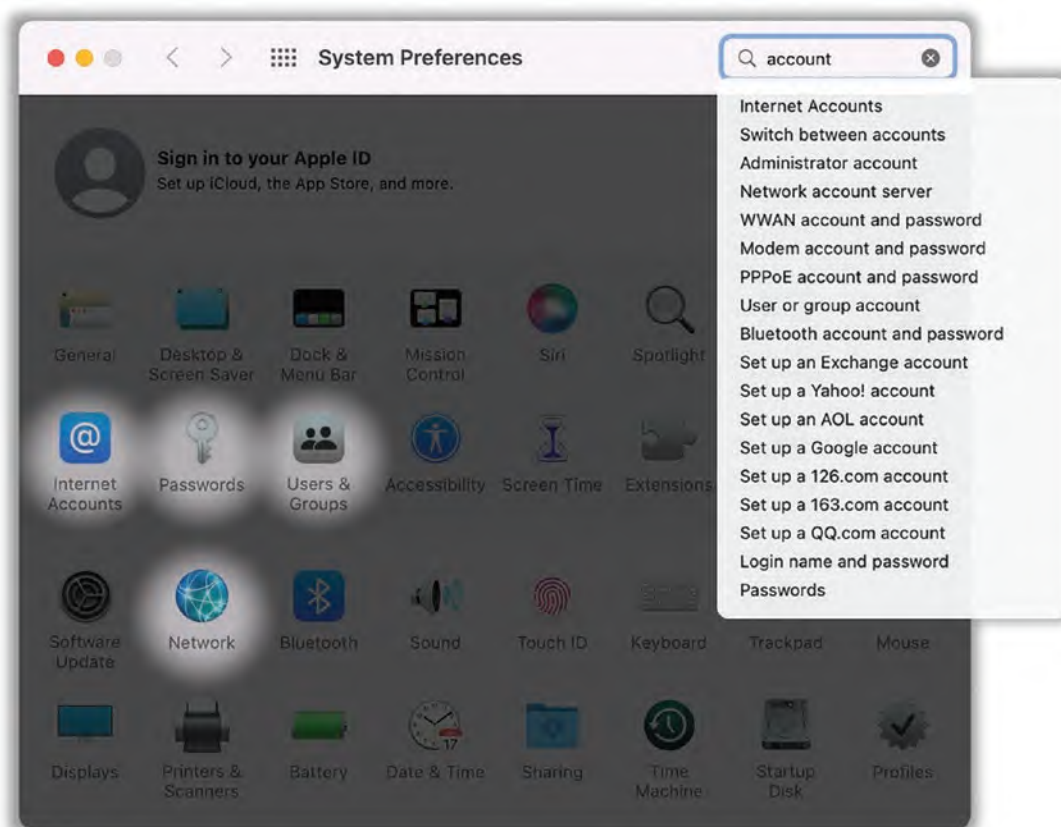


Figure 4-12. *macOS Monterey System Preferences Search*

You'll see that there are several results just below the search bar, as well as several icons highlighted in the dialog window. Ignore the icons and just click the search result in the list that you want. I will always attempt to give you the exact search term you need, resulting in the top result being the one you want. As you start typing, as soon as you see the text I specify, you can select it in the list to jump right to this setting.

Tip 4-2. ★ Back Up to an External Drive

Backing up your computer is one of the best ways to protect your important computer files and data from getting lost or messed up (either maliciously or accidentally). If you have a solid backup of all your important files, you can always replace them if something should go horribly wrong.

You have two main options for backup: an external hard drive or a cloud (online) backup service. If you can afford it, I would do both. If you feel you have to choose just one option, read the section of the chapter on backups to help you choose which one would be best for you.

Before you can configure the backups, you'll need to get yourself an external hard drive and connect it to your computer. *Please follow these instructions carefully and in order.*

Buy an External Hard Drive

External USB hard drives have gotten very affordable, and the prices are constantly falling (in terms of cost per gigabyte). These boxes come in various shapes and sizes but are generally rectangular and about the size of a deck of cards. These devices are frequently on sale at chain stores like Best Buy, Target, Office Depot, and Fry's. You can also buy them online at places such as amazon.com or newegg.com. I would look for a sale on a name-brand drive such as Western Digital (WD), Toshiba, LaCie, or Seagate. If you need help, go to a local store, and ask someone in the computer department to make some suggestions.

You have three main choices to make: type of drive, USB version, and size of drive.

- *HDD vs. SSD:* Older hard drives contain spinning magnetic disks—we call them *hard disk drives* (HDDs). Modern hard drives are purely electronic and contain no moving parts—we call them *solid state drives* (SSDs). HDD technology has been around for decades. These drives are larger and cheaper than solid state drives. They're also a lot slower, but for backing up your computer, that doesn't matter much. If you can afford it, I'd go with SSD over HDD, but either will work for this purpose.
- *USB version:* Be sure to get a drive that uses USB version 3.0 or higher, even if you have an older computer. Most recent PCs and Macs support USB 3. USB 3 drives will still work on older USB 2 ports, and it will "future proof" your next computer upgrade. USB 3 is a *lot* faster than USB 2. (Note that if you plan to use this drive with a newer Apple MacBook laptop, you'll need the connecting cable to have the smaller USB-C-type connector on the end that plugs into the laptop.)

- *Drive size:* I would plan to buy a drive that is at least twice the size of your computer's internal hard drive. If you're barely using all the space on your computer's hard drive, you can get away with a smaller backup drive, maybe one that is the same size as your internal drive. To check what size of hard drive you have inside your computer
 - *Windows:* Open File Explorer, and click "This PC." Look at the little bar graph under the drive icon to get the drive's size and total space used.
 - *Mac:* Open the Apple menu, and click "About this Mac." Then click the "Storage" tab. Look at the little bar graph under Macintosh HD to get the drive's size and total space used.

Note Many external drives come with bundled software, including backup software. In this book, I will walk you through using the free backup software that already comes with Windows and macOS, which is (in my opinion) your best option. If you decide to use the included backup software, then you can ignore the rest of the steps for this tip and just use the instructions that come with your hard drive. However, I strongly suggest you do *not* use the proprietary backup software. It often comes with all sorts of extra crap you don't need or want. Some drives come with a trial subscription for a cloud backup service, as well—often free or discounted to begin with, but of course the cost goes up later. Again, I would *not* use any software or service that comes with the external drive, unless by some miracle it comes with one of the services I recommend in the next tip.

Connect the Drive to Your Computer

Once you have the new shrink-wrapped hard drive box in your hands, open it up and take out the contents. The drive will almost surely come with some instructions for attaching the drive to your computer—a "quick-start guide" or similar. Follow these instructions for connecting the drive to your computer, but it's pretty straightforward: the USB cable can connect only one way. That is, the ends of the cable are different—one will connect to your computer (or USB hub), and the other will connect to the drive. Note that you should leave this drive connected to the computer so that the backup software can do its thing when it needs to. If you have a laptop, you should get in the habit of connecting this drive every night.

Note On a Mac, when you first plug in a new hard drive, you may get a system notification at the upper right that asks you if you want to use it for Time Machine. *Ignore this for now.* Just let the notification go away or close it explicitly.

Disconnecting the Backup Drive

You're not going to do this now, but for future reference, you should always "eject" a hard drive before disconnecting it from your computer. If you have a desktop computer, you will probably leave this backup drive connected all the time. But if you have a laptop, you'll going to want to disconnect this drive whenever you go mobile. Here's how to safely disconnect a drive:

- *Mac:* Right-click the drive with your mouse, and select "eject." Wait until the icon disappears.
- *Windows:* Click the "Safely Remove Hardware" icon in your taskbar at the lower right. Choose the proper "eject drive" option, and wait for the notification that it's safe to disconnect it.

Configure Your Backup

How you configure your backups will differ depending on your operating system type and version. Be sure that your new external hard drive is connected properly before continuing.

Tip 4-2a. Windows 11

1. Make sure your new external hard drive is attached. For this example, my drive is called "BACKUP."
2. Using the technique we discuss in the previous tip, search your PC for "file history" and open this control panel. You should see something like Figure 4-13, which should show your connected external drive. If you don't see the correct drive, click "Select drive" at the left side of the settings window to choose the correct backup drive.

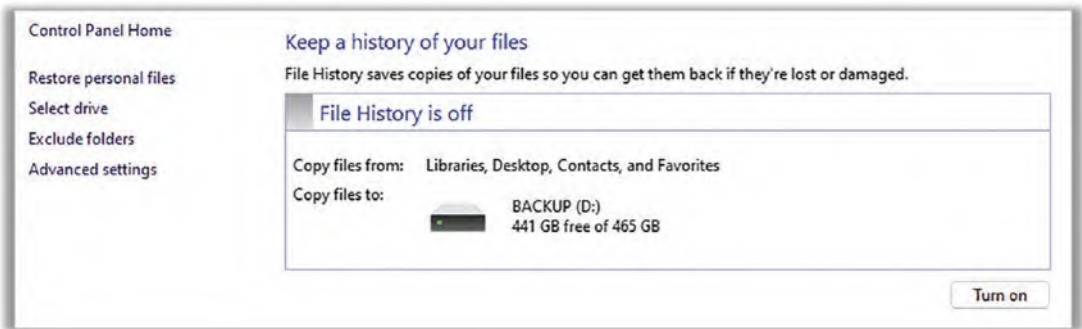


Figure 4-13. Windows 11 File History

3. At this point, simply click the “Turn on” button. This dialog should now look like Figure 4-14.

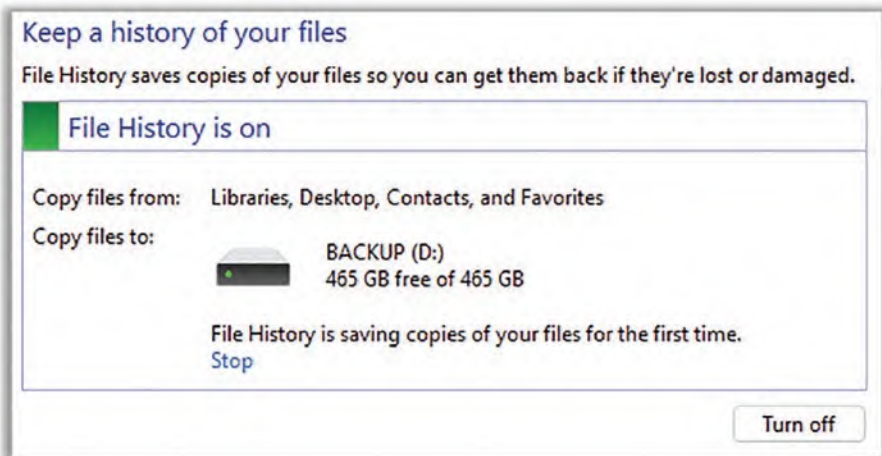


Figure 4-14. Windows 11 File History enabled

4. There are advanced settings, but I would just use the defaults (hourly backup, keep saved versions forever). Note that Windows 11 has a default set of files and folders that it backs up (Documents, Music, Pictures, Videos, and Desktop). While you can exclude some folders, you have to do some weird stuff to include custom folders. I won't cover that here.

Tip 4-2b. Windows 10

1. Make sure your new external hard drive is attached. For this example, my drive is called “BACKUP.”
2. Using the technique we discuss in the previous tip, search your PC for “backup settings” and open this system setting. You should see something like Figure 4-15.

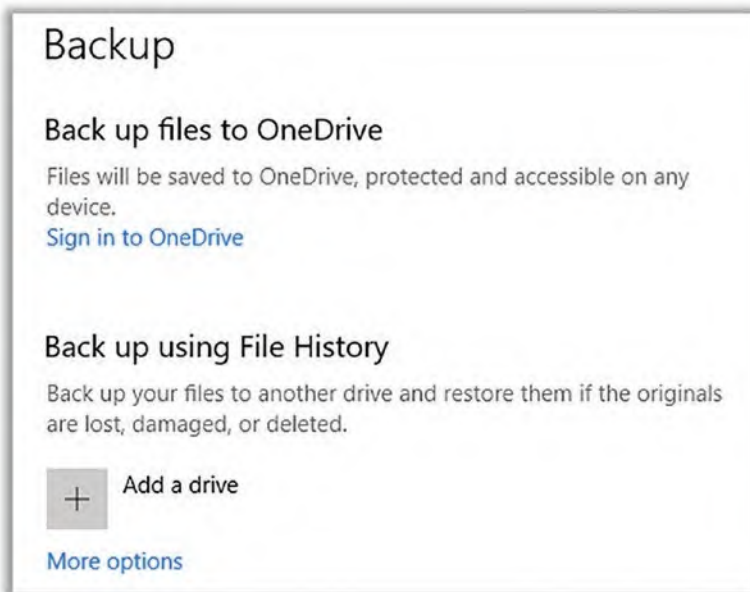


Figure 4-15. *Windows 10 Backup*

3. Now click the “Add a drive” button and add your backup drive. You should now see something like Figure 4-16.

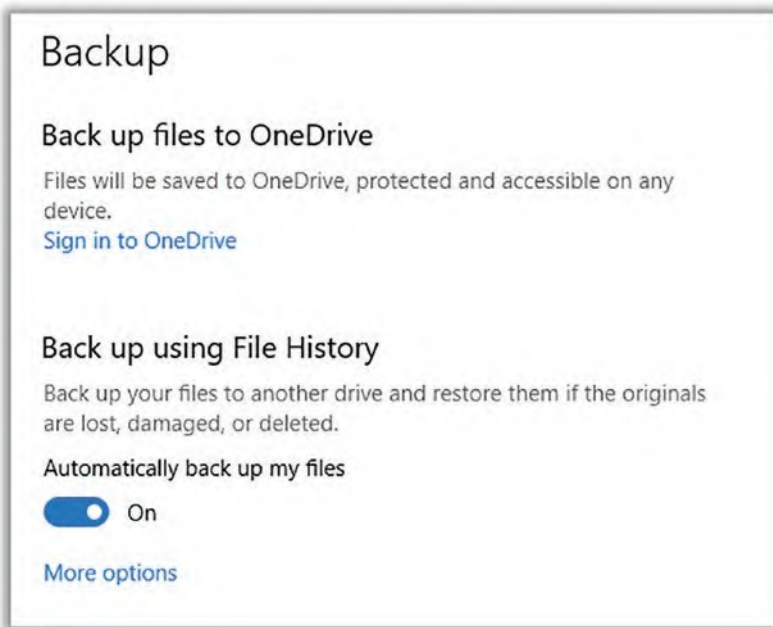


Figure 4-16. *Windows 10 Backup enabled*

4. By default, this will back up the cover all user folders (Documents, Music, Pictures, Videos, and Desktop). You can add more folders by clicking “More options” and then “Add a folder.” (Note that you can’t do this on Windows 11.) There are other advanced settings here, but I would just use the defaults (hourly backup, keep saved versions forever).

Tip 4-2c. macOS Ventura

Setting up backups on a Mac is pretty easy. At this point you should have your new drive plugged in and ready to go. You should see the drive on your Mac desktop. For this exercise, my drive is named “BACKUP.”

Open System Settings and search for “Time Machine.” You should see it on the right side, like in Figure 4-17.



Figure 4-17. macOS Ventura Time Machine preferences

Click the box for “Add Backup Disk.” If necessary, enter your admin credentials. You should then see a little dialog asking you to set up the disk with your backup disk selected (Figure 4-18). If you see more than one option here, be SURE you’ve selected the correct backup drive—whatever drive you select will be completely erased!

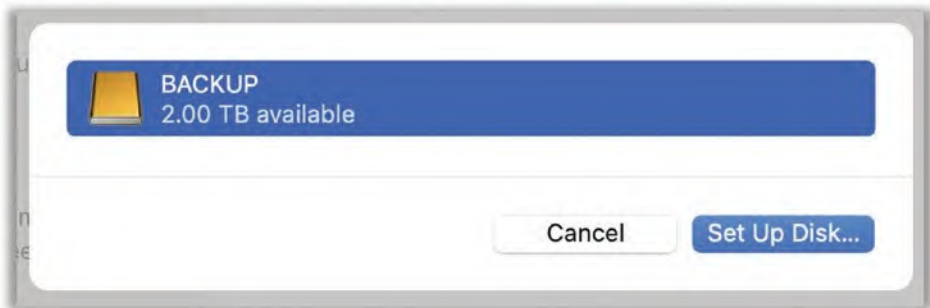


Figure 4-18. macOS Ventura Set up time machine disk

You will now need to choose a password for the drive encryption. Unfortunately, Apple seems to have removed a helpful built-in utility for generating secure passwords called Password Assistant. I have no idea why—maybe they’ll bring it back. In the next chapter,

you'll learn how to generate killer passwords, but that doesn't help us here. For now, let's use a password generator from BitWarden⁸:

<https://bitwarden.com/password-generator/>

Check the “all characters” option and then drag the little slider until the password is at least 20 characters long (Figure 4-19). When done, you can click “Copy Password.”

Password Generator

Need a strong password? Try the Bitwarden Password Generator to create complex passwords that will keep your information safe.

Your password's score: **strong**

Estimated time to crack: **centuries**

Trpb@^sDv!NN4#UZX!X7

Copy to Clipboard **Regenerate**

Type

☒ Password

☐ Passphrase

Characters: 20

Additional Options

☒ A-Z ☒ 0-9

☒ a-z ☒ !@#%&*

Figure 4-19. BitWarden Online password generator

⁸If you're already a BitWarden user, then you can just use the app or browser plug-in to do this.

SAVE THIS PASSWORD: If you lose it, *all the data will be lost*. If you happen to already be using a password manager, then save this password there in a secure note with a helpful title like “Time Machine backup password”; otherwise, *carefully* write this password on a piece of paper and put it somewhere safe.

When done, paste this new password into the Time Machine password fields (Figure 4-20). You can also give yourself a nice hint of where to find this password—I suggest you use it.

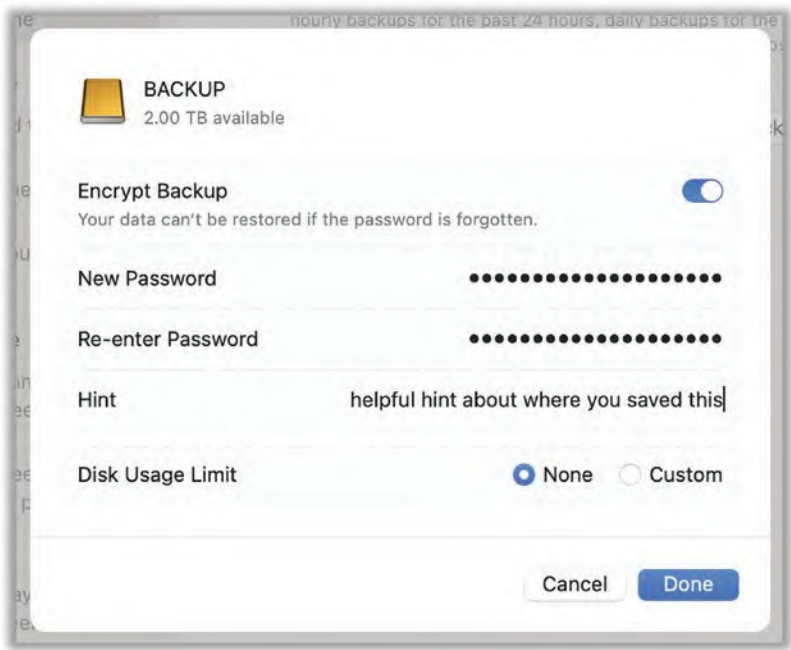


Figure 4-20. macOS Ventura Encrypt backup disk

Click the “Encrypt Disk” button—macOS will then prepare your drive for Time Machine and start your first backup. You will see a progress window like the one in Figure 4-21. You can close this window at any time; you don’t have to wait for the backup to finish. That’s it; you’re done!



Figure 4-21. *macOS Ventura Time Machine backing up*

Tip 4-2d. macOS Monterey

Setting up backups on a Mac is pretty easy. At this point you should have your new drive plugged in and ready to go. You should see the drive on your Mac desktop. For this exercise, my drive is named “BACKUP.”

1. Open System Preferences and search for “Time Machine.” Select this option and open it. It should look like Figure 4-22.

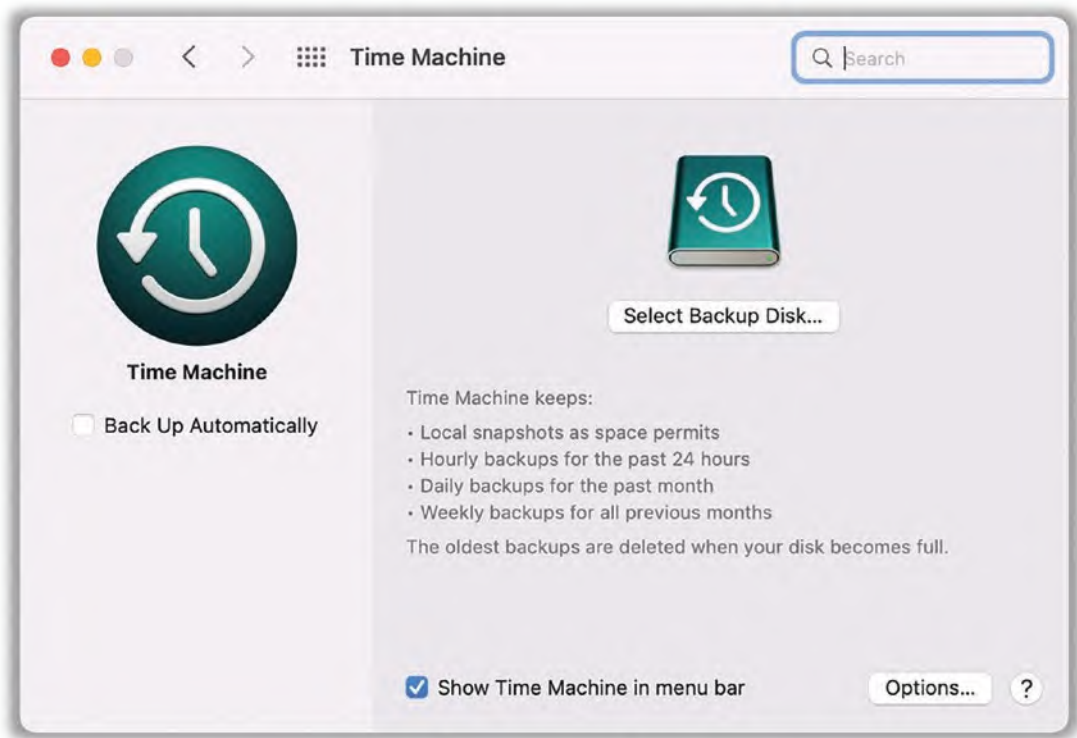


Figure 4-22. *macOS Monterey Time Machine preferences*

Check the box at the left for “Back Up Automatically,” which will bring up a dialog asking you to choose your backup drive (Figure 4-23). Check the box at the bottom for “Encrypt backups” and then click the “Use Disk” button. You may be warned that the drive will be completely erased. It’s a new drive, so there’s nothing to lose here—it’s safe to do this.

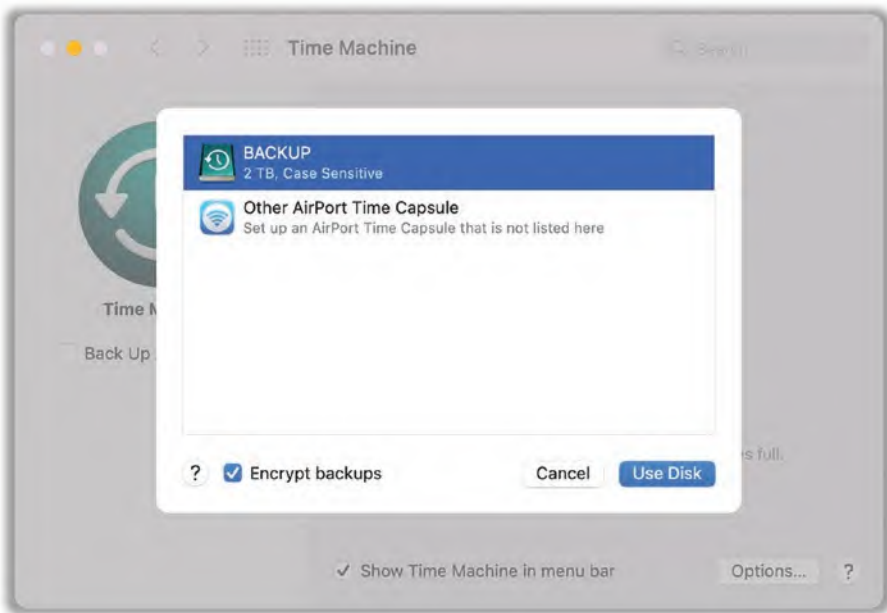


Figure 4-23. macOS Monterey Select backup disk

You will now need to choose a password for the drive encryption (Figure 4-24).

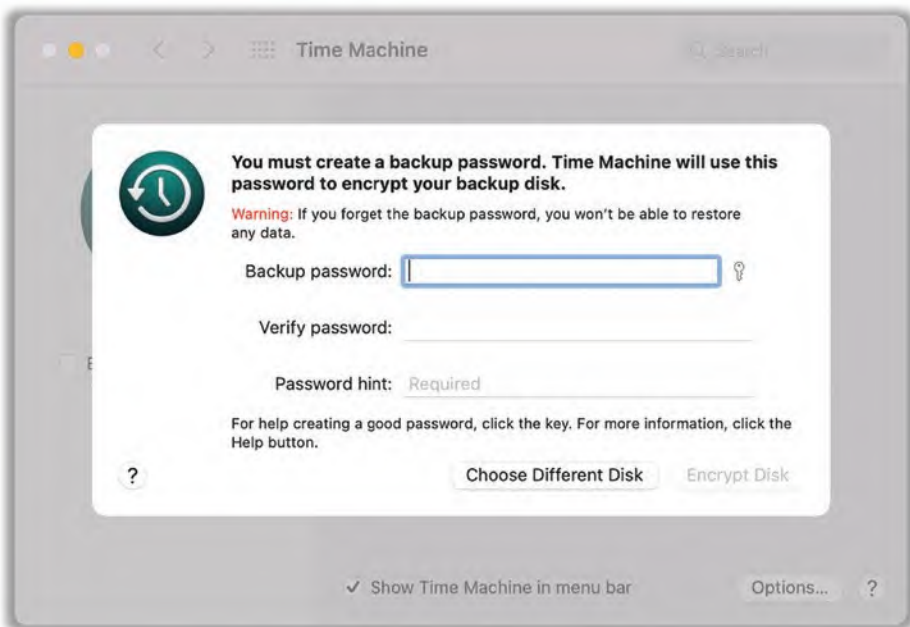


Figure 4-24. macOS Monterey Choose backup password

Thankfully, macOS comes with a great little utility for generating secure passwords called Password Assistant.⁹ Click the tiny little key icon to the right of the “Backup Password” text box. This will bring up a password generator. Drag the little slider until the password is at least 20 characters long (Figure 4-25).

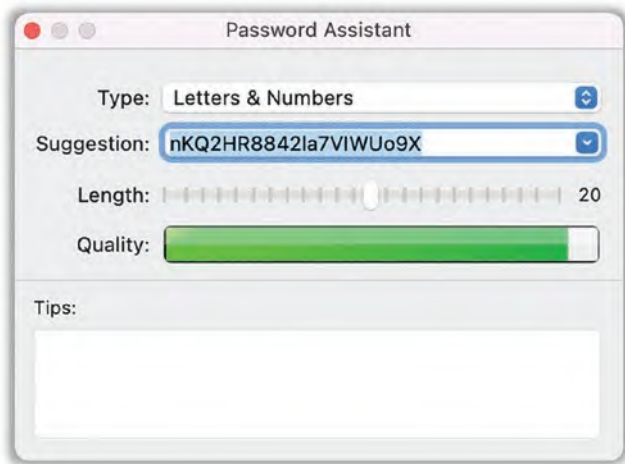


Figure 4-25. macOS Monterey Password generator

⁹It seems to have removed this in macOS Ventura for some reason. Maybe they’ll bring it back.

SAVE THIS PASSWORD: If you lose it, *all the data will be lost*. If you happen to already be using a password manager, then save this password there in a secure note with a helpful title like “Time Machine backup password”; otherwise, *carefully* write this password on a piece of paper and put it somewhere safe. Close the Password Assistant window—macOS will automatically fill in the generated password (Figure 4-26). You’ll need to jot down a short note for the password hint—I’d write down where you saved the password.

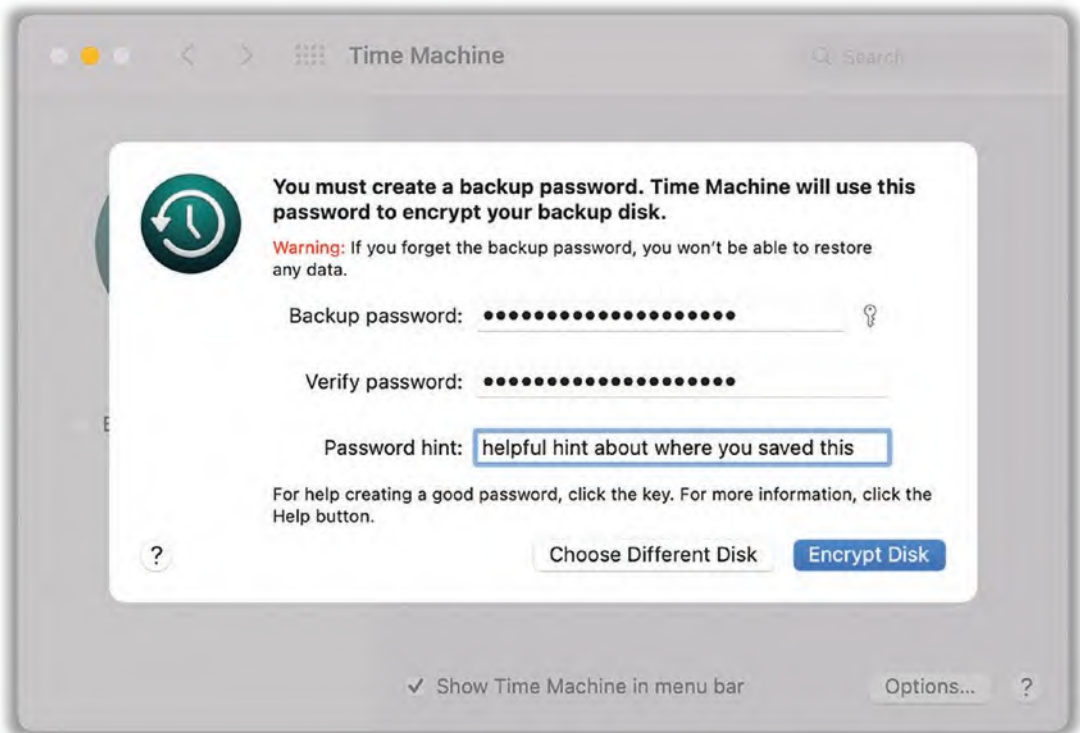


Figure 4-26. macOS Monterey Encrypt backup disk

Click the “Encrypt Disk” button—macOS will then prepare your drive for Time Machine and start your first backup. You will see a progress window like the one in Figure 4-27. You can close this window at any time; you don’t have to wait for the backup to finish. That’s it; you’re done!

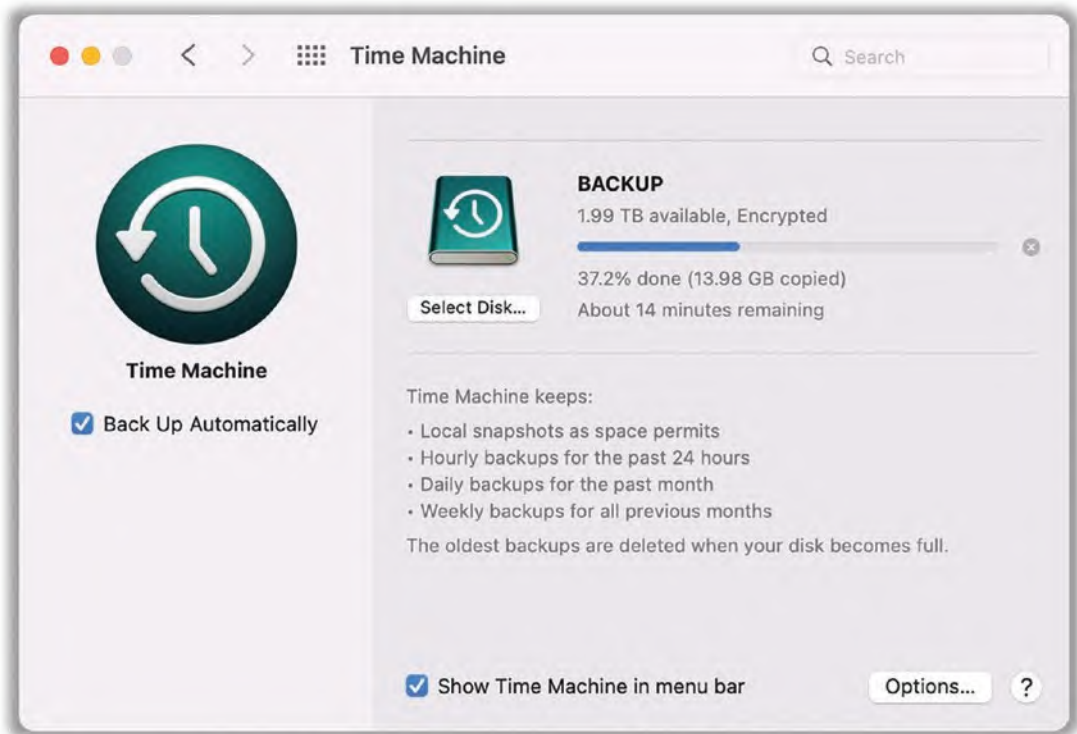


Figure 4-27. macOS Monterey Time Machine backing up

Tip 4-3. ★ Back Up to the Cloud

Recommending a specific cloud backup service is difficult. The features and prices for online backups are changing all the time. This is good because the features are increasing and the prices are decreasing. But trying to do a cost-benefit analysis when the costs and the benefits are in a constant state of flux is like trying to hit a moving target.

Any cloud service worth mentioning will come with full encryption of your data in transit and while stored on their servers. But few cloud services will allow you to control the keys for that encryption, meaning that the service provider would be able to access your data, if they were served a warrant or if a rogue employee wanted to go snooping around.

I've done a good bit of research and there are two main options that I can recommend: iDrive and Backblaze. There's one key difference: iDrive has limited storage but unlimited devices; Backblaze has unlimited storage but only for a single device. I have many, many devices—but I only have one main computer that contains the stuff I want to back up. The other computers access a subset of my key files using a file syncing service (which I'll discuss in Chapter 10). The base pricing between the two is very similar—about \$70/year. Backblaze is a little easier to use, but iDrive has better privacy. For this book, I'm going to choose Backblaze, but iDrive is a great option if it makes more sense for you.¹⁰

iDrive and Backblaze work much the same way: you sign up for an account, and then download and install their software. When you run their app for the first time it will walk you through configuring your backups. Then it just silently does its thing in the background, and you never have to worry about it again, unless you need to restore something.

Tip 4-3a. Windows

In this section, I'll be showing Windows 11 screenshots, but Windows 10 should look almost identical.

1. Go to the following website and select “Personal Backup” at the top. Select the free trial option and create your account. The installer should automatically download.

<https://www.backblaze.com>

¹⁰This article does a good comparison, though their scoring system doesn't really show how close these two really are. Both have 4.5 stars, but the “score” is 2 vs. 6 points: <https://www.cloudwards.net/idrive-vs-backblaze/>

Find the installer in your Downloads folder. Right click it and select “Run as administrator” (Figure 4-28).

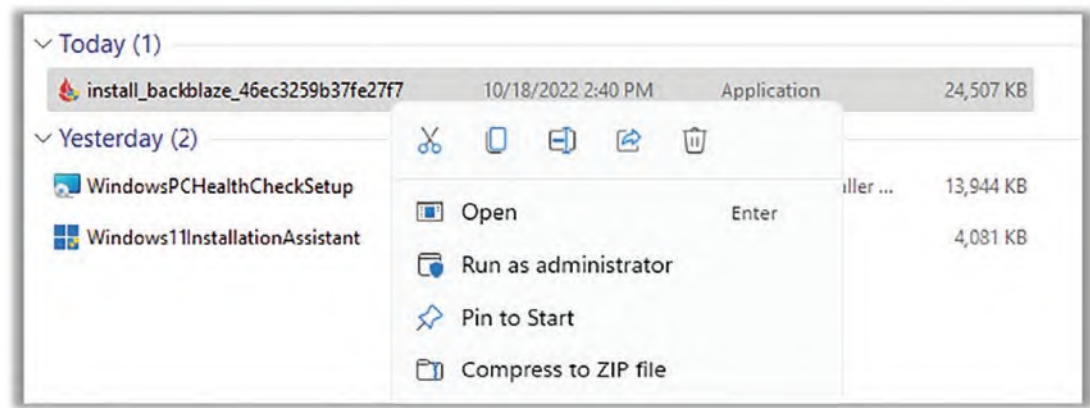


Figure 4-28. Windows 11 Run Backblaze installer as administrator

In the next window, click “Install Now.” See Figure 4-29.

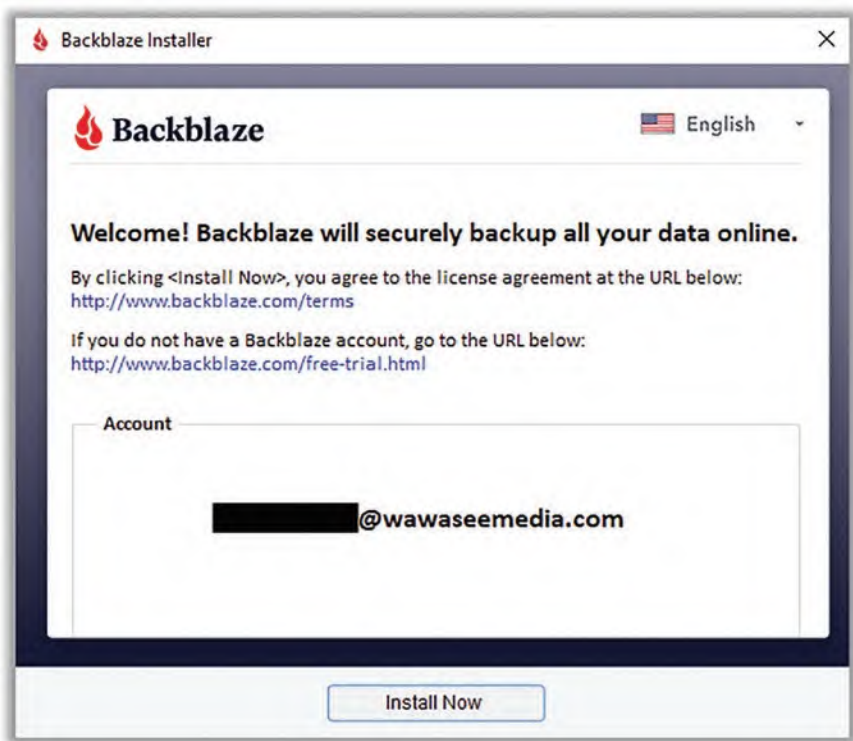


Figure 4-29. Windows 11 Backblaze install now

Backblaze will then analyze your drive, which may take some time. Let it complete this process. When the install is complete, simply click “Okay” (Figure 4-30).

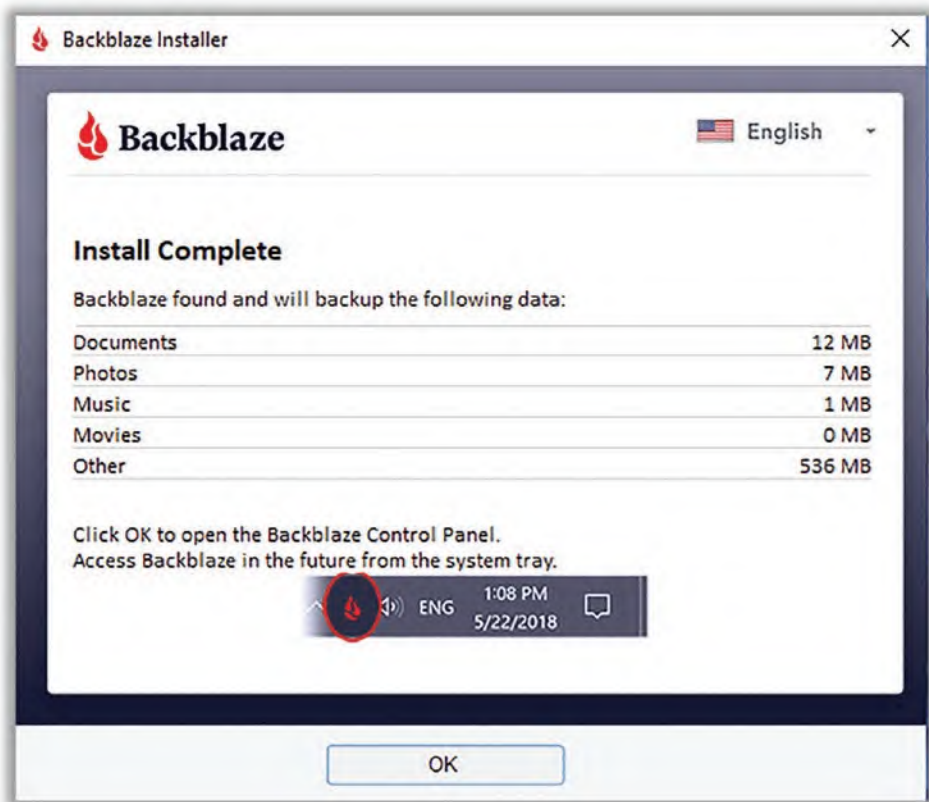


Figure 4-30. Windows 11 Backblaze install complete

At this point, Backblaze will automatically begin backing up all of your files. There should be a little flame icon in your system tray at the lower right. If you open Backblaze from there, you'll see something like Figure 4-31. If you decide to stick with the service, you will eventually give them your credit card or other payment information.

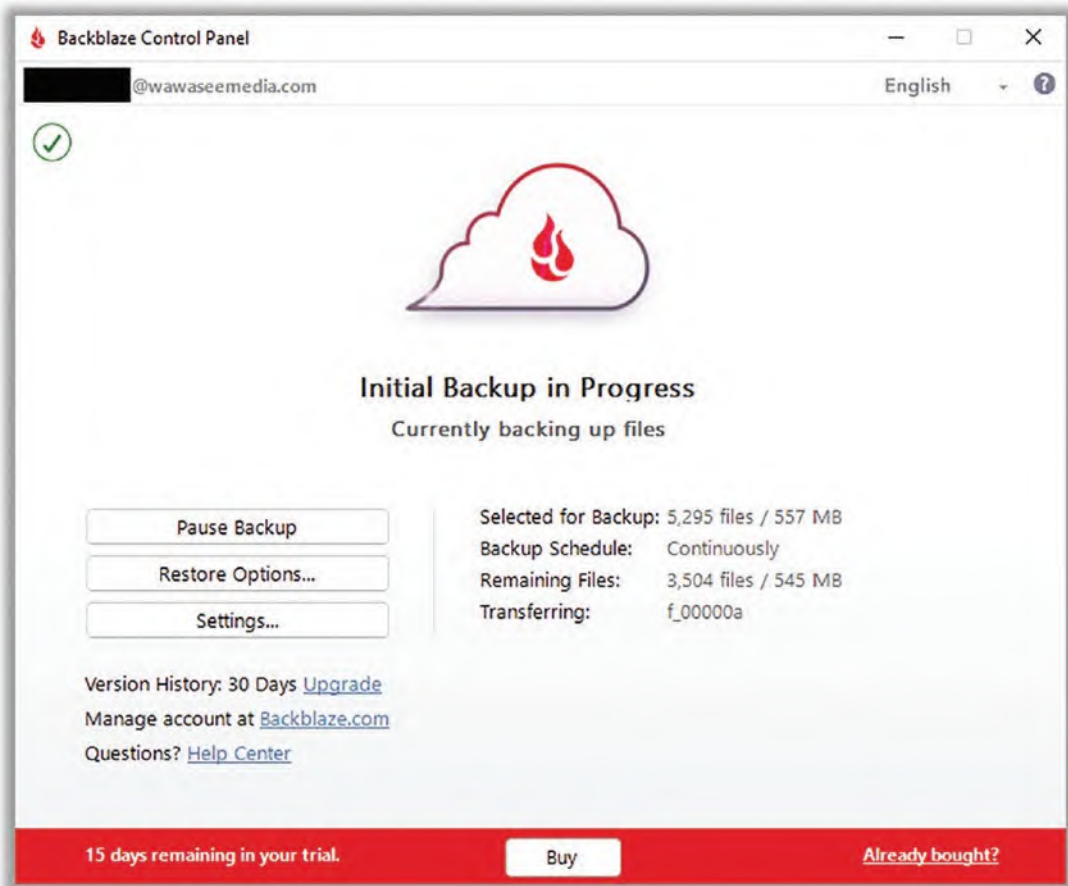


Figure 4-31. Windows 11 Backblaze information

Backblaze has several settings, but in most cases, you can simply accept the defaults which will back up all the data for the current computer user (documents, photos, music, etc.). However, one option you might want to seriously consider is setting a private encryption key (on the Security tab in Settings; see Figure 4-32). Even though your files will be encrypted in

the cloud, Backblaze will have the key. If you lock your files with your own encryption key, Backblaze will not have access to your files...with one major caveat: if you need to restore files, Backblaze will ask you to give them this key. They pinky swear not to keep it, but this is pretty dumb and it's the one privacy flaw for this service. Still, I would do this.

If you already use a password manager (or if you want to use the BitWarden online password generator mentioned in Tip 4-2c), use it to generate a killer password, enter it here as your “private encryption key,” and save this value as a secure note in your password manager. We'll cover password managers in the next chapter—you can return here to complete this step after your read that chapter.

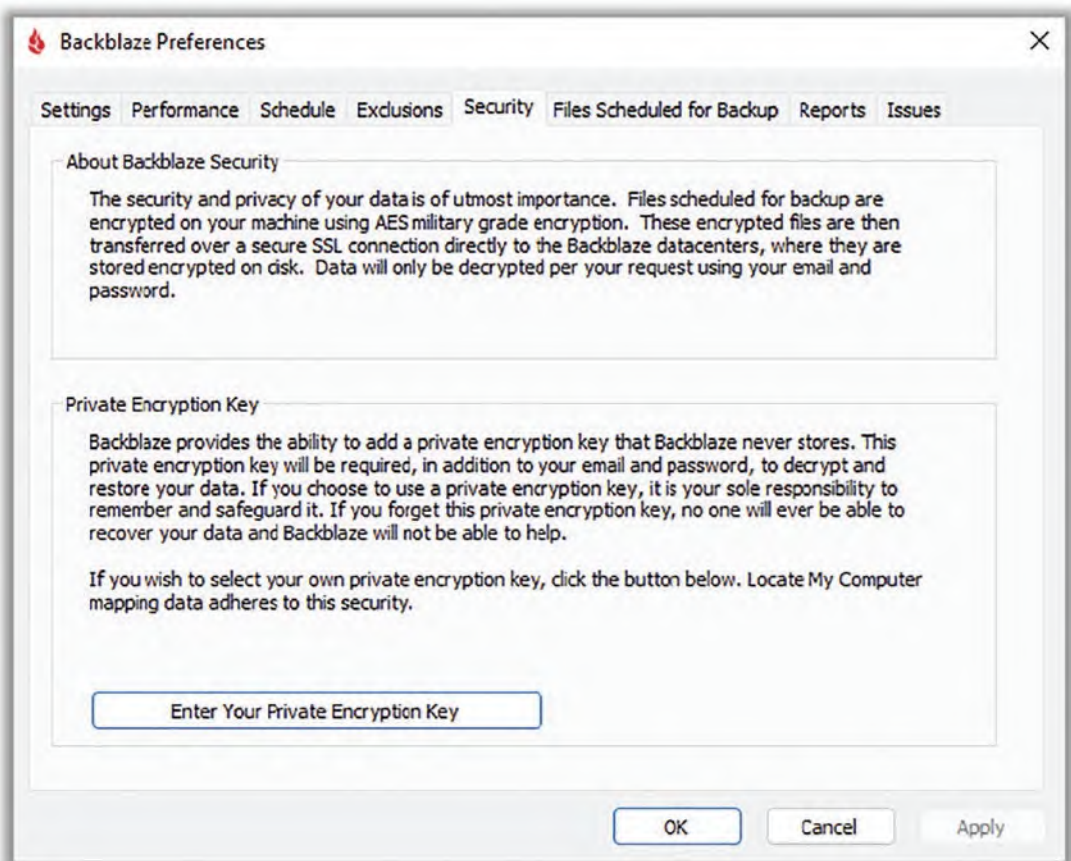


Figure 4-32. Windows 11 Backblaze private encryption key

Tip 4-3b. macOS Ventura

Note Macs have some built-in security features that will require you to jump through some hoops when installing apps like Backblaze. This is a good example of the trade-off between convenience and security that we talked about. Honestly, this is the trickiest part of the entire process, but I'll walk you through it.

1. Go to the following website and select “Personal Backup” at the top. Select the free trial option and create your account. Then download the installer (this may happen automatically).

<https://www.backblaze.com>

Open the installer “.dmg” file, and then run the “Backblaze Installer.” See Figure 4-33.

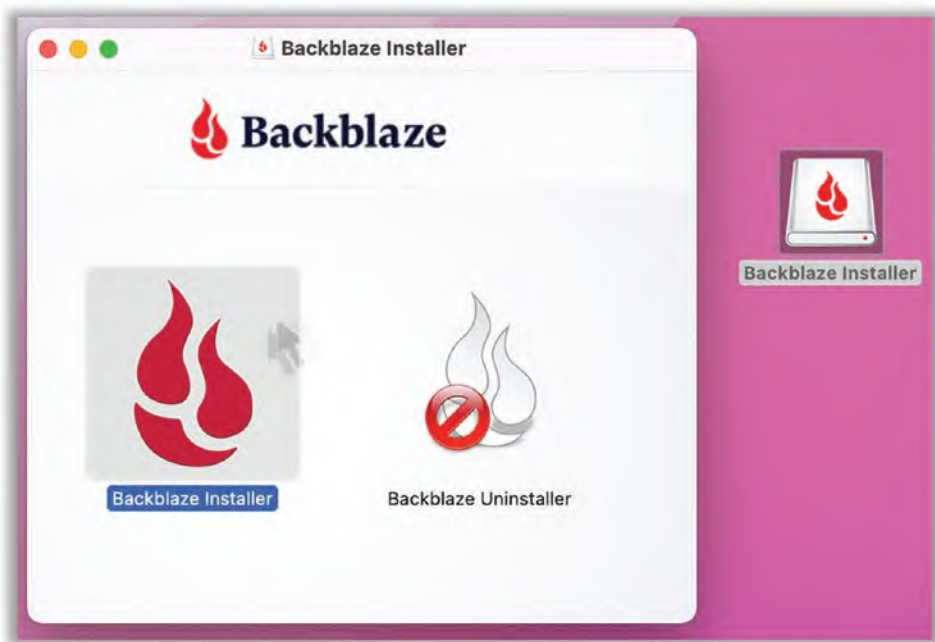


Figure 4-33. macOS Ventura Backblaze installer

Your Mac may ask you if you're sure you want to open this—click “Open.” It may ask you if you want to allow the installer to access files—say yes to all. Then click “Install Now.” See Figure 4-34.

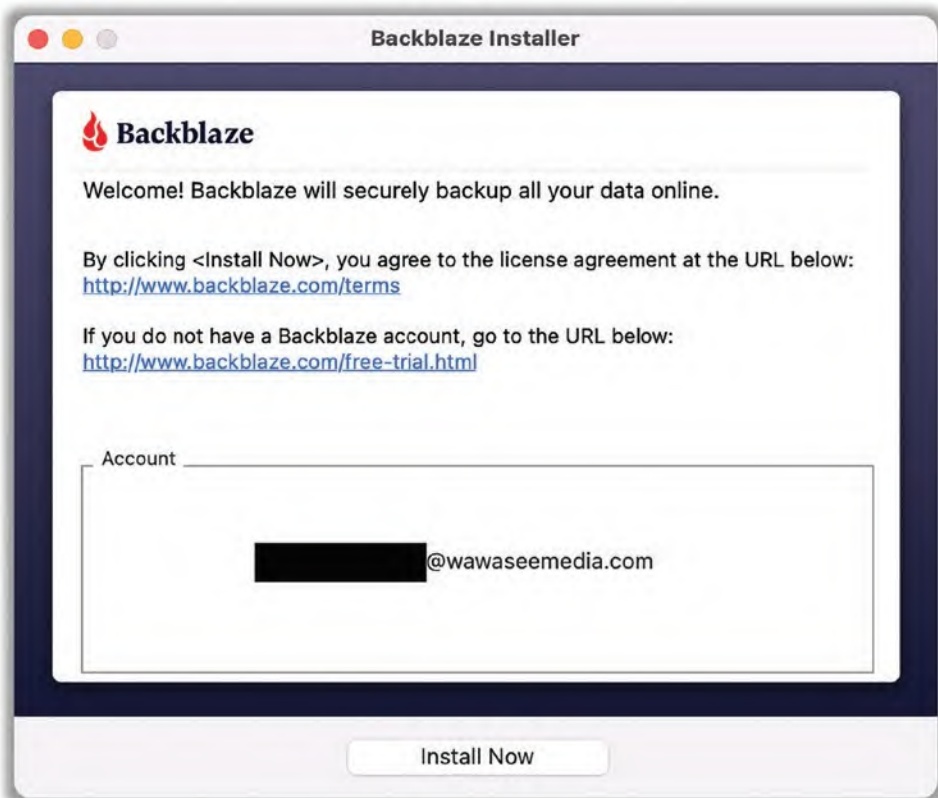


Figure 4-34. *macOS Ventura Backblaze install now*

Backblaze will then analyze your drive, which may take some time. Let it complete this process.

When this is over, you may be asked to grant “full-disk access” to Backblaze. For this service to back up your files, it will need to have this permission. Now, it will tell you to drag the Backblaze icon from your Applications folder to your Full Disk Access settings window with a nifty animation (Figure 4-35). However, you shouldn’t actually need to do that for macOS Ventura; it should already be listed there; you just need to enable it. So ignore this.

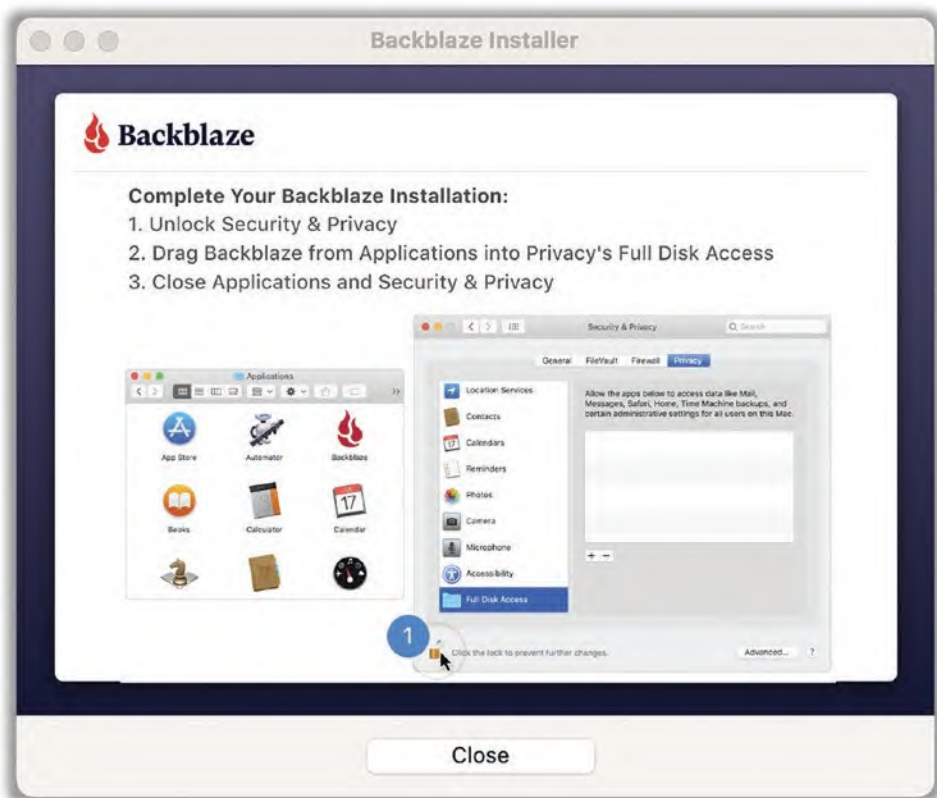


Figure 4-35. macOS Ventura Backblaze animation

Click the button that says “Open Applications Folder and System Settings”¹¹ (not shown; this is a separate window). This will do precisely that: open your system settings and also open your Applications folder. You can close the Applications folder and focus on the System Settings window for Full Disk Access (Figure 4-36). Click the slider next to Backblaze to enable Full Disk Access, and then close System Settings. Finally, click the “Close” button on the pop-up window (Figure 4-35).



Figure 4-36. *macOS Ventura Full Disk Access settings*

¹¹ Note that Backblaze’s installer was a little behind the times when I captured these screenshots and followed their installation process—they didn’t seem to be updated for Ventura. So unfortunately, these steps may change a little by the time you read this. But follow along anyway—the important information and steps should be correct.

At this point, Backblaze will automatically begin backing up all of your files. There should be a little flame icon in your menu bar. If you open Backblaze, you'll see something like Figure 4-37. If you decide to stick with the service, you will eventually give them your credit card or other payment information.

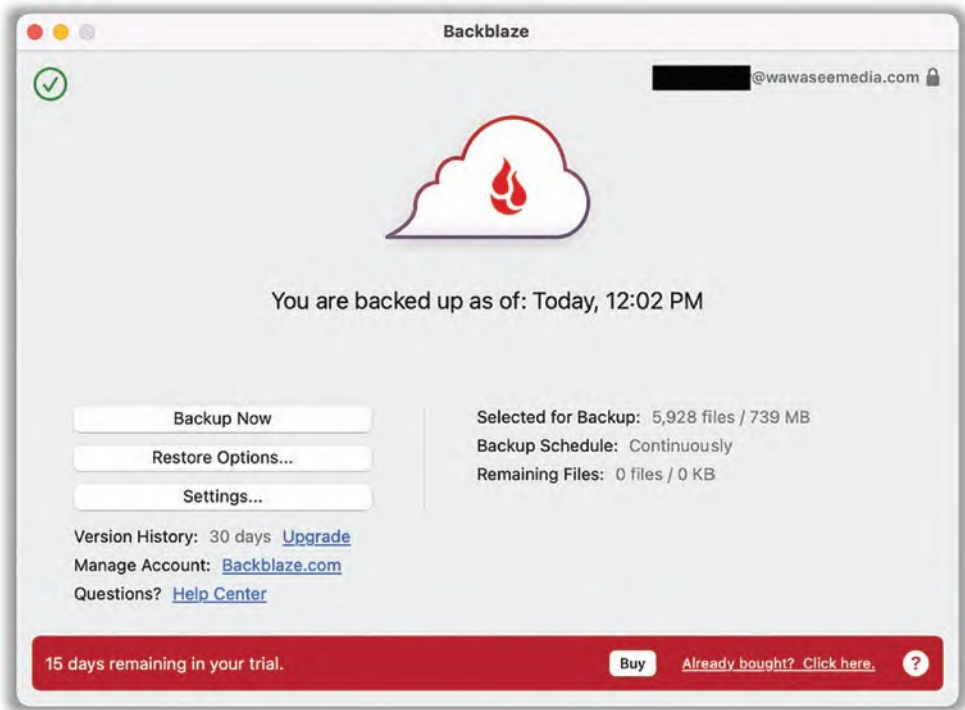


Figure 4-37. *macOS Backblaze information*

Backblaze has several settings, but in most cases, you can simply accept the defaults which will back up all the data for the current computer user (documents, photos, music, etc.). However, one option you might want to seriously consider is setting a private encryption key (on the Security tab in Settings; see Figure 4-38). Even though your files will be encrypted in the cloud, Backblaze will have the key. If you lock your files with your own encryption key, Backblaze will not have access to your files...with one major caveat: if you need to restore files, Backblaze will ask you to give them this key. They pinky swear not to keep it, but this is pretty dumb, and it's the one privacy flaw for this service. Still, I would do this. If you already use a password manager, use it to generate a killer password, enter it here as your "private encryption key," and save this value as a secure note in your password manager. We'll cover password managers in the next chapter—you can return here to complete this step after you read that chapter.

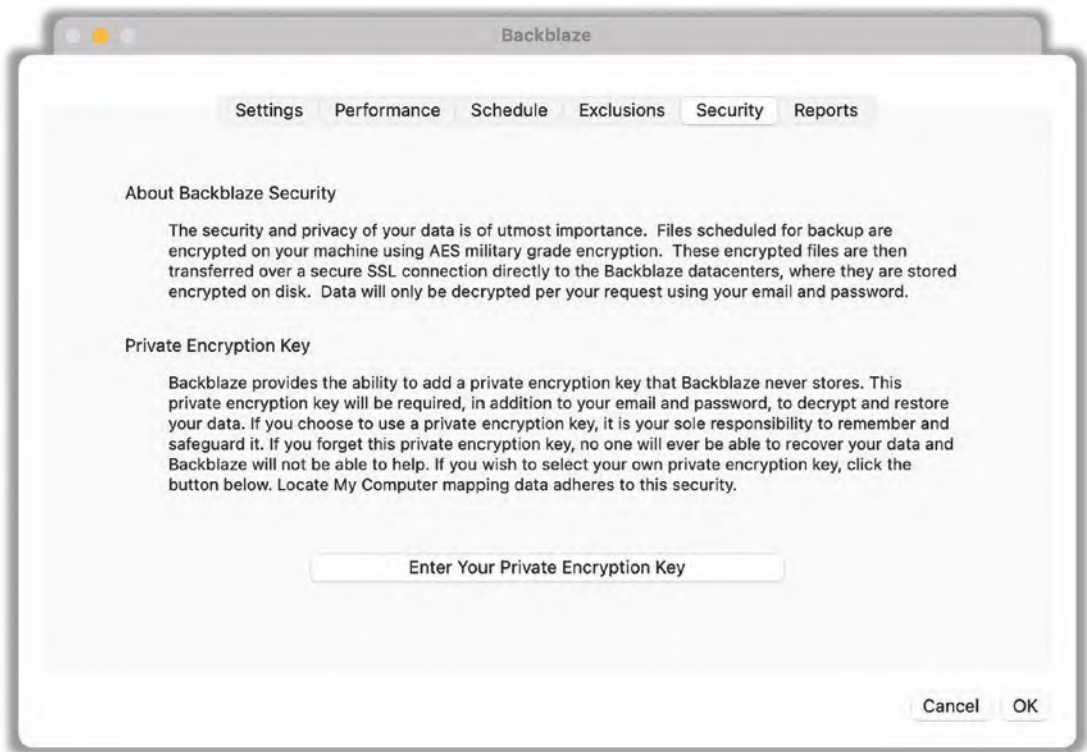


Figure 4-38. macOS Backblaze private encryption key

Tip 4-3c. macOS Monterey

Note Macs have some built-in security features that will require you to jump through some hoops when installing apps like Backblaze. This is a good example of the trade-off between convenience and security that we talked about. Honestly, this is the trickiest part of the entire process, but I'll walk you through it.

1. Go to the following website and select “Personal Backup” at the top. Select the free trial option and create your account. Then download the installer (this may happen automatically).

<https://www.backblaze.com>

Open the installer “.dmg” file, and then run the “Backblaze Installer.” See Figure 4-39.

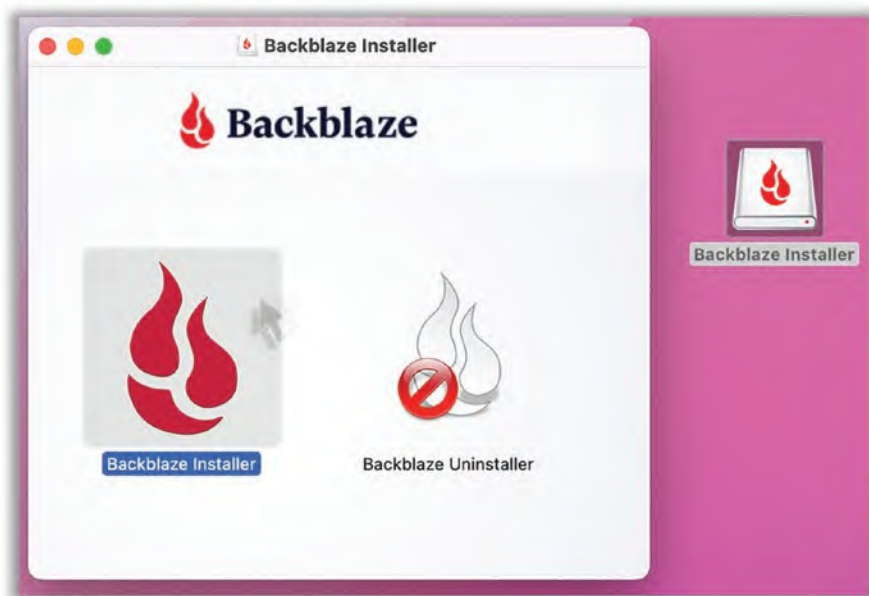


Figure 4-39. *macOS Backblaze installer*

Your Mac may ask you if you’re sure you want to open this—click “Open.” It may ask you if you want to allow the installer to access files—say yes to all. Then click “Install Now.” See Figure 4-40.

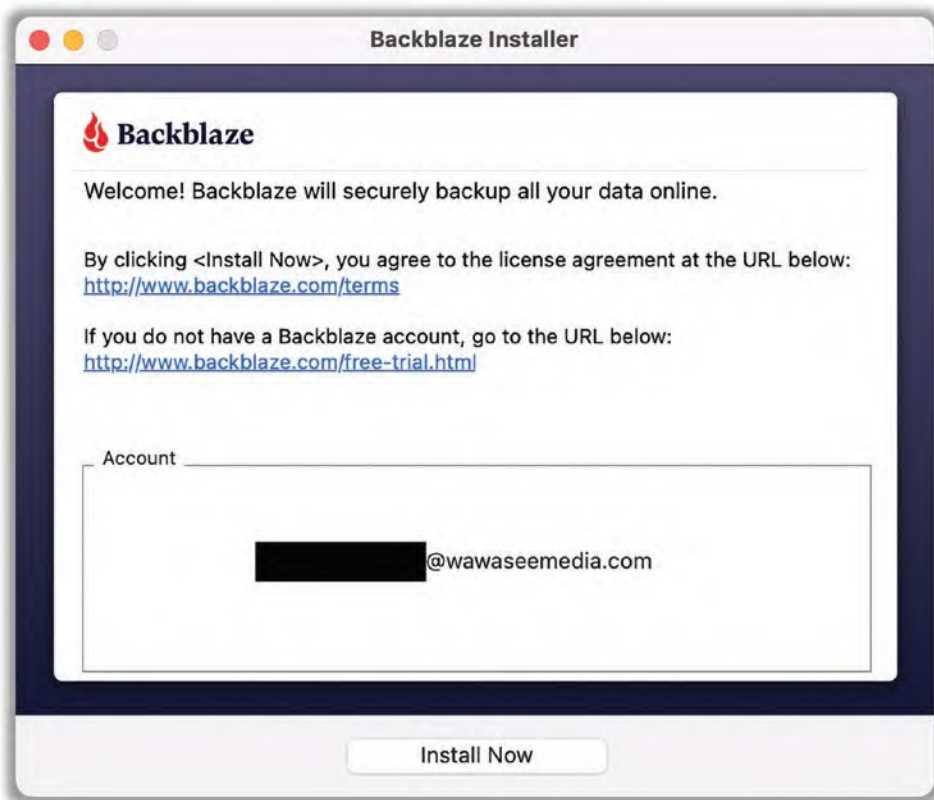


Figure 4-40. *macOS Backblaze Install now*

Backblaze will then analyze your drive, which may take some time. Let it complete this process.

When this is over, you may be asked to grant “full-disk access” to Backblaze. For this service to back up your files, it will need to have this permission. Watch the nifty little animation—you’ll be doing this shortly. Click the button that says “Open applications Folder and System Preferences” (macOS Monterey) or “Open Applications Folder and System Settings” (macOS Ventura). This will do precisely that: open your system settings and also open your Applications folder.

When the System Preferences window opens up, you may notice that it’s locked (see the lock icon in the lower left, Figure 4-41). To make changes to this setting, you’ll need to click the lock icon and then enter your computer account credentials or use Touch ID.

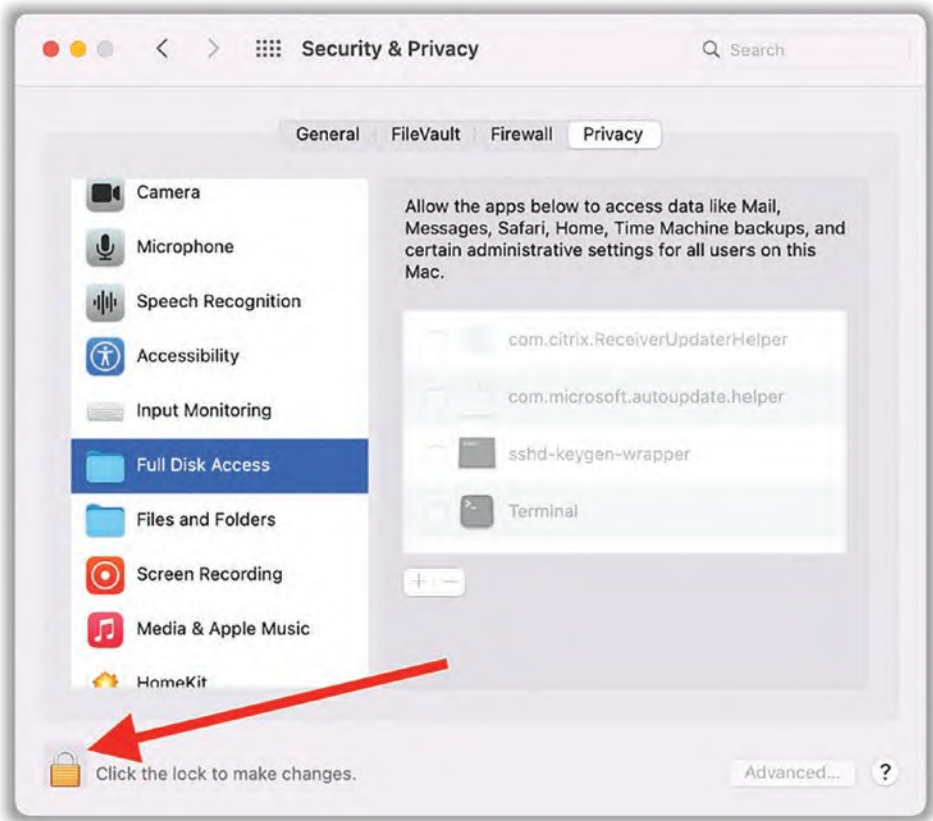


Figure 4-41. macOS Privacy settings unlock

The easiest way to give Backblaze the access it needs is to drag the application “Backblaze” from the Applications folder into the list of authorized applications under “Full Disk Access” (which should already be selected for you at the left, as shown). When done, you should see Backblaze listed there with a check mark (see Figure 4-42).

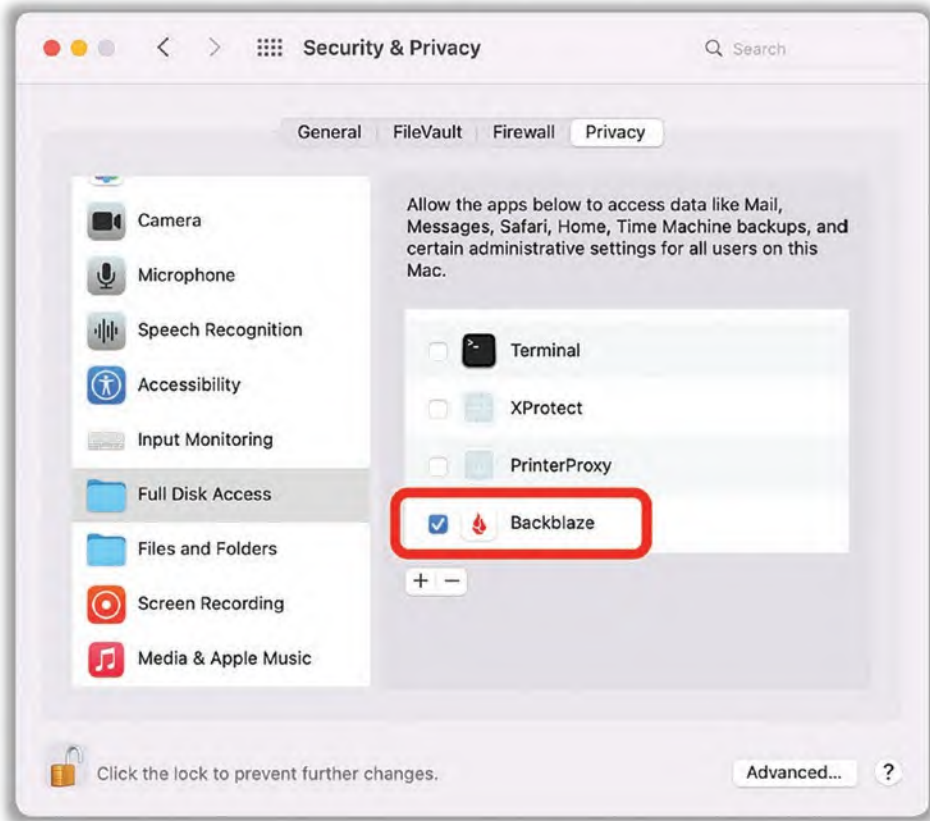


Figure 4-42. macOS Backblaze Full Disk Access granted

At this point, Backblaze will automatically begin backing up all of your files. There should be a little flame icon in your menu bar. If you open Backblaze, you'll see something like Figure 4-43. If you decide to stick with the service, you will eventually give them your credit card or other payment information.

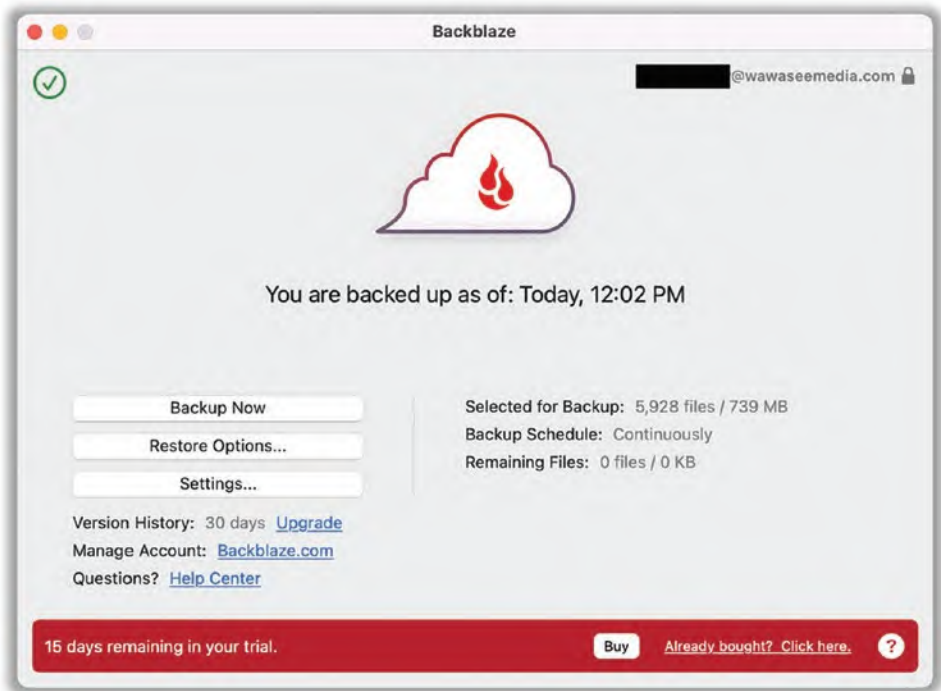


Figure 4-43. *macOS Backblaze information*

Backblaze has several settings, but in most cases, you can simply accept the defaults which will back up all the data for the current computer user (documents, photos, music, etc.). However, one option you might want to seriously consider is setting a private encryption key (on the Security tab in Settings; see Figure 4-44). Even though your files will be encrypted in the cloud, Backblaze will have the key. If you lock your files with your own encryption key, Backblaze will not have access to your files...with one major caveat: if you need to restore files, Backblaze will ask you to give them this key. They pinky swear not to keep it, but this is pretty dumb, and it's the one privacy flaw for this service. Still, I would do this. If you already use a password manager, use it to generate a killer password, enter it here as your "private encryption key," and save this value as a secure note in your password manager. We'll cover password managers in the next chapter—you can return here to complete this step after you read that chapter.

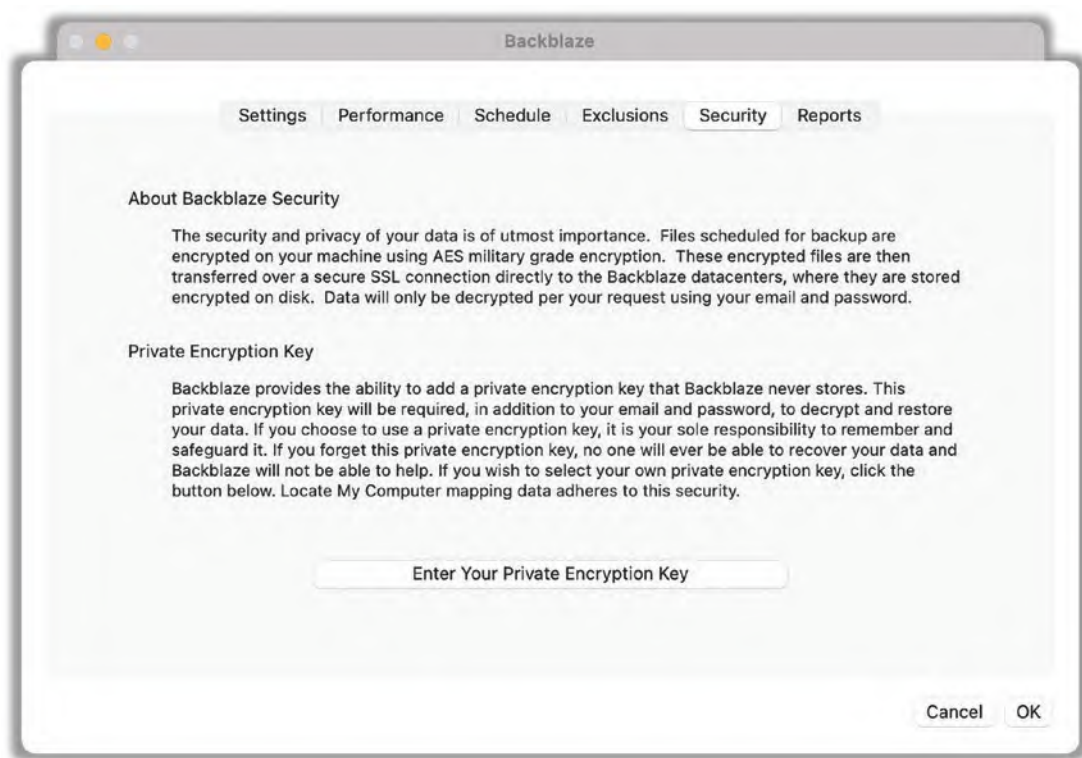


Figure 4-44. *macOS Backblaze Private encryption key*

Tip 4-4. Buy a UPS

If you have a desktop computer, you should seriously consider buying an uninterruptible power supply (UPS). (Laptops have built-in batteries and do not need this.) Most UPSs are just big batteries that sit between your computer and the AC wall outlet. Some are big, heavy lead-acid batteries (like the one in your car), and some are smaller, lighter Li-ion batteries (like in smartphones and laptops). When there's a power spike, glitch, brownout, or complete outage, the device provides juice to your computer from the battery.

Most UPSs have a separate data cable that allows it to talk to your computer so that if the power is out *and* the battery is running low, the UPS can tell your computer to shut down gracefully before power runs out. A UPS can be expensive, but suddenly cutting the power to a computer while it's running can cause real harm, including corrupting data on the hard drive.

Look for name brands like APC or CyberPower. Generally speaking, the more you spend, the bigger the battery—and the longer your computer can run without wall power.

However, for most of the protection benefits, you just need one that will smooth out the power glitches and give your computer a chance to shut down gracefully. If possible, buy a UPS that has automatic voltage regulation (AVR).

Tip 4-5. ★ Clean Up Your Apps

The goal of this step is to remove software you're not using. This includes utilities, games, and anything else you might have added over the years. All software has bugs, so the fewer apps you have installed, the lower your risk, statistically speaking.

I wouldn't remove any applications that were preinstalled with your operating system and that were made by Microsoft or Apple—I would focus on the ones that were intentionally installed, or the crapware that often comes preinstalled with Windows PCs. If you are unsure of what a particular application is or what it does, try searching the Web for more information. If you're not sure about any specific piece of software, just let it be. Though, even if you do accidentally delete something you need, you should be able to reinstall it.

Note Before uninstalling anything, exit all running applications. Some applications have strange interdependencies, and it's best to quit everything while you're uninstalling stuff. (If you're reading the electronic/digital version of this book on your computer, you can print off these few pages while you complete this tip.) If you want to be extra careful, restart your computer first, and then quit any applications that automatically start before uninstalling anything.

Tip 4-5a. Windows

Windows 11 and Windows 10 work very similarly. I will be showing you Windows 11 here.

1. Search settings for “add or remove programs,” and then select it.
2. Scroll through the list and get rid of any apps you no longer use or need. You can either click the three-dot menu next to the app (Windows 11, Figure 4-45) or click the app to select it (Windows 10, Figure 4-46), and then click “uninstall.”

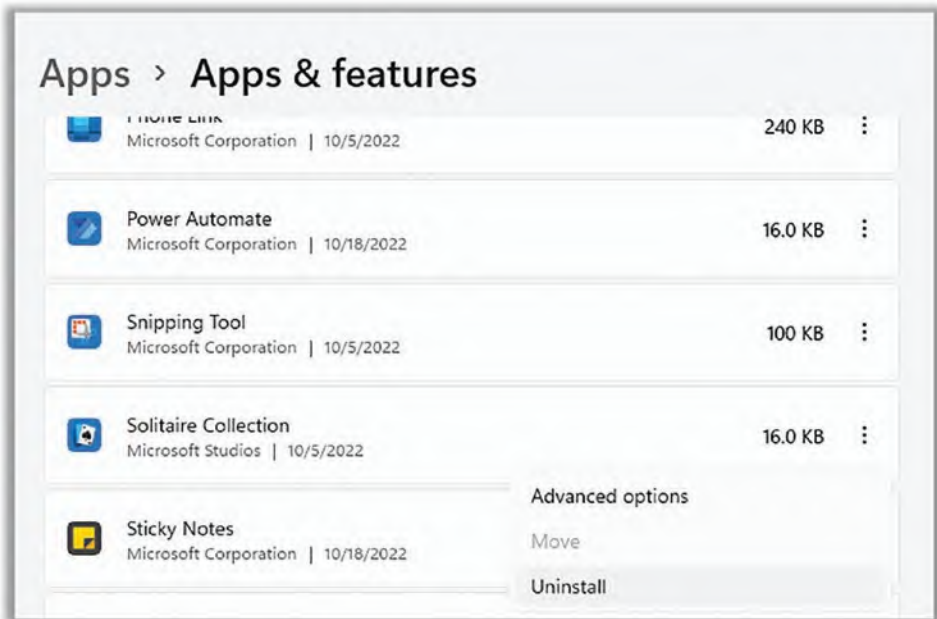


Figure 4-45. Windows 11 Add or remove programs

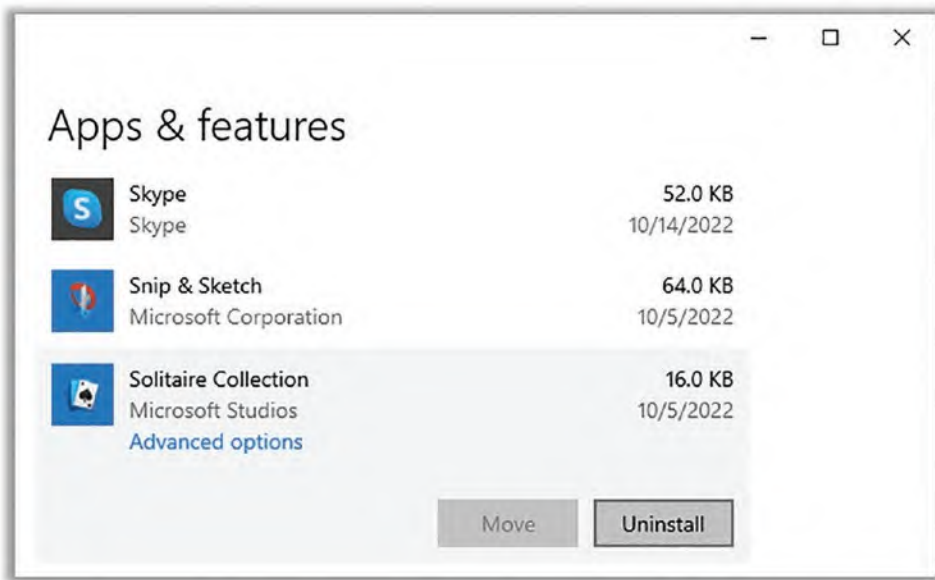


Figure 4-46. Windows 10 Add or remove programs

Scroll through the list of applications and uninstall any applications that you would like to remove. Some applications will launch a special, custom uninstaller application. In this case, just follow the instructions to remove/delete the application.

While not usually necessary, if you want to make sure to delete all remnants of an app, there's a nifty, free utility for Windows called Geek Uninstaller. Its whole job is to find extraneous files and folders that some apps leave behind. If you'd like to be squeaky clean, this app can help.

1. Download and install Geek Uninstaller (the free version).¹² You can find this application here:

<https://geekuninstaller.com/>

2. Launch Geek Uninstaller. You can scroll through the list of apps and uninstall the ones you no longer need or want. In many cases, this will do exactly what the built-in Windows "uninstall" will do, but it may find some other stuff lying around too (Figure 4-47).

¹² Note that as of this writing, there's a new Microsoft utility in beta called PC Manager for cleaning up your Windows PC. If this is available, I would use it over any third-party application, at least as a first pass.

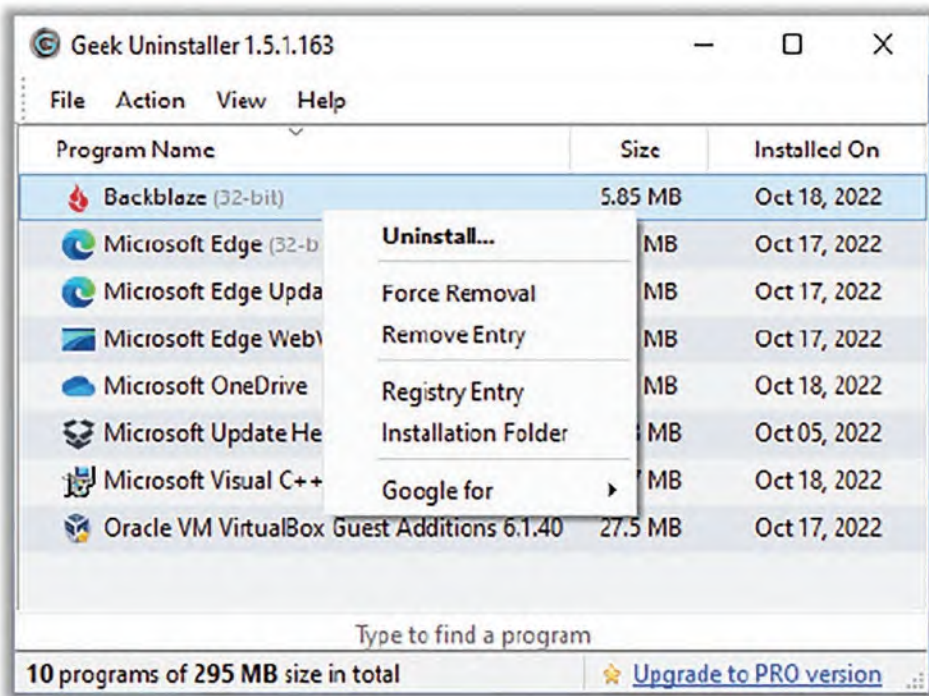


Figure 4-47. Geek Uninstaller

Note Microsoft is rumored to be launching a new “cleaner” utility called PC Cleaner.¹³ Keep your eye out for this application. It would make cleaning up your apps and getting rid of digital cruft easier on your Windows PC.

Tip 4-5b. macOS

In most cases you can simply drag unused applications to the Trash to delete them in macOS. Open your Applications folder and drag any apps you want to remove to the Trash icon in your Dock. You may have to enter your Mac credentials to approve the deletion.

¹³ <https://www.pcworld.com/article/1360140/microsoft-releases-beta-of-a-cleaner-style-pc-manager-tool.html>

There are a couple notable exceptions. Microsoft and Adobe apps are notorious for installing lots of extra crap and generally spreading roots throughout your Mac. For these apps, seek out the accompanying uninstaller utility to remove them (it's usually somewhere in the folder along with the main app).

While not usually necessary, if you want to make sure to delete all remnants of an app, there's a nifty, free utility for Mac called AppCleaner. Its whole job is to find extraneous files and folders that some apps leave behind. If you'd like to be squeaky clean, this app can help.

1. Download and install AppCleaner. You can find this application here:

<https://freemacsoft.net/appcleaner>

Drag and drop to delete them. Open the newly installed AppCleaner application. Then open your Mac's Application folder and simply drag and drop every app you want to delete onto this window where it says "Drop your apps here" (Figure 4-48). It will not only delete the app itself but find all the little extra files that the app may have scattered around. When you drop the app, it will show you all the files that it found and will delete.

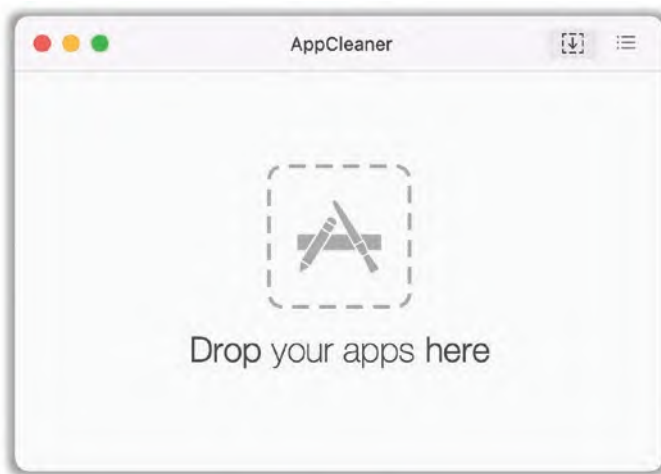


Figure 4-48. *macOS AppCleaner*

Tip 4-6. ★ *Turn on Auto-Update for Your OS*

Keeping your operating system up to date with the latest security fixes is crucially important. Thankfully, both Microsoft and Apple have mechanisms for automatically updating their operating systems—and they’re usually enabled by default.

Note that these OS auto-update mechanisms will only automatically install the “minor” updates, not major updates or upgrades that include big new features. They will notify you when these upgrades are available but will not install them without your explicit consent.

Tip 4-6a. Windows

Windows 10 and 11 Home versions will always automatically install OS updates for you—there’s no (officially supported) way to avoid this behavior. I’m not usually in favor of your operating system taking choices away from you, but in this case, I think it’s the right move. You can delay updates, but you can’t put them off forever.

You can verify this setting by searching for *windows update* in the system settings and opening the Windows Update Settings panel. It should look something like Figure 4-49, which shows the Windows 11 version—but it’s very similar in Windows 10.



Figure 4-49. *Windows 11 Windows update settings*

I would go further, however. Open the “Advanced Options” and enable the following settings (Figure 4-50).

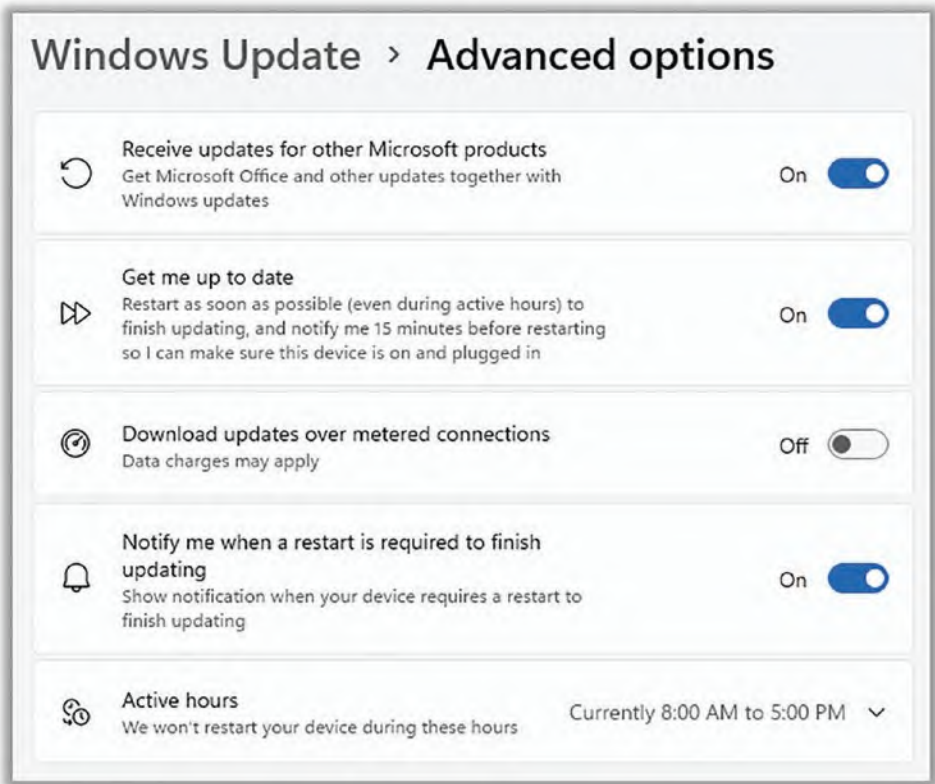


Figure 4-50. Windows 11 Windows update advanced options

The “Get me up to date” setting may be a bit much for some people. If you find it too annoying, you can disable that. You can also change the “active hours” here to reflect when you’re likely to be using the computer (and when you might not want it to automatically restart).

Tip 4-6b. macOS Ventura

1. Open System Settings and search for “software update,” and then select it (Figure 4-51).



Figure 4-51. macOS Ventura software update settings

2. Click the little “i” with a circle around it. Make sure all the settings are enabled (Figure 4-52).

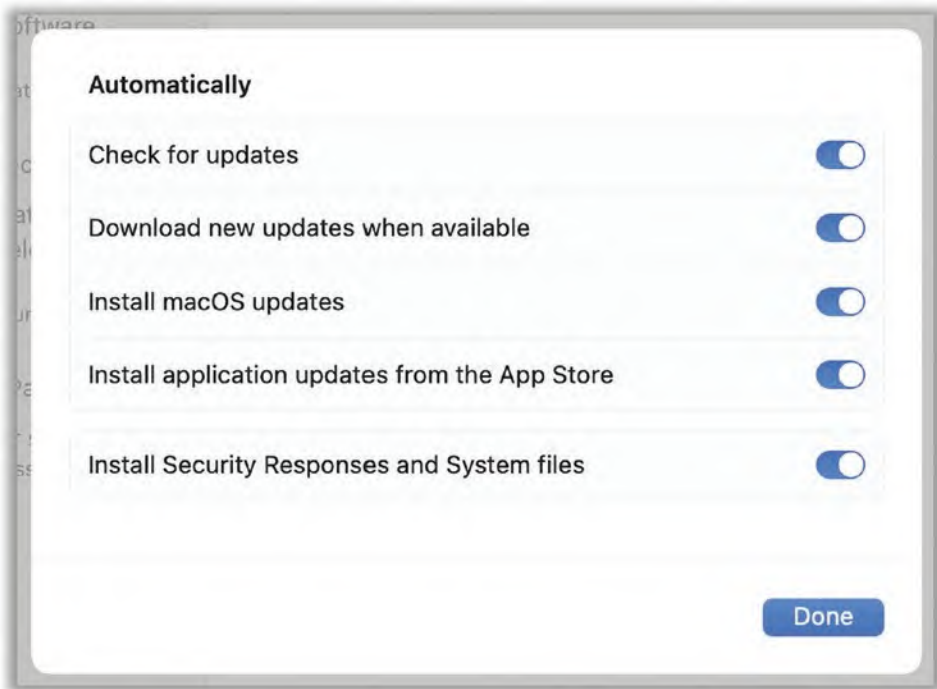


Figure 4-52. macOS Ventura software update options

Tip 4-6c macOS Monterey

Apple enables operating system updates by default, which I believe is the right call. You can verify these settings using the following steps.

1. Open System Preferences and search for “software update.” Select it.

Make sure “Automatically keep my Mac up to date” is enabled (Figure 4-53).



Figure 4-53. macOS Monterey software update

2. Click “Advanced” and make sure all the options are checked (Figure 4-54).

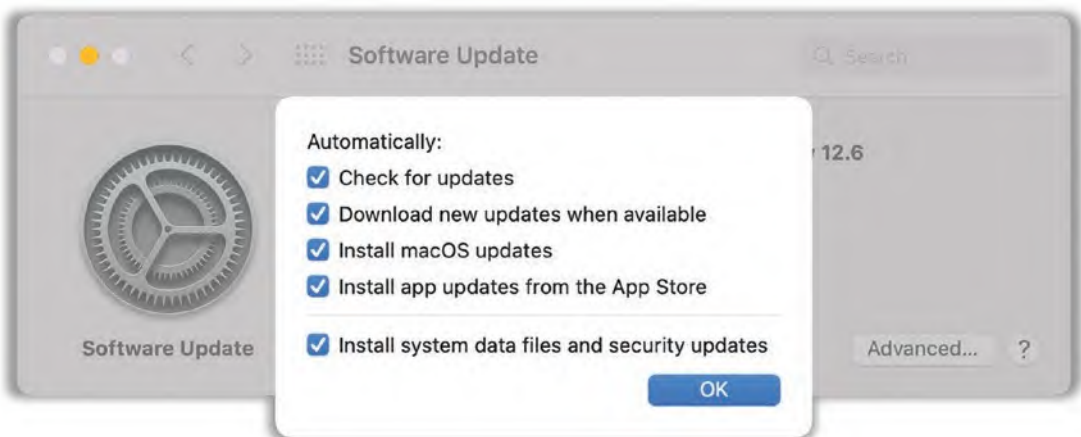


Figure 4-54. macOS Monterey software update advanced

Tip 4-7. ★ Turn on Auto-Update for Your Applications

Updating applications that you got from Apple's App Store or the Microsoft Store is simple and painless. Like with operating system updates, this mechanism will make sure to install security fixes as soon as they're available but will not perform major upgrades without asking you first.

If you installed an application by downloading it from the Internet or installing it from a disk or flash drive, then you will need to update it manually. If you're lucky, the app has a built-in mechanism to check for updates, and you can ask it to check for updates automatically. If not, you'll have to check it yourself. Maybe set a weekly reminder to do this for all such applications.

Some apps are available directly from the maker as well as through the app store. It may cost more through the app store, but the auto-update functionality is worth it. Software in the app stores is also vetted, at least to some degree, by Apple and Microsoft.

If you have an app that is so old that it's been abandoned by the maker, you should probably delete it. Again, all software has bugs—and if your app is no longer getting updates, that also means that its security vulnerabilities will never be fixed.

Here's how to set up auto-updating for apps you got from the app store.

Tip 4-7a. Windows

Windows 10 and 11 Home are almost identical for these settings, so I will only show Windows 11. But like OS updates, app updates should already be enabled by default. You can verify this by searching system settings for "Microsoft store" and click it. Then click the little avatar/icon for your account at the upper right (Figure 4-55).

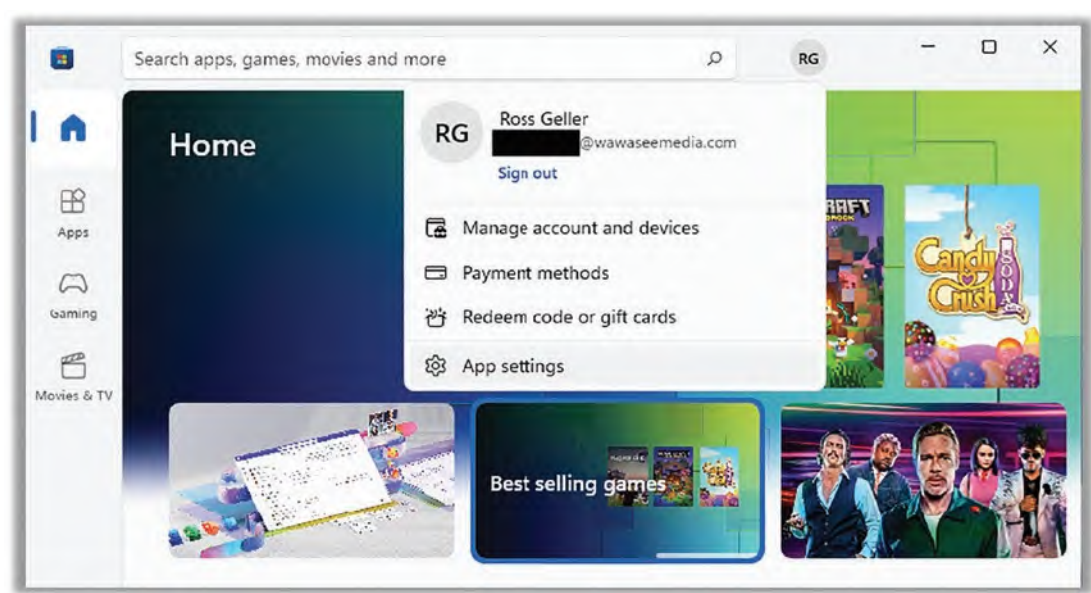


Figure 4-55. Windows 11 Microsoft Store account menu

Click “App settings” at the bottom. Make sure that “App updates” is enabled (Figure 4-56).



Figure 4-56. Windows 11 Microsoft Store app settings

Tip 4-7b. macOS

This is pretty simple and it's probably already done for you. Just open the Apple App Store (it's the blue icon in the Dock with the letter "A" that looks like three sticks). Open the Preferences/Settings from the App Store menu and make sure the "Automatic Updates" box is checked. See Figure 4-57.

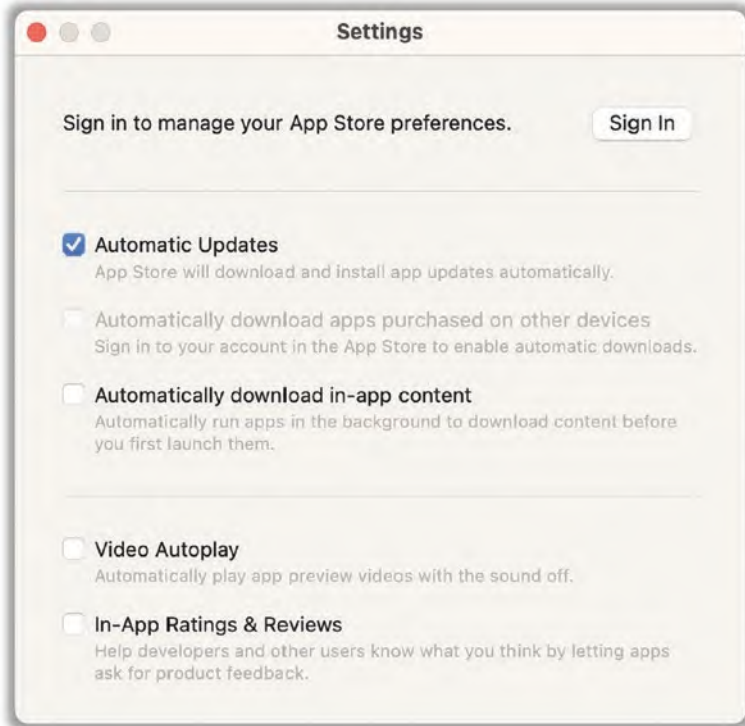


Figure 4-57. macOS App Store Preferences

Tip 4-8. Download Software Safely

It may surprise you to learn that legitimate software download sites often install things you don't want and didn't ask for (what we called "potentially unwanted programs" in Chapter 3). Sites like Download.com, Softpedia, Softonic, Tucows, and SourceForge will often install trial offers, adware, and other junk, along with the software you actually wanted. This is how these sites make money.

But it's actually worse than that. There have been several cases where these bundle installers have been hacked to install nasty malware too. It's just not safe to use these sites anymore.

Always, always go to the original source for software downloads. Find out who makes the software and go directly to their website. Or, better yet, get the app from the Apple App Store or the Microsoft Store, if you can.

See also <https://firewallsdontstopdragons.com/how-to-safely-download-software/>.

Tip 4-9. Scan Your Paper Documents

You can back up your physical, paper documents by scanning them to your computer as PDF files. Obviously, you'll need a document scanner to do this properly, though you can try just taking pictures of smaller documents in a pinch. If you have a lot of documents, it would be worth buying a scanner with a sheet-feeder function. I don't have any particular recommendation on brands.

Once you've scanned the documents and set up your computer backups, you can shred the paper documents and regain some precious space in your home. (See the next tip.)

I scanned all my documents years ago and am fully digital now for just about everything. Special documents like car and house titles, marriage and other licenses, and other official papers are scanned and then put in a safe or safe deposit box at my bank.

Whenever possible, I download documents now, including product manuals and receipts. When a document is natively in PDF format, the contents are searchable, which is extremely handy. But even scanned documents now are often searchable, thanks to optical character recognition (OCR) technology.

Tip 4-10. Shred Your Paper Documents

Many people don't realize this, but once you throw something away, it's fair game for anyone to take. Legally, once you "abandon" your trash and place it off your property (at the curb), you give up any expectation of privacy.¹⁴

¹⁴https://en.wikipedia.org/wiki/California_v._Greenwood

At a high level, you want to shred anything that's private and personal. That would include financial, medical, and legal papers. It also includes any documents that show your social security, credit card, financial account, or medical insurance account numbers or even papers that show your birth date. Maybe that seems obvious, but I'll bet you still throw away a lot of stuff that you should be shredding.

You're going to want to buy a decent shredder for this work. The main feature you want is *crosscutting*. Strip-cutting shredders that just cut paper into long, thin strips are not good enough. Even crosscut paper can be painstakingly reassembled, but it's a lot harder—especially if it's mixed up with a bunch of other shredded documents.

You can also buy shredders that can handle credit cards and optical disks (CDs and DVDs) in addition to paper, which is handy. We don't use CDs and DVDs much anymore to store data—which is possibly why you might be throwing them away. When you get rid of old credit cards or when some company sends you a “starter card” as part of a trial offer, you definitely want to shred them before you throw them out.

The last thing to consider is the size of the output bin. I would just get yourself the biggest one that fits your needs—it means having to empty it less often and mixing a lot more stuff together. You can find shredders at office supply stores or online.

CHAPTER 5

Who Goes There?

We can't go much further in this book without discussing passwords. I *hate* passwords. I hate them with a passion. And I know I'm not alone. But despite some promising new technology, I'm here to tell you that password-based authentication is still your most secure option for proving your identity today, if you use them correctly. By the time you finish this chapter, you'll understand why.

How Did We Get Here?

Passwords have become the bane of our modern computer existence. Just about every website we visit requires that we create an account to use any of its features. That means creating and remembering yet another password. To make it interesting, every website has a slightly different set of rules for its passwords. Your password has to be long, but not too long. You have to use upper- and lowercase letters and throw in at least one number. Most require you to use a "special character," but only certain ones. Some sites don't let you use special characters at all. Some of them have more weird rules, like you can't use any dictionary words or you can't have repeated letters. The password can't contain your name or user ID or anything that looks like a date. In short, they all require that your password be very hard to guess and yet somehow also be something you can easily remember. And just to add insult to injury, some systems require that you change your password on a regular basis.

It would be bad enough if we had to do this only once, but in our modern online world, most of us have dozens if not hundreds of different websites and accounts that require us to log in using a password. And so we all do the same thing: we come up with one or two favorite passwords that meet all the stupid rules, and we use them for *everything*. How else can we possibly remember them all? And yet, that's precisely what you should never do. I'll explain why in a bit.

So how did we get into this horrid state of affairs? Why do we need all of these passwords? In some cases, it's obvious—you don't want just anyone to have access to things like your online bank accounts. Somehow you need to convince your bank's website that you are who you say you are and prevent someone else from impersonating you. This process is called *authentication*. We use these credentials (username and password) to prove our identity. It's not foolproof, of course—someone could steal or guess your password and then gain access to your account. It's like the key to your house. Ideally, only you have the key that opens your front door, but if you lose your key or lend it to someone who secretly makes their own copy, then someone else can open the lock. It's better than nothing, but it's not perfect.

However, there are many websites that have nothing of yours that needs protecting, and yet they still require you to sign up for a “free” account, meaning you have to create a set of login credentials. Why is that? Because they want to track you and they want to be able to send you emails with advertisements. They may tell you it's for your own benefit—allowing you to customize your settings, share things with your friends, save payment info for later, get customer support, and so on. And those *are* benefits for creating an account. But creating an account also allows them to build up a profile on you that they may use for themselves or sell to others or both.

There has to be a better way, though, right? Isn't there something else besides passwords? Let's look at this a bit because it's good to understand how we got where we are.

May I See Some ID?

Proving your identity usually involves one or more of the following three things:

- Something you know (like a password or personal identification number (PIN))
- Something you have (like a key, a badge, or your smartphone)
- Something you are (like your fingerprint, your face, or your eye's iris pattern)

Which of these techniques is the best? Obviously, it depends on what you mean by “best.” In this book, I'm concerned with security, but also with privacy. Convenience comes second. However, convenience is still important because if something is truly inconvenient, then it won't be used—so it doesn't matter how secure or private it is. Let's look at the pros and cons of each of these authentication techniques.

Something You Are

Most people love the idea of using “something you are” for authentication. Most of these methods involve some form of *biometrics*—that is, measurements of your physical body. You can’t forget it! You can’t lose it! No one else can use it! However, biometrics have some serious drawbacks as a primary means of authenticating someone. For one thing, almost by definition, you can’t change something you are. In fact, biometrics represent more of a username than a password: it uniquely identifies you. The assumption is that your fingerprint or face can’t be faked, copied, or lost, but that’s a bad assumption. In 2015, the US Office of Personnel Management (OPM) had 5.6 million digitized fingerprints stolen via a computer hack. It’s not like those 5.6 million can change their fingerprints like they can change a password. In late 2022, someone bought a used biometric scanning device on eBay for \$68 and found the iris scans and fingerprints of over 2600 people were still stored in the memory.¹ These people are screwed for life. And you can recreate and use someone else’s fingerprint using cheap technology. Finally, you can also lose your biometric identifiers—for example, if you have a disfiguring accident.

But there’s actually a more important problem here: when using biometrics, you can’t hide or change who you are. Therefore, you can’t be anonymous. Identity is a really important consideration when it comes to authentication, but we’ll circle back to that later in this chapter. For now, just know that using your fingerprint or face pattern or any form of “something you are” is a bad choice as your primary source of authentication. However, as we will see shortly, it can be extremely useful in combination with other techniques.

Something You Have

What about “something you have”? This would be something you have with you whenever you need to prove your identity and something that would be very difficult for someone else to steal or copy. One main problem with this solution is that, until recently, it was not common for computers to have any sort of mechanism for detecting and identifying something you have in your possession. Computers of old were pretty much guaranteed to have one and only one form of user input: a keyboard. So back in

¹<https://www.nytimes.com/2022/12/27/technology/for-sale-on-ebay-a-military-database-of-fingerprints-and-iris-scans.html>

the old days, authentication had to be done using something that every computer could do. This is why they settled on entering a string of characters that only the right person should know: a password.

Nowadays, computers have many other sources of input, which opens up more options in the “something you have” department. Using Bluetooth wireless technology, we can program our smartphones and smartwatches to automatically unlock our computers when we’re nearby. Technically, though, you have to first authenticate yourself to these devices (enter a passcode or PIN—something you know) before they can be used to transitively vouch for your identity.

Another option that has been around for many years but hasn’t gained much traction is a hardware key. This is usually a little USB device, often the size of a thumb drive but can be much smaller (Figure 5-1).

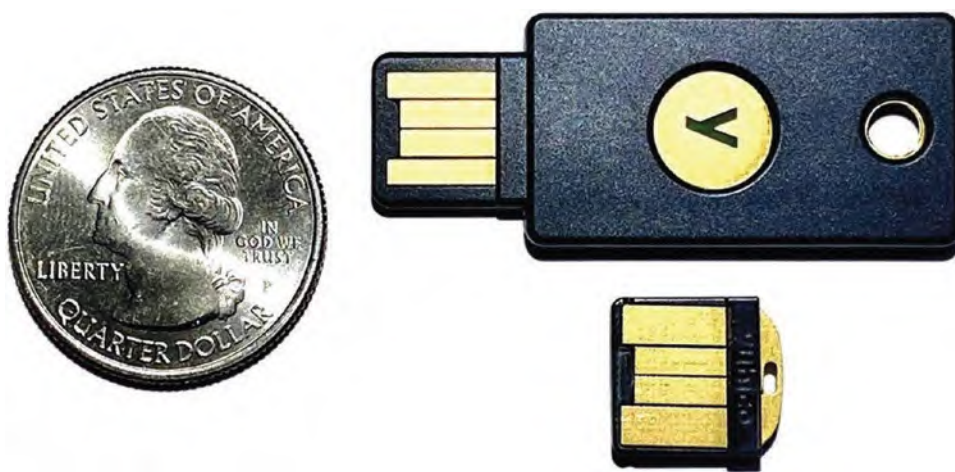


Figure 5-1. A sample FIDO hardware key (YubiKey)

The technology behind this is called Fast Identity Online (FIDO). How it works is very technical, but let me use a grossly oversimplified analogy to explain how it works at a high level.

First, I create a totally unique question that has two important properties. First, no one else could possibly answer correctly but myself—only I know the answer, and it can’t be figured out independently. Second, if you ask me the question and I give you the answer, you can then verify that the answer is correct. Basically, it’s an answer that no one can guess, but once you hear it, you know it’s correct. I write down this question and give it to you (the question itself is not secret). But I also give you the answer, locked in a box

using a secret key that I keep well-guarded. In the future, I meet you again, and I want to prove to you that I'm the same person you met before and not an imposter. You ask me the question and give me the locked box. I unlock the box and read you the answer. Now, because (a) I was capable of unlocking the box and (b) I gave you the correct answer, you believe that I am the same person who gave you that box in the first place. I am now authenticated!

Why bother locking the answer in a box and giving it to the other person to keep? Because FIDO devices don't have much digital memory space. They can't physically hold all the answers for every website you want to authenticate with.

This standard is being used by some large companies and people who are big hacking targets (CEOs, politicians, and other rich and/or famous types), but it never really caught on for everyday users. People just don't like carrying these hardware keys around everywhere they go and having to plug them in every time they need to log in somewhere. And if you lose it, you're in deep trouble. For the average person, I think this is too restrictive and cumbersome.

However, in today's world, there is a single device that almost everyone owns and that people willingly keep with them every minute of every day, no matter where they go: a smartphone.

SQUIRREL!

There is another interesting technology called Secure, Quick, Reliable Login, or SQRL² (pronounced "squirrel"). It works similarly to FIDO, with a couple key differences. First, it runs as a software app on your computer and/or smartphone, not a physical hardware key. This allows it to be run on and synchronized to multiple devices simultaneously. SQRL also has a way to revoke your identity in case you lose control of one of your devices.

Second, SQRL doesn't require the website to remember anything (no locked boxes containing answers). SQRL generates its answers based on a combination of a secret key and the name of the website. This means that your password can't be stolen by hackers if (when) the website has a data breach. (However, anything else the website may store for you, like credit card numbers, still could be stolen.)

²<https://www.grc.com/sqrl/sqrl.htm>

SQRL was created originally by a single guy (Steve Gibson) and has recently been finalized with the help of several devotees. It will be free and open, though it remains to be seen if it will be adopted (and perhaps folded into the FIDO standard).

Passwordless

This brings us to a truly promising new technology that should finally rescue us from the scourge of passwords. It uses existing technology (FIDO) but in a new way. And I believe that it will replace passwords for most logins in the not-too-distant future. It's called *passwordless* or *passkeys*. It actually does still require the use of encryption keys, but you don't have to see, create, or manage them—it's all done for you by your smartphone or computer.

Remember back in Chapter 3 when I explained how public key crypto works? This technology is the basis for passwordless authentication. Passkeys work by generating a pair of keys: a public key that you share with the website where you have an account and a private key that's very securely stored inside your smartphone. All of your private keys are locked in a digital vault (often in a dedicated secure computer chip called a *secure enclave*) that can only be accessed by the owner of the phone. How do you prove your identity to your phone? You use a fingerprint, face pattern, or PIN code. This is where “something you are” can be a crucial element in an authentication process. Your fingerprint or face pattern is also stored securely in the digital vault and never leaves your device. You authenticate with your phone, and then your phone authenticates you to all these websites using the passkey system.

Here's roughly how it will work. When you create an account on a website that supports passkeys, you'll be asked to scan a QR code with your iPhone's camera or perhaps even just click a “Create account” button on the web page. (You will also be able to switch an existing password-based account to use passkeys.) This will generate the key pair, sending the public key to the website and storing the private key on your phone. When you go to log in, instead of entering a username and password, you will do... something else. There are a few options, including scanning another QR code with your phone and just clicking a button. It's not clear yet which methods will be used. But in no case will you have to type in a password. (Okay, you might have to type a single PIN into your phone.)

Besides convenience for you, this actually has significant security benefits. Passwords are a shared single key—both you and the website have to keep this secret. In Chapter 3, we called this symmetric encryption. But passkeys are based on two-key *asymmetric* encryption—a public key and a private key. So, with passkeys, you no longer have to

worry about password database breaches. Stealing the public key (which is all the website has) won't do the bad guys any good. Also, passkeys won't work on fake websites, meaning that it will be basically impossible for bad guys to trick or “phish” you into giving up your credentials. Also, these keys are generated by your device automatically, so they are crazy strong, unique for every site, and you don't have to remember them.

There's really just one thing standing in the way of this technology: for it to work, all the websites where you have an account will need to support it.³ Apple's iPhones support this today with iOS 16, and both Google (Android) and Microsoft have also announced support for passkeys. So the client (user) side of the equation is covered—now we just need the server side to support it. I think this is the winning solution, and I believe that most major websites will support passwordless login within 2–3 years. But until then, the plain old password—that is, something you know—is still, sadly, our best option.

Understanding Password Strength

So, if we're stuck with passwords as our primary form of authentication for a while longer, then we need to understand what constitutes a “good” password. Look, I know you've had the “good password rules” drilled into your head by dealing with all those password strength meters when signing up for online accounts, but I'm going to explain *why* they force you to use mixed-case letters, numbers, and symbols. I'm actually going to prove it, mathematically, and then you'll see why most of those web-based password strength meters are pretty dumb and often just plain wrong.

How to Crack a Password

Let's approach this from the bad guy's perspective. How do cybercriminals try to hack our passwords? There are two key scenarios to consider: I will call them *online attacks* and *offline attacks*. I think when most people consider the threats to their accounts, they think of online attacks: a live human being sitting at a computer somewhere trying to log into your bank account. They try to guess your password over and over till they either get in or give up. That's actually not very common, but let's discuss it because it does happen. In this case, a human has somehow picked you out of the billions of people out there and

³You can keep track of support for passkeys on your devices and major websites here: <https://passkeys.dev/>

decided they want to hack your account. So they figure out or guess where you do your banking (there aren't that many big banks), guess your user ID (maybe it's just your email address), and then slowly and methodically try to guess your password. If they know you (or maybe if they've found your Facebook page), they can make some educated guesses: your pet's name, your kid's name or grandkid's name, your address, your anniversary, your alma mater, your favorite sports team, and so on. While this is a real risk, it's actually a small one, statistically speaking—and I think most of us realize this. What are the chances that someone is going to target little old me? Unless you're rich or famous or somehow drew the attention of a hacker, there's not much of a reason for someone to attack you, specifically. This sort of attack is also just not that efficient—it's hard to pull off.

The more common threat for John Q. Public is the offline attack. We've all seen the news stories about companies having their servers hacked and then asking all their customers to reset their passwords. In these situations, hackers break into the computer systems of a large company, and they steal their customers' information. This often includes names, addresses, phone numbers, credit card numbers, and passwords. The passwords are almost always scrambled, but unfortunately, the scrambling is not always done properly. So, at this point, the bad guys have this juicy vault full of information in their possession, and they have all the time in the world to try to crack it open. That is, they have copied thousands or millions of encrypted passwords to their local computer and can now try to crack them all.

Let's compare this with the previous case. In the online attack, a human (or perhaps a computer) is trying to log into a single person's online account by guessing individual passwords. The website input form is slow, so you can't roll through a long list of different passwords quickly. And if the website is secure, they will cut you off after you fail too many times. But in an offline attack, the bad guys have a massive collection of scrambled passwords in their hot little hands, and they can just crank up a computer to guess billions of passwords per second until they start finding matches.

Now do you see the difference? Hang on. It gets worse. People are notoriously bad at choosing good passwords. Table 5-1 contains a list of the top 25 most used passwords, based on sets of passwords that were recovered from stolen databases in 2022.⁴ The number one hacked password was 123456 (and it has held that spot year after year). Scanning the list, you will see just how bad people are at choosing good passwords.

⁴This is from an annual report from SplashData (<https://www.splashdata.com>). Note that this is the list of all *hacked* passwords... that is, of all the passwords the bad guys were able to guess, these are the most popular.

Table 5-1. *Most Common Hacked Passwords for 2022*

Rank	Password
1	123456
2	Password
3	12345678
4	qwerty
5	12345
6	123456789
7	letmein
8	1234567
9	football
10	iloveyou
11	admin
12	welcome
13	monkey
14	login
15	abc123
16	starwars
17	123123
18	dragon
19	passwOrd
20	master
21	hello
22	freedom
23	whatever
24	Qazwsx
25	trustno1

So the bad guys aren't starting from scratch. They know human nature, and they know that most people will choose something they can remember, probably something pronounceable. That *significantly* reduces the number of guesses they have to make. The scrambling process for the passwords they've stolen is not directly reversible, but the scrambling process (known as *hashing*, which we discussed in Chapter 3) is well known and repeatable—so all they need to do is take a guess, scramble it the same way the passwords were scrambled, and see whether it matches one of the stolen scrambled passwords.

That is, if I take *123456* and hash it, I get something like this:

7c4a8d09ca3762af61e59520943dc26494f8941b

So, if I find “7c4a8d09ca3762af61e59520943dc26494f8941b” somewhere in my stolen list of scrambled passwords, then I know the password for that account is *123456*. (There are techniques that make it harder to do this, but sadly they're not used as much as they should be.)

The first passwords the bad guys try are the popular ones, based on much larger lists like the one in Table 5-1—tens of thousands of them. In fact, this list is so useful that hackers usually have all the scrambled versions of these passwords precalculated to save time (they call it a *rainbow table*). If these don't work, they have also precalculated the scrambled versions of most dictionary words, common names, phrases from pop culture, sports teams, and so on. They try them all forward and backward. They replace some letters with numbers or symbols (zero for O, @ for a, etc.). Believe it or not, this process is usually enough to guess most of the stolen, scrambled passwords.

But surely this must take a lot of time, you say. It doesn't. Computers can crank out these guesses and compare them to every stolen password millions or even billions of times per second. Using common guessing techniques like this, hackers can usually recover most of the stolen passwords in a matter of *hours*. This is why companies that have been hacked will often immediately lock all their user accounts and force everyone to reset their password.

Forcing a password reset would seem to be pretty effective, right? If we just invalidate all the stolen passwords, then this must stop the hackers dead in their tracks. What's the point of guessing these passwords if they're almost immediately reset? The problem is that people tend to *reuse* their passwords. If you used “CowboyUp!” as your password for one website, the bad guys know that it's very likely that you used that same password for some of your other online accounts. While hacked-site.com has invalidated that password

on their system, what about other-site.com and still-another-site.com where you used that same password? This hacking method has become so common that it has been completely automated. The bad guys have computers trying these cracked passwords on dozens or even hundreds of high-value websites. They call it *credential stuffing*.

This is why it's crucially important that you use a strong, *unique* password for each and every online account you have, at least the ones that are important. Important ones would be your financial accounts, any website that has your credit card or medical information, your social media accounts, and your email accounts. You might not think your Facebook and Gmail accounts are that important, but they can be used to impersonate you, luring people you know into clicking malicious links or giving up information that will get them in trouble. Also, when you forget your password, many websites use your email account to send you a link to reset your password. If a bad guy can get to your email account, they can log into your banking site and request a password reset. They intercept the password reset email and set the password to whatever they want. Worse yet, they can change your email password and lock you out, preventing you from fixing the problem. It's very hard to convince your email provider that you are the true owner of your account when you can't even log in. (And good luck getting them on the phone.)

Doing the Password Math

Now we come to the crux of the chapter: what makes a strong password? When choosing a new password, many websites will tell you to include numbers, uppercase and lowercase characters, and "special characters," like punctuation marks. They will often have a little password strength meter that will indicate, as you type, how strong your password is. These strength meters are handy, but they're often too simplistic and may give you a false sense of security. So I want to educate you on what truly makes a strong password. We're going to get into a little math here, but don't be afraid... I've got you covered.

Let's start with a simple case: a personal identification number (PIN). These are most often used with ATM and debit cards, but we also use them on our phones and sometimes on door locks. They are often only four digits long—some sequence of numbers from 0000 to 9999. Each character in this PIN has ten possible values: 0–9. If you take all possible combinations of four digits, that's 10,000 total possible values. To get that value (10,000), you take the number of possible choices for each digit (in this case ten) and multiply by itself for each digit in the PIN (four). That's 10 times 10 times

10 times 10, or 10,000. This is the same as 10 to the fourth power. (I know, your eyes are starting to glaze over, and you're having horrible flashbacks to middle school math... but hang with me here.)

Ten thousand possibilities may seem like a lot, but a computer can crank through those values in a fraction of a second. However, PINs are almost always used in cases that require human input, and that's why they're usually good enough. That is, trying to guess a PIN would be an example of an "online" attack—the hacker would have to be there, in person, entering all of these guesses into the ATM by hand. (The attacker would need to steal or somehow copy your card, as well.) Finally, most systems will lock the user out (and probably keep the card) if there are too many wrong guesses in a row. For these reasons, PINs are usually good enough for these in-person situations.

Now let's consider the case of passwords. Remember that the worst-case scenario for guessing passwords is an offline attack where the bad guys can just sic a computer on the problem and walk away. Assuming we avoid the common passwords as we discussed earlier and choose a truly random password, then the attackers have no choice but to just try to guess all the possible passwords—that is, start with *a*, then *b*... eventually *aa* and *ab* and *bb*, and so on and on and on. This is known as a *brute-force attack* and is limited only by the speed of the computer and the complexity of the password. This is enormously more difficult to do, as long as the password is sufficiently long and random. In fact, for all practical purposes, if you choose a strong password, then it is effectively *unbreakable*.

To understand this, we have to use the same mathematical approach we used earlier on PINs to judge the strength of a password. First, we're adding more possible values for each character—not just numbers but letters and other keyboard characters. There are 10 numbers and 26 letters in the English alphabet. Each letter can be uppercase or lowercase. If you're keeping count, we're now at 62 possible values (10 numbers + 26 lowercase letters + 26 uppercase letters). Let's stop right there and check our math. If we have an eight-character password that is only made up of letters and numbers, that means we have 62^8 (62 to the eighth power) possible values.

If you whip out your scientific calculator, you'll see this:

$$62^8 = 221,919,451,578,090$$

That's more than 200 trillion possibilities! Wow, surely that's good enough, right?

Not really. A fast computer performing an offline attack could conceivably guess 100 billion passwords per second, meaning that it could try all 221 trillion values in just under 37 minutes. That's not nearly good enough, especially when you have to assume that the supercomputers by government agencies are probably at least 1000 times faster (100 trillion guesses per second). Such a computer could chew through all those possible values in just *2.21 seconds*. In the age of mass surveillance, we need to consider the worst case—and we need better passwords.

This is why adding more types of characters to the mix is so important. If you add punctuation characters (period, comma, semicolon, etc.), you can add about another 33 possible values, bringing the total number of character variations to 95. If you raise 95 to the eighth power (95^8), you can lengthen the guessing time for our regular hacker's computer from 37 minutes to almost 19 hours. For the supercomputer, we go from a paltry 2.21 seconds to a little over a minute.

Hmm... still not good enough for me. The answer is to make the password longer—with all due respect to our intrepid Mr. Bradford from 1970s TV, eight is simply not enough! Look at Table 5-2 to see how much difference a few extra characters make, and you'll see why longer passwords, even just a little longer, are so important.⁵

Table 5-2. *Estimated Brute-Force Time to Crack Passwords by Length*

Length	Computer Time	Supercomputer Time
8	18.62 hours	1.12 minutes
9	2.43 months	1.77 hours
10	19.24 years	1.00 week
11	18.28 centuries	1.83 years
12	1074 centuries	1.74 centuries

You can see that at ten characters, we've pretty much gone beyond what regular hackers might be able to crack in a reasonable amount of time. But we need to use at least 12 characters to really feel good about protecting ourselves from the big boys! Remember that computers are doubling in computing power about every 18 months and realize that you might want to protect certain things at least until you're dead.

⁵Special thanks to Steve Gibson's excellent website for these figures: <https://www.grc.com/haystack.htm>

So how can we possibly come up with dozens if not hundreds of unique, strong passwords and expect to remember them? The obvious answer is you can't. And that's why you need a password manager.

Using a Password Manager

The bottom line is that you should not know any of your passwords. Any password you can readily remember will have some sort of inherent pattern, and the bad guys have gotten really, really good at predicting those patterns. The human brain is just not up to this task. The only possible way to create an unguessable, unique password for every online account you have (at least until passkeys become a viable alternative) is to use a *password manager*.

What is a password manager? A password manager is a software application or web browser plugin that helps you generate crazy, long, and truly random passwords and then remembers them all for you. A good password manager will automatically fill in these passwords for you on websites that require a login and even synchronize your "password vault" securely across multiple computers and devices so you can access them anywhere.

Now, if I've done my job here, there should be all sorts of sirens going off in your head. If you're properly paranoid, you must be screaming right now: "Why on Earth would I trust all of my passwords to some unknown third party? What if *they* get hacked? All my eggs are in one digital basket!" And guess what... you're absolutely correct. However, I'm here to tell you that it's still the best option available to you right now. The pros far outweigh the cons; the benefits trump the risks. Think of putting all your valuables in a big safe. Yes, all the goodies are in one box... but that box is really, really strong. People who make these vaults are experts in making them secure; it's what they do, and they wouldn't be in business very long if they didn't do it well.

Password managers are built for the express purpose of being secure. Password managers will encrypt all of your precious data on your local machine, using a master key or password that you provide. The password manager company will have no way to access your passwords, and neither would a hacker who got hold of your password vault. That's the whole point, really. You open your vault with one master password that only you know, and then you put all your other passwords and sensitive information inside this vault and lock it. The locked (encrypted) vault can be safely sent between your devices

and even stored on the password manager's company servers. Yes, it's scary—and you should be nervous about trusting any third party with all your passwords. But in reality, they don't have your passwords; they have a blob of scrambled data that is completely inscrutable to them or to any hacker who manages to steal it. (If that's still not convincing enough, there is a compromise solution you could use—I'll cover this in the checklist.)

As a sidenote, many cloud storage companies will tell you that they lock up your data with “military-grade” encryption. That may well be true, but the real question is: who holds the keys? Here's a little test for whether you can trust a third party with your sensitive encrypted data. Call up their technical support staff and ask them what they can do to recover your data if you forget your password. The answer better be “nothing.” If they have any way to get to your encrypted data back for you, then they can get at your data any time they want because you don't have the *real* master key—they do.

A password manager can also hold other sorts of sensitive information for you: credit card and bank account info, PINs, medical and healthcare data, Wi-Fi passwords, driver's license number, passport info, lock combinations, social security numbers, and any other secrets you may want to store in a safe place. Where do you store this info now? Slips of paper in your wallet? Notes in your address book? Sticky notes on your computer monitor? This information is much safer in a secure digital vault, and as an added bonus, your passwords will be accessible anywhere you have a computer or a smartphone (even without an Internet connection).

Some password managers will allow you to securely share specific bits of information with friends and family, as well. It's even possible to allow them to log into one of your online accounts (i.e., use your password) without letting them see your password! When hooked up to your web browser, you can use password managers to automatically fill in credit card and address forms, saving you the hassle. Once you've installed a password manager, you'll be amazed at all the things it can do for you, and you'll wish you had done it sooner.

You might know that most web browsers will also offer to store your passwords for you and automatically fill them in. Some will even sync them across computers for you. But I strongly recommend that you do not use these built-in services—use a separate password manager and turn this feature off in your web browser. We'll talk more about that later.

Spoiler alert: When we get to safe web surfing later in the book, we'll learn about how the bad guys often try to trick you with fake websites. Another major plus for using a password manager is that they aren't fooled by look-alike web addresses!

Choosing a Master Password

While a password manager can be used to remember all your website passwords and other secret info, you will still need to memorize at least one password: the master password for your password vault. So now we're back to the drawing board, right? You still have to find some way to come up with a really tricky password that you can easily remember but the bad guys can't guess. However, you only need to remember one such password, not hundreds.

There are various techniques for creating a strong password that you can still remember easily. I'm going to discuss some options here to get you started, but you should then come up with your own personal technique. The key is to find a string of letters, numbers, and special characters that do not have any obvious patterns, like words in the English dictionary, dates, ZIP codes, phone numbers, names, common phrases, and so on.

Here's my personal favorite. Think of a phrase from a movie, poem, song lyric, or book—a phrase that you can easily memorize, perhaps one you already know by heart. It shouldn't be a phrase that people would associate with you, though, because you don't want anyone to be able to guess it. Then take the first letter of every word in that phrase to create your password. Include things like punctuation that exists in the phrase—capitalization, commas, question marks, and exclamation points. Change some letters to numbers or symbols, too—like 3 instead of *E*, \$ instead of *S*, and so on.

It's probably easiest to explain this with an example. Let's choose the first line to "Stairway to Heaven" by Led Zeppelin:

There's a lady who's sure all that glitters is gold.

That phrase has ten words in it. If we take the first letter of each word, plus punctuation, we get:

Talwsatgig.

That brings us to 11 characters. Now, let's change some letters to symbols:

T@lw\$@tg1g.

I changed *a* to @, changed *s* to \$, and changed *i* to 1 (one). Now, you don't have to do all of these changes; you might just do some of them. The key is that you must remember which substitutions you made.

That's a pretty good password. But we can do better, without adding hardly any complexity. I could include the possessive parts, for example:

T's@lw's\$@tg1g.

But we can do something else that's even easier... Just add some characters at the end, even if it's all the same character. Semicolons are fun, and they're easy to type. Let's add three semicolons!

T@lw\$@tg1g.;;;

That's a 14-character password that includes uppercase and lowercase letters, numbers, and symbols. That's plenty strong enough for our purposes. The semicolon trick may seem trivial—it may even seem wrong. It's a repeated character! Isn't that a no-no for passwords? Yes, usually, but in this case you're adding them to an already strong password. You just made the password three characters longer with almost zero effort. This is the concept of *password haystacks*, which I referenced in the previous section. If a bad guy is trying to guess your password and can't figure it out using the standard dictionary-type attacks, then they will have no choice but to brute-force it (i.e., try every possible combination of letters, numbers, and symbols). And at that point, every character you add multiplies the guessing effort by almost 100. Adding three semicolons to your already-hard-to-guess password just made it almost a *million times* harder to guess!

Now you need to come up with your own technique. Maybe you put your three extra characters at the beginning. Maybe you put a period between every letter. Maybe you repeat every punctuation character twice. But just make sure that whatever you come up with is something you'll remember, something that “makes sense” to you.

Using a Passphrase

There's another great option for creating a master password you can try if the previous option doesn't appeal to you. Instead of using a jumble of letters and numbers, you can instead use a random series of words. The key here is *random*—like you use a mathematically random technique to select the words. We call this a *passphrase*.

But if a passphrase uses dictionary words, wouldn't that make it easy for a computer to guess? Not if you select the words randomly and you use enough words. Again, let's look at the math. There are about 95 possible characters you can use in a password when

you add up all the letters, numbers, and special characters. The number of possible passwords you can make (i.e., the possible permutations) is equal to the number of character possibilities (95) raised to the power of the number of characters in the password (its length). If you have a 12-character password, there are 95^{12} possible passwords. That's a big number... It's 23 digits long, in fact.

Let's do the math on passphrases. Let's say you use a dictionary list of 8000 words and you randomly choose those words from the list. The number of possible passphrases is the number of word possibilities (8000) raised to the number of words in the passphrase (length). If you have a six-word passphrase, there are 8000^6 possible passphrases. That's also a very big number, which also has 23 digits in it. In other words, it's roughly as secure as a truly random 12-character password.

Now... the actual math is a lot more complicated because there are several nuances I've glossed over to keep the math simple. But the next obvious question is: how do I generate a random passphrase?

There are actually a couple cool ways to generate a passphrase. You need a word list, a good source of truly random numbers, and a simple way to map your random numbers to a particular word in the list. The classic tool for this is called *diceware*. You just need some standard six-sided dice and the dice word dictionary. You roll five dice, and this will choose a word from the list.

But here's another really fun way to generate your passphrase. Head over to my website:

<https://d20key.com>

Instead of using boring old six-sided dice, you can use 20-sided dice—the classic “d20” dice used in *Dungeons and Dragons* role-playing games! You choose the style of dice and the number of words you want in your passphrase and then click each row to “roll” your dice and randomly select your word. If you don't trust a web page to generate truly random numbers, you can also select the “Manual” style to roll your own dice and enter your results.⁶

⁶If you want a truly unique and fun way to “roll” your dice, check out the official *Firewalls Don't Stop Dragons* challenge coin! <https://d20key.com/#/coin>

Doing the Two-Step

Earlier in this chapter, we talked about the various ways—or *factors*—we use to prove our identities: something we know, something we have, or something we are.⁷ When you require more than one of these, we call it *multifactor authentication*. In the case where two factors are required, we call it *two-factor authentication (2FA)*. Many websites now offer a two-factor authentication option, which is a fantastic way to increase security with only a little extra effort. The primary factor is your password (something you know); the second factor is something you have (usually your smartphone).

Let’s look at a couple of examples to see how it works. Google offers various ways to add a second authentication factor to your Gmail account. This second factor can be required all the time or, more commonly, only for “untrusted” computers and devices. That is, the first time you try to log in from a device that Google doesn’t recognize, Google will require that you use a second factor to prove you are really you. At that point, you can decide to tell Google that this device is trusted and, whenever you log in from this device in the future, you can skip the second factor—at least for a period of time. But if you were logging in from a public computer, say at a library or a cybercafe, you would not “bless” this device, leaving it as untrusted.

One method for doing two-factor authentication is to send a text message to a cell phone that you registered with the website. After registering your cell phone, the website will send you a text message with a one-time PIN code that you will have to enter in addition to giving your regular login credentials. This PIN code usually expires after a short amount of time (probably minutes).

A much better method uses a special smartphone authenticator app that generates a time-based one-time passcode (oddly abbreviated as TOTP). This app, once properly registered and synchronized with the website, will generate a six-digit PIN that you will need to enter along with your regular credentials. The PIN code will change every 30 seconds or so. When you registered your app with the website, you synchronized an algorithm for generating PIN codes based on the exact time of day. So the website and your authenticator app will generate the same PIN code at the same time. Each website registration is unique, and therefore each website has its own PIN code. The authenticator app will have a list of all your registered websites and their current PIN codes.

⁷Security people sometimes cheekily refer to these as “something you forget, something you lose, or something you cease to be.”

The key thing to realize about two-factor authentication is that now the bad guys have to beat you *two* ways in order to access your accounts. Even if they somehow manage to guess or bypass your password, now they also need to have your cell phone. That makes their job a hell of a lot harder. Also, if you have an account that is protected with two-factor authentication and that company's servers are hacked, you now have a little extra time to change your password on their website because you know that the password alone isn't sufficient to access your account.

Note that there have been several successful attacks against the texting services. It's not easy, but it's possible. One technique involves a person convincing your cellular provider that they are you and claiming they've lost their phone. They convince your provider to give them a new phone with a copy of your SIM⁸ card. And now the cloned phone is getting all your calls and text messages. This is called *SIM jacking*. Another technique is to hack the cellular communication network itself, which isn't as hard as it should be. So, if you have the choice, you should always go for the time-based PIN (authenticator app) method over the text/SMS method.

One more important thing to note about two-factor authentication is that it only protects access to your account, not the password vault itself. If bad guys manage to steal your encrypted vault—say by hacking your computer, your device, or your password manager service provider—then the only thing protecting that data is your master password. So it's crucial that you choose a very strong master password to protect your vault.

Periodically Changing Passwords

If you've ever worked at a large company with an information technology (IT) department, then you've probably had to have a password to log into your work computer. Furthermore, you've probably also been required to change that password every 3–6 months.⁹ You can't reuse old passwords, and sometimes they even check to see that your new password is sufficiently different from your previous one.

⁸SIM = subscriber identity module. It's what ties your account to your phone number and the smartphone itself.

⁹Most people attribute this to a 2004 policy written for the National Institute of Standards and Technology by a guy named Bill Burr. He got it from a whitepaper from the 1980s! He's since apologized for this, and NIST has removed this from their security recommendations.

You're probably wondering (a) why they do this and (b) whether you should do the same thing yourself for your personal passwords. For companies, the real issue is not preventing employees from getting access to sensitive information; it's to prevent nonemployees from getting in—not just hackers but previous employees. Companies will also compartmentalize information so that some people can access things and others can't. If your personal login credentials were somehow stolen or cracked, then someone could get to whatever company resources that you can access. Someone with these credentials in hand would usually try to snoop around without being caught—that is, they probably wouldn't do anything that would draw attention, at least not until they were done gathering data or maybe unleashing malware. If the bad guys allow themselves to be discovered, then your IT department will lock your account, and they will lose their access. Your password will be reset, and you will be allowed back in, but they won't know that new password. To combat this, companies try to limit these windows of opportunity. Forcing you to change your password every so often will also mean that someone else who managed to figure out your password will have only a short time to use it.

For your personal accounts, the problem is usually different. Someone who wants access to your accounts will probably want to use them (as opposed to just spying on you without leaving a trace). They may buy things in your name or try to transfer your money to their accounts, for example. If they were breaking into your email account, they might be satisfied to just read your emails, in which case changing your password every so often would help. But generally speaking, you will probably know if someone hacks your account because they will probably do something with it.

So should you periodically change your passwords? And if so, how often? This is completely up to you. Generally, I don't think it does much good to change passwords periodically for no reason. If you're worried that someone might be lurking on your account, just reading information but not actually changing anything, then you might want to change that password. If you have ever given out your password to someone else for any reason, you should change your password when they're done using it. When one of your online service providers is hacked and the password database is compromised, they should send you an email telling you to change your password, and of course you should do that right away. They may even reset it for you or lock you out until you reauthenticate. But beyond that, you can probably just leave your passwords alone, as long as they're strong (and particularly if you have two-factor authentication turned on).

A Rose by Any Other Name

Before we get to the checklist, I wanted to discuss one more topic: identity. So far, we've focused mostly on the notion of authentication—that is, proving to someone else that you are who you say you are. This presupposes that we've established who you are. In fact, we've assumed that you even want the other party to know who you are.

In Chapter 2, I claimed that privacy is the ability and the right to share what you want, when you want, and with whom you want. You may share different aspects of yourself with different people or groups of people. You may even purposely share incorrect or conflicting information. And of course, there will be some things you may not share with anyone.

So what does this mean when it comes to identity? There will be some cases when you absolutely must declare your true and full identity—for example, when obtaining a driver's license or passport or applying for government benefits or opening up financial accounts. You can forego those things, if you wish, but if you want them, then you will need to identify yourself to do so. Yes, you can create a legal entity to shield your personal identity in some situations, but that's not something most people have the desire or patience to do. You can also create fake personas in some cases, as long as you're not using that fake ID to defraud someone. All of this is beyond the scope of this book, however.¹⁰

At the other end of the scale, there are many online relationships that can and should be completely anonymous—that is, tied to no identity whatsoever. However, advertisers and retailers *really* want to know about you, and many sites will require you to set up some sort of account with them, even if it's not technically necessary (I'm looking at you, *New York Times*). In most of these cases, you can give them an identity that is not tied to your true identity—a persona or avatar that represents you but cannot be tied to the real you. We call this a *pseudonym* or an *alias*. And when you successfully use this technique, you are not anonymous, but instead you are *pseudonymous*.

You might think this sounds like spy stuff... having burner phone numbers, wearing disguises, having fake IDs, etc. But there are much simpler forms of masking your identity that can have real, tangible security and privacy benefits. For example, if you

¹⁰ If you're interested in this level of privacy, I will have some recommendations at the end of the book.

use the same email address to sign up for all of your online accounts and one of those accounts gets compromised, then suddenly the bad guys now have at least half of your login info for all your other accounts. And if you also reuse your password on those accounts, they now have everything they need. Also, using a single email address for all your accounts allows marketing companies to correlate your data across those accounts and track you in other ways. Later in this book (Chapter 9), I'll show you how to easily create new email addresses for each account while still only needing a single inbox and email service.

Even though email addresses are globally unique and most people only have one or two of them, marketers today know that people can easily create email aliases. More people are starting to do this, making it harder for them to track you and send you junk email (spam). So many are now requiring you to give them a valid cellular phone number. Your cell phone number is arguably as identifying as your social security number or other government-issued ID number. Because you can port your phone number easily between cellular providers and because people want to avoid having to tell everyone they know that they have a new phone number, most people keep their cell phone number *for life*. Furthermore, while it's very easy to get an email alias and it costs no money to do so, it's much more difficult to get a second phone number that can send and receive text messages—and marketers know this. That's why they will try every trick in the book to get you to cough up your cell phone number. There are solutions for this, and I'll discuss them in Chapter 12, but it's not easy or free. In the meantime, you should avoid giving away your cell phone number unless absolutely necessary. Try to use an email address instead—and use an email alias, if you can.

So the bottom line here is this. You don't have to identify yourself in all situations, and it can greatly enhance both your security and privacy by remaining anonymous or at least pseudonymous wherever you can do so. Create unique aliases for yourself for online accounts, newsletters, and so on. (I'll help you do this in Chapter 9.) Challenge anyone who claims that they need your information and give them the least amount you can.

PRIVATE SHIPPING SOLUTION

When you buy something online, you need to provide a valid shipping address. For most people, that's their home address—which is unique to you and can therefore be used to track you and correlate your data across multiple accounts or websites.

Let's stop and challenge a key assumption here: does the retailer really need to know where I live? No. Only the shipping company needs to know your address. All the retailer needs to know is the shipping cost and maybe enough location data to properly calculate the sales tax. Also, does the shipping company need to know what I bought? No, it just needs to know the rough size and weight of the item(s) to be shipped (and perhaps special information like “fragile” or “hazardous”).

This is similar to asking: does this nightclub bouncer really need to see my driver's license? No, they only need to verify my age—in fact, they *really* only need to know if I'm over the legal limit for drinking alcohol, not my actual age. It's a yes-no question. And yet, I have to hand them an ID with my full name, picture, home address, height, weight, eye color, and birthdate. We often give out much more information than is strictly required for the situation. We should operate on a need-to-know basis more than we do.

Okay, so here's my idea. We create a tool to coordinate shipping, giving each party (the retailer and the shipper) only as much information as each of them needs. I envision this as something the shipping companies provide to their retail partners. Here's how it would work. You're buying something online that requires shipment. Instead of giving your address directly to the retailer, the retailer website sends the pertinent package info to its chosen shipping service, and a separate window/form pops up from the shipper. You give the shipping company your address. The shipping company then returns a special one-time token to the retailer, which contains the cost for shipping and a rough location, so the shipper can calculate sales tax. It may also contain the estimated shipping time or a tracking number. The retailer and shipper each have what they need, but also no more than they need.

Summary

- Passwords and PINs are used to authenticate us to someone else: an online account, our computer, our mobile device, an ATM, and others. Passwords are “something we know” and currently are the best primary form of authentication. Other factors like “something you have” and “something you are” are good as secondary forms of authentication.
- A new technology called “passwordless” or “passkeys” will finally replace passwords, and it can’t come soon enough. However, it will require websites to support the technology, and it may be a few years before most of your passwords will be replaced with passkeys.
- Password strength depends on a few things. First, you should never use regular words, phrases, or guessable numbers like birthdates. Second, you need a wide variety of characters: uppercase and lowercase letters, numbers, and special characters. Third, you need at least 12 characters to prevent a brute-force attack.
- You should have a unique password for every website. If you reuse a handful of passwords and one of those passwords is compromised (possibly without you knowing it), then bad guys will try using that same password for your other accounts.
- You should not know any of your online passwords—you should instead generate and save passwords using a password manager. It’s impossible for humans to remember more than a few truly strong passwords, and we all have dozens if not hundreds of online accounts.
- You will still need to remember at least one strong password: the master password for your password vault. We discussed some techniques for generating a strong password that you can easily remember.

- When possible, protect your critical accounts using two-factor authentication. These include email and financial accounts, social media websites, and any sites that have your credit card or medical information. It greatly increases your protection over just a password. Prefer using a time-based rolling PIN for this (i.e., an authenticator app) vs. text, SMS, or email.
- While it's fine to change your key passwords periodically, it's not that crucial, especially if you have two-factor authentication enabled.
- Do your best to safeguard your identity—don't give it away unless truly necessary. If some form of identity is required, use an alias whenever you can. This not only improves your privacy but can also improve your security.

In the next chapter, we'll dive into computer security—how to protect your desktop and laptop devices and their associated cloud accounts.

Checklist

This checklist covers one of the most important, most powerful defensive steps in the entire book. Please do not skip this one!

There are a handful of good password managers out there, each with their own pros and cons. You are of course free to choose whatever password manager you want, but for this book I am recommending Bitwarden. For many years I recommended LastPass, but literally as this book was in the publication process, information came to light as the result of a data breach that caused me to abandon LastPass. I encourage you to read my blog article on this if you have any reservations about using a password manager and want to understand why I chose Bitwarden:

<https://firewallsdontstopdragons.com/special-lastpass-breach/>

The short version is that Bitwarden has all the features most people need in the Free version—and the Premium version is very reasonably priced. It's also completely open source, meaning their software can be reviewed and vetted by experts. Bitwarden is supported by all major web browsers on all major operating systems including iOS (iPhone and iPads) and Android devices. The downside of Bitwarden is that it's a little flaky about offering to save passwords when you log into a new site.

If you don't like Bitwarden for some reason, I recommend using 1Password. All of the recommendations in this chapter and most of the password manager advice in the rest of this book will be applicable with 1Password or really any decent password manager service.

If you're already using another password manager, you might want to consider moving to one of the ones I've recommended here. Note that your web browser's built-in password-saving feature is not secure enough, so you should definitely move away from using that (and I'll help you do that).

This chapter contains several tips, but the first five are by far the most important. You should plan to do these things first, in order, and all in one sitting. I'd allocate at least an hour for this to be safe, but you can do it in 20–30 minutes if all goes smoothly and you aren't interrupted.

Tip 5-1. ★ Choose a Strong Master Password

Use the techniques we discussed in this chapter to come up with your master password. You will use this password to log into your password manager. (If you skipped the chapter, then you should at least go back and read the section on choosing a good master password.) Do not use this password for anything else! If necessary, you can write this password down on paper and store it in a safe place. You don't need to label this piece of paper. Just write the password on it—you'll know what it's for. Don't leave it out in the open but know where you can find it if you get stuck.

You can also generate a passphrase instead of a regular password. This should be a lot easier to remember, but longer to type. See my d20 website for help (including the “Why?” and “How?” tabs at the top of the page):

<https://d20key.com/>

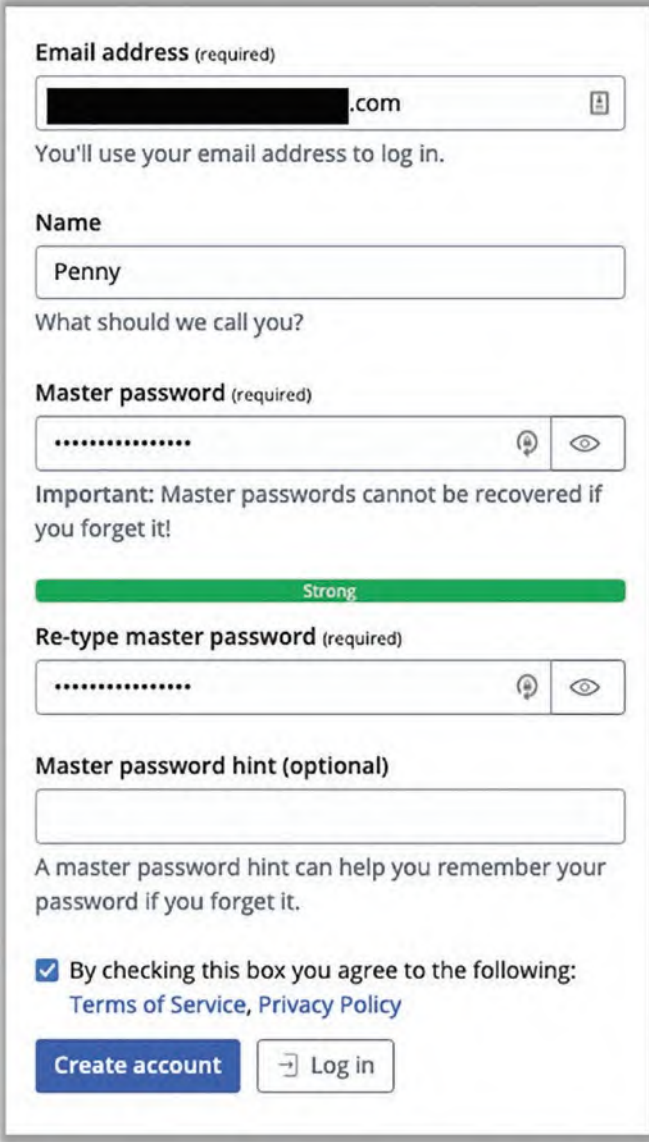
Tip 5-2. ★ Sign Up for Bitwarden

Before we install Bitwarden, let's get your Bitwarden account set up. Bitwarden offers personal and business accounts—we will be using the personal one. Bitwarden offers three types of personal accounts (as of the time of this writing): Free, Premium, and Families. The Free version will do everything we need it to do, but I would recommend getting the Premium (\$10/year) or Families plan (\$40/year). However, if you want to start with the Free plan, you can always upgrade later.

1. Go to the Bitwarden Personal home page. You should see a big button saying “Get Started Today.” Click that.

<https://bitwarden.com/products/personal/>

2. You should see a form to sign up (Figure 5-2). Give them your email address and the master password you created in the previous step. For the “Master password hint,” I would not give any hints about the password itself. However, if you printed off your password and stored it somewhere safe, you might make a vague reference here about where you stored it that you would understand but others wouldn't. Note: Don't click “Create account” just yet.



Email address (required)



You'll use your email address to log in.

Name

What should we call you?

Master password (required)

Important: Master passwords cannot be recovered if you forget it!

Strong

Re-type master password (required)

Master password hint (optional)

A master password hint can help you remember your password if you forget it.

☒ By checking this box you agree to the following:
[Terms of Service](#), [Privacy Policy](#)

Create account

Figure 5-2. Bitwarden account sign-up form

- When you click “Create account,” your browser will probably offer to save this password for you—but resist the temptation to say yes. We will no longer be using your browser to store passwords, and this password in particular (your master password) is one we do *not* want it to save. (If you did say yes, don’t worry. We’ll fix that

later in this checklist.) Now you can click the “Create account” button. You should see something like Figure 5-3, asking you to log in. Go ahead and do that. You will probably see a message there asking you to verify your email—click the button, check for an email in your inbox, and follow the instructions there to verify that you own and can access this email account. If you don’t see the email, check your junk/spam folder.

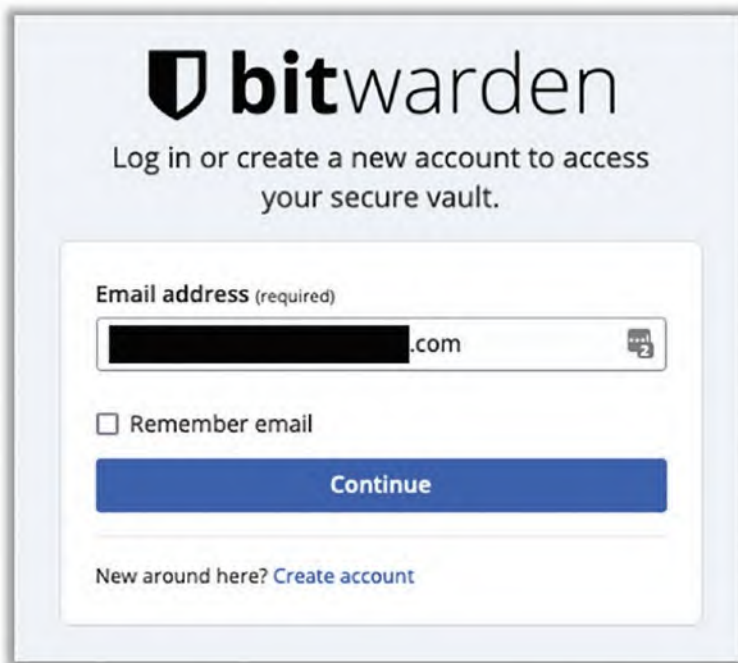


Figure 5-3. Bitwarden login screen

Tip 5-3. ★ Install the Bitwarden Browser Plugin

Since you use your web browser to log into websites, you need to have the Bitwarden browser extension (a.k.a. “plugin” or “add-on”) installed. This will allow Bitwarden to automatically fill in your login credentials, so you don’t have to type anything.

The four most common web browsers are Safari (default for macOS), Edge (default for Windows), Chrome, and Firefox. (If you happen to still be using Internet Explorer, you should definitely upgrade to Edge.) However (spoiler alert), in Chapter 8 I will be

recommending that you install and use Firefox as your default web browser. If you are already using Firefox, great! If not, proceed with installing the Bitwarden plugin on whatever browser you're currently using.

The installation process is similar for most browsers. Go to the following website and scroll down to the “Web Browser” section. Then click the icon for your current web browser (Figure 5-4). From there, you'll click “Install” or “Get” or something like that. Instead of trying to cover all of that here, I'll just let Bitwarden tell you what you need to do. So go ahead and do that now.

<https://bitwarden.com/download/>

When you're done, you'll need to log into Bitwarden (i.e., log in using the new Bitwarden browser plugin). Use the email address and master password you used when you registered your account. Bitwarden may offer to transfer your existing browser passwords. See the next tip for help with that.

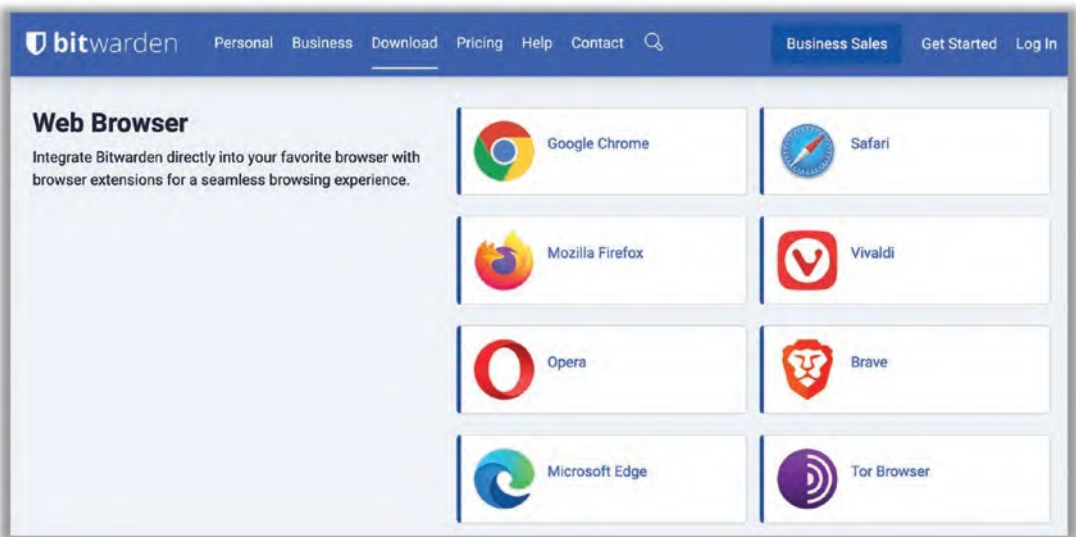


Figure 5-4. Bitwarden browser plugin choices

Tip 5-4. ★ Transfer Existing Passwords to Bitwarden

When you first install the Bitwarden browser plugin and sign into your Bitwarden vault, Bitwarden may offer to transfer your existing passwords to your new Bitwarden vault. Go ahead and follow their instructions if offered.

If not, you can find the instructions for transferring your existing passwords from your browser or even from some other password managers here:

<https://bitwarden.com/help/import-data/>

If you have passwords that are written down somewhere or just in your head, the easiest way to enter them into Bitwarden is to just go to each of those websites and log in. You can do this all at once, in chunks, or just as you visit these websites and log in again.

When you log into a web page, Bitwarden should notice this.¹¹ If it does not already have those exact credentials in its vault already, it should pop up a window just under your browser’s address bar asking if you want to save this information in Bitwarden (Figure 5-5). You will almost always want to do this, so click “Save.” If you use folders to organize your vault entries, you can choose the folder here, as well.

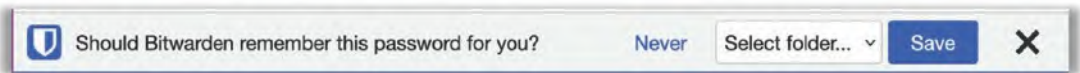


Figure 5-5. *Bitwarden save password dialog*

Since we’re new to this, let’s give ourselves a nice fuzzy warm feeling by checking to make sure the password was saved okay. In the process, we’ll see what a vault entry looks like.

You can do this from the browser plugin drop-down menu, but it’s easier to see everything by going to your web vault. Do this by going to the following website and logging in. (You might want to add a bookmark/favorite for this site in your browser.)

<https://vault.bitwarden.com/>

¹¹ For some really stupid reason, we have not settled on a simple login standard for websites. And apparently, one common issue with Bitwarden is that it doesn’t always recognize when you’re logging into a website for the first time. In those cases, you can explicitly add your website credentials using the plugin menu on your browser.

Click any item in the list to edit the entry. You should see something like Figure 5-6.

The screenshot shows the 'EDIT ITEM' form in Bitwarden. The form is titled 'EDIT ITEM' and has a close button in the top right corner. The form is divided into several sections:

- Name:** A text input field containing 'secure.backblaze.com'.
- Folder:** A dropdown menu showing 'No folder'.
- Username:** A text input field containing a redacted email address.
- Password:** A password input field with a strength indicator and a 'Premium' badge.
- Authenticator key (TOTP):** A text input field.
- URI 1:** A text input field containing 'https://secure.backblaze.com/user_overview.htm'.
- Match detection:** A dropdown menu showing 'Default match detection'.
- Notes:** A large text area for notes.
- CUSTOM FIELDS:** A section with a 'New custom field' button and a dropdown menu showing 'Text'.
- Updated:** 'Jan 4, 2023, 10:20:51 AM'
- Created:** 'Jan 4, 2023, 10:20:51 AM'
- OPTIONS:** A checkbox for 'Master password re-prompt'.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom left.
- Footer:** A red number '8', a star icon, and a trash icon at the bottom right.

Figure 5-6. Bitwarden password vault entry edit

Let's take a quick tour of a typical password vault entry:

- 1) This is a name automatically chosen by Bitwarden based on the web address. You can change this to whatever you want. Here, I might change it to "Backblaze."
- 2) You can organize your passwords into folders. For some dumb reason, it appears that you can't create new folders in this form—you have to do this at the top level of your vault.

- 3) This is obviously the username portion of your login credentials. Don't change this.
- 4) And this is obviously your password. You can click the little eye icon to show it.
- 5) Bitwarden has the capability of generating two-factor authentication codes, which is very convenient. But I recommend you do not use this and instead use a different app (see the next tip). You should keep your passwords separate from your 2FA codes.
- 6) This is the web address that was active when you saved the password, and this is the web address that will be used whenever you hit that "Launch" button from Bitwarden. This often contains a lot of weird junk you don't need, and you can edit it down here if you wish. For example, I would probably change my preceding example to be just "<https://backblaze.com>".
- 7) The Notes box is a great place to store other information related to your account, and it's also fully encrypted and secure. I use this feature a lot. For example, sometimes accounts will give you backup login codes to use if you forget your password—you can put those here. Or maybe just other notes like when you created the account, keywords or "tags" that might help you find this and related entries, etc.
- 8) Finally, you can mark a password as a "favorite" by clicking the star icon.

When done, click "Save" to preserve any edits you made or "Cancel" to exit without saving changes. There are a few other options here we didn't cover, but later I'll recommend that you skim through the Bitwarden help documentation to learn about these.

Tip 5-5. ★ Enable Two-Factor Authentication

Turning on two-factor authentication (2FA) is ***strongly*** recommended. You’re going to be putting all of your passwords in a single place—all your eggs will be in one digital basket. You should protect it *well*. It’s essential to have some “defense in depth.” But you also want to do this before the bad guys do. If they manage to hack your account and set up 2FA on your account, it can be nearly impossible to regain control. I also encourage you to set up 2FA on every important online account that you can.

Note that once you enable two-factor authentication, you must have your cell phone with you whenever you want to log into Bitwarden on any computer or device from which you have not logged in recently. I know that sounds like a pain in the butt, but you honestly get used to it pretty quickly.

Bitwarden uses the time-based PIN code method for two-factor authentication (the TOTP method we discussed earlier in the chapter), which means that you will need to download and install an “authenticator app” on your smartphone. There are several such apps to choose from. Bitwarden makes one called (unsurprisingly) Bitwarden Authenticator. But the most popular by far is Google Authenticator. In fact, many websites will specifically tell you to use Google Authenticator as if it was the only option. Google Authenticator is sort of the “Kleenex” of authenticator apps. People use the two terms interchangeably. But anywhere you can use Google Authenticator, you can use any TOTP-type authenticator app.

Note that some websites offer SMS-based two-factor authentication, where they will text you the one-time PIN code at the time of login. This is way better than nothing, but it’s not nearly as secure as the time-based PIN codes from an authenticator app.

I personally prefer an app called **Authy**. It works very well, it’s secure, and it allows you to safely back up your 2FA codes to the cloud. This is a *crucial* feature: if you lose your phone or even just get a new phone, you’ll need a way to transfer all of your 2FA accounts to the new phone. With Authy, you just need to install the app on your new phone and log in—and then all your 2FA accounts will download from the cloud.

Because backing your codes is critically important, I'll give you another tip during this process that you can use with all your 2FA accounts. I do this myself for every single one.

1. Download and install the Authy app on your smartphone from either the Apple App Store or Google Play Store. Launch the app and set up your Authy account. This will require setting up a primary phone number via a call or a text message. (It might actually be easier to set up your Authy account using a web browser on your computer, where you can generate a password using Bitwarden and save it to your vault. Then when this information syncs to Bitwarden on your phone, you can copy and paste the credentials into the Authy app.)
2. Using your computer's web browser, go to your Bitwarden web vault as we did in the previous tip and log in if necessary to open your vault. Click your account icon at the upper right and select "Account settings" (Figure 5-7).

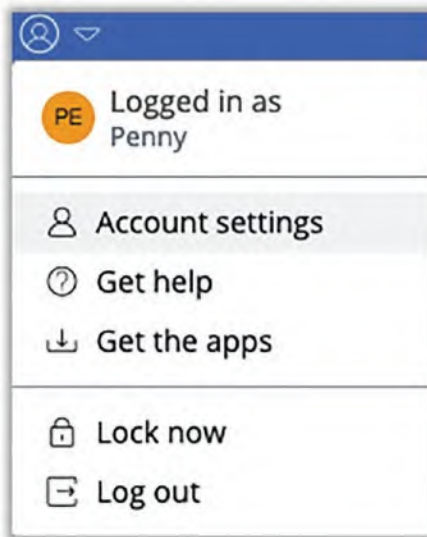


Figure 5-7. Bitwarden Account settings menu

3. At the left, select the “Security” section. Then click the “Two-step login” tab at the top (Figure 5-8). You will see a warning about two-step login, recommending that you view and save your recovery code. We will do this, but you have to set up two-step login first. Click the “Manage” button next to the “Authenticator app” option. There are other options like hardware keys, but for most people, I recommend an authenticator app.

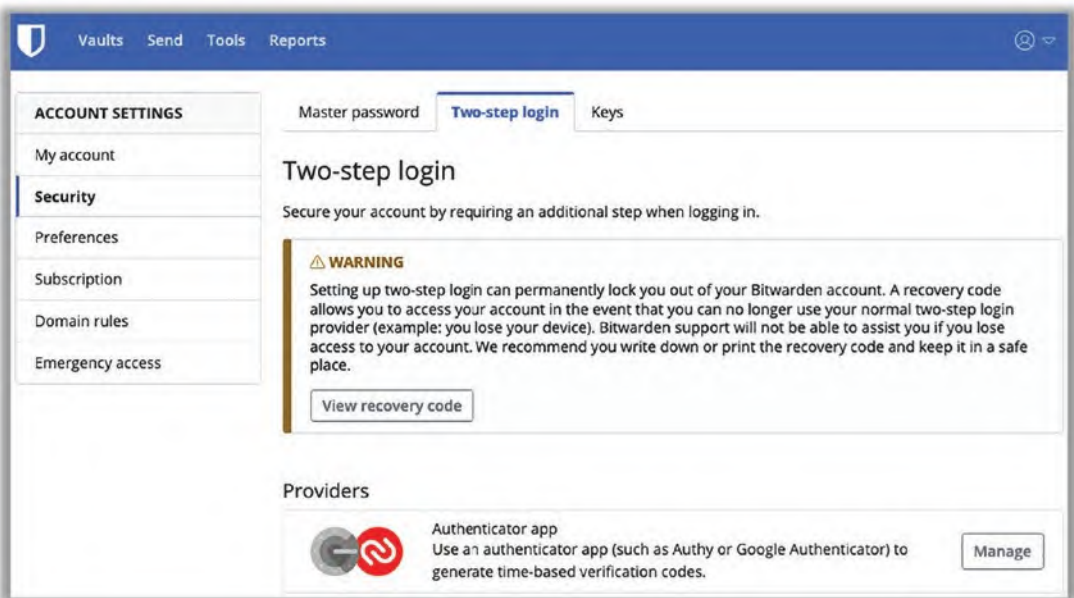


Figure 5-8. Bitwarden two-step login options

4. If asked, enter your Bitwarden master password. You should then see a square QR code similar to the one in Figure 5-9. This QR code represents a “TOTP seed code”—it’s used to synchronize your authenticator app with the website’s server. (The long string of characters you see underneath the QR code is the text form of your seed code.) Scanning this QR code is a one-time process for each site where you set up TOTP-based two-factor authentication.

- a. Note: If for some reason the Authy service goes away or you decide to move to a different TOTP service, you will need these seed codes to transfer to another service. Authy doesn't make that easy, but there's a simple workaround: just print off each QR code, write down on the paper printout which site this code is for, and then store it somewhere safe. I do this for all my TOTP seed codes. (To print this, you'll probably need to take a screenshot. If you're not familiar with this process, just do a web search for "screenshot" and either "macOS" or "Windows." Throw the screenshot image file in the macOS Trash or Windows Recycle Bin when done.)
- b. Alternatively, some sites (like Bitwarden) have the option to use a long text-based code for setting up your 2FA account. You can instead print this information off and save it, if that's easier. But do NOT save this value into Bitwarden or any digital file. A printout is better. If your computer or Bitwarden is hacked, you do not want the bad guys to be able to find these codes. (Some people actually use an entirely different password manager service just for saving these 2FA seed codes.)



Figure 5-9. Sample QR code for initializing an authenticator

- 5. Open the Authy app on your phone. Click the plus icon to add a new account. Click the "Scan QR Code" button, which will turn on your camera. Hold the phone up to the QR code on your computer

screen until it scans. You should then start seeing the PIN codes on your screen. These codes will change every 30 seconds.

6. At this point you will need to enter one of your six-digit codes into Bitwarden to verify that your Authy app and Bitwarden are in sync. Enter the code and click the “Turn on” button and then “Close.” When this step is completed, two-factor authentication will be enabled.
7. Now we can (and should) view and save our Bitwarden recovery code. Click the “View recovery code” button and enter your master password. You will see something like Figure 5-10. You should click the “Print code” button, print this off, and save it somewhere safe. Don’t save this in Bitwarden or any digital file.



Figure 5-10. *Bitwarden recovery code*

Note that this is exactly the process you’ll use when adding other accounts to Authy. Whenever you see the option to use Google Authenticator, you can select that and use Authy instead.

Tip 5-6. Take a Tour of Bitwarden

Once you have the Bitwarden plugin installed and you’ve signed up for your account, you should take some time to explore your new password vault. You can access your password vault by clicking the Bitwarden icon at the upper right of your browser that looks like a blue shield or going to the website for your vault. For most browsers, it will be gray if you are not logged in and blue if you are.

I strongly recommend that you take a minute right now to skim through the Bitwarden “Getting Started” documentation here:

<https://bitwarden.com/help/>

There are also several short video tutorials that you might want to watch at some point. You can get to these using the following site:

<https://bitwarden.com/help/getting-started-videos/>

Tip 5-7. ★ Install the Bitwarden App on Your Smartphone

You should install the Bitwarden app for your mobile phone, even if you don’t think you’ll use it there. Get the official app from the Apple App Store (iPhone) or the Google Play Store (Android).

Once you have installed the application, launch it and sign in using your email address and Bitwarden master password. You should be asked at this point to enter your 2FA code. Switch to the Authy app and tap the Bitwarden account icon. You will see a six-digit code with a 30-second timer (Figure 5-11). Note that these codes will work for a little while after that timer expires, maybe another 30 seconds.

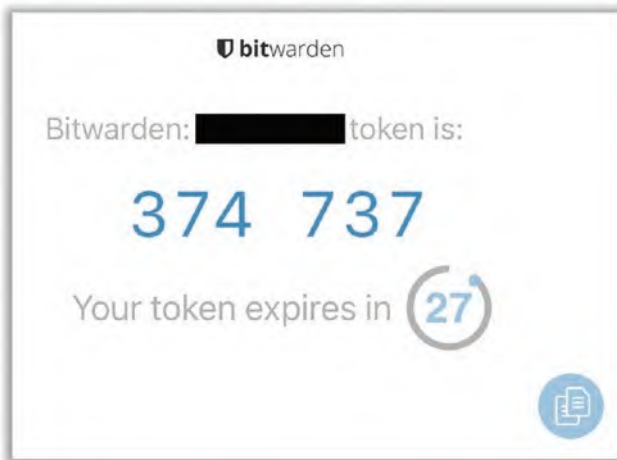


Figure 5-11. Authy 2FA code for Bitwarden

If you click the little icon at the lower right that looks like two overlapping pieces of paper, it will copy the current code to your clipboard. Switch back to the Bitwarden app and either paste the 2FA code or manually type it in and then complete your login.

If you have a phone with a fingerprint reader or a face scanner, you may be asked whether you want to allow the password vault to be opened using these biometric methods. This is really a personal choice. Personally, I'm fine using this because I'm not worried about being coerced into unlocking my phone (say, by the police or a border agent).

It's frankly not settled law yet as to whether it's legal to compel you to open your phone if it's locked, though at the time of this writing, the general trend in the United States is that passwords and PIN codes are considered "testimony" and therefore are protected under the Fourth Amendment. Biometric locks are (so far) not protected in the same way. If you're at all concerned about this, you should do your own research before you decide.

Tip 5-8. Use Bitwarden to Fill in Passwords

Now that you have some passwords in your Bitwarden vault, it's time to give them a test run!

1. In your web browser, go to a website that you know you've saved in Bitwarden.
2. When you go to that site, you will see a little number on your Bitwarden plugin icon (Figure 5-12). You may also see a little Bitwarden icon in the login form field.



Figure 5-12. Bitwarden icon with a saved password

3. Bitwarden will not automatically fill in the credentials by default, though there is a setting that will allow this (currently marked “experimental”). To fill in your password, click the icon and click anywhere on the name of the site (Figure 5-13). You can also right-click in the form fields and find the “fill” action in the Bitwarden submenu. Some forms are stubborn and will still not properly fill in. In this case, you’ll need to copy the username and/or password and paste it in the form. You can copy the username and password using the other buttons shown.

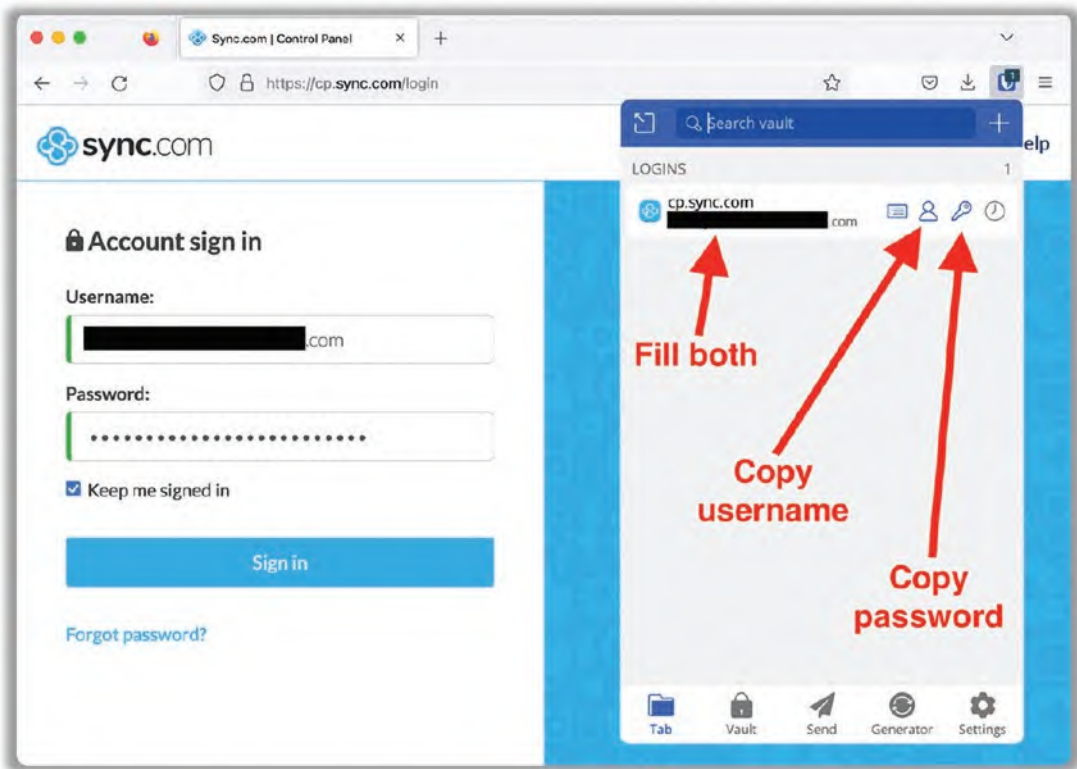


Figure 5-13. Bitwarden “fill” button on the login form

Tip 5-9. Disable Password Saving on Your Browser

Since you will now be using Bitwarden to save your passwords, you should disable the autosave feature in your web browser, so they don’t compete with each other. How you do this will differ depending on which browser you use. If you have multiple browsers,

you should disable this on all of them. Browsers change constantly, so the instructions here may be stale. If so, search for “*disable password saving <browser>*”, where *<browser>* is your particular web browser application.

Edge:

1. Open the Edge menu at the upper right (three dots).
2. Select “Settings.”
3. Click “Profiles” and select your profile.
4. Select Passwords from the list on the right.
5. Uncheck the box next to “Offer to save passwords” and “Automatically save passwords.”

Safari:

1. Select Preferences from the Safari menu.
2. Click the AutoFill tab.
3. Uncheck the box next to “User names and passwords.”
4. You may want to also uncheck “Credit cards”—Bitwarden can do that, too (see Tip [5-11](#)).

Chrome:

1. Open the Chrome menu at the upper right (three vertical dots) and select “Settings.”
2. Select the “Autofill” tab and then “Password Manager.”
3. Disable the switch next to “Offer to save passwords.”

Firefox:

1. Open the Firefox menu at the upper right (three horizontal bars) and select “Options.”
2. Select the “Privacy & Security” tab.
3. Scroll down to the “Logins and Passwords” section.
4. Uncheck the box next to “Ask to save logins and passwords for websites.”

Tip 5-10. Delete Saved Passwords from Your Browser

Once you feel confident that you have transferred **all** the passwords from your browser to your Bitwarden vault, you should then delete all the saved passwords from your browser. Browser-based password vaults just aren’t as secure as Bitwarden.

Edge:

1. Open the Edge menu at the upper right (three dots).
2. Select “Settings.”
3. Click “Profiles” and select your profile.
4. Under “Saved passwords,” use the menu at the right of each password listed (three horizontal dots) and select “Delete.”

Safari:

1. Select Preferences from the Safari menu.
2. Click the “Passwords” tab. If necessary, enter your macOS password.
3. Select each password in the list and click the “Remove” button.

Chrome:

1. Open the Chrome menu at the upper right (three vertical dots) and select “Settings.”
2. Select the “Autofill” tab and then “Password Manager.”
3. Under “Saved Passwords,” use the menu at the right of each password listed (three horizontal dots) and select “Remove.”

Firefox:

1. Open the Firefox menu at the upper right (three horizontal bars) and select “Options.”
2. Select the “Privacy & Security” tab.
3. Scroll down to the “Logins and Passwords” section.
4. Click the “Saved Logins...” button.
5. Select each saved password and click the “Remove” button at the upper right.

Tip 5-11. Store Credit Cards in Bitwarden

Bitwarden can store much more than passwords—it can also store credit card information. With this, you can quickly fill out when purchasing something online—and avoid saving this information on the site itself.

1. Open the Bitwarden browser plugin menu and click the plus (“+”) icon or go to your vault and click “Add Item.”
2. For “Type,” choose “Card” from the drop-down menu.
3. Enter the credit card information. I usually give it a name like “Capital One Visa x1234” (the bank, the type of card, and the last four digits of the card number). This makes it easy to find later. Note that if you want to be safer, you can leave off the security code (CVV), but then you’ll have to either remember it or have your card handy when you use this.

When you later come to a page that asks you to enter your credit card information, you can go to your browser plugin menu, find the card you want to use, and click the entry to fill in the form.

Note again that credit card forms aren't standardized (though they're working on this), so you may find that some fields don't fill properly. This is particularly true for drop-down menus for expiration date. For this, you'll need to view the stored information in Bitwarden and manually copy the missing information. (Why on Earth we haven't come up with a simple standard for entering credit card info and logging in via web forms is beyond my comprehension. This should Just Work.)

Tip 5-12. Store Personal Info in Bitwarden

Filling out shipping addresses can be painful on web forms, even though you have it memorized. It's also hard to remember other information like social security, passport, or driver's license numbers. Just like credit cards, Bitwarden can also be used to save and fill in personal information. Using the same steps as in the previous tip, just select "Identity" as the type and save as much information as you wish. You can create several identities for yourself (e.g., "work" and "home"), and you can also create identities for your family members.

Tip 5-13. Run a Vault Health Report

This is one of the best features of Bitwarden: the Vault Health Report, which is actually a series of individual reports. (Note that most of these reports are not available in the Free account.) These tools can analyze all your saved passwords to see which ones are bad and also help you find websites that were hacked (meaning you should probably change those passwords).

Note that if you haven't imported any passwords yet (or had the opportunity to add your passwords), then there won't be much info here for Bitwarden to work with. You might want to return to this step once you have your vault populated with your main account passwords.

1. From your web browser, open your Bitwarden vault website.
2. Select the “Reports” tab at the top to see the available reports.
I would run them all, except the one for “inactive two-step login” (since we’re not using Bitwarden’s built-in two-step authenticator).

Tip 5-14. ★ Generate Strong Passwords for Key Accounts

You will eventually want to generate strong, unique passwords for *all* of your online accounts, which may be time-consuming. At first, focus on the critical ones: your email, social media, insurance, medical, benefits, governmental, and financial accounts, plus any websites that have your credit card information on file. You should also prioritize accounts that don’t support two-factor authentication. You can use the output of your Vault Health Report to find the passwords for these sites.

1. First, let’s configure the default settings for Bitwarden’s password generator. Log into your Bitwarden web vault and click the “Tools” tab at the top and then select “Generator” at the left (Figure 5-14).
I would set the length to be at least 20 characters long. You’ll probably never need to type this in by hand, so why not? I would also select all the options for types of characters. Finally, I would check the option to “avoid ambiguous characters,” which restricts some characters that look alike in some fonts. As you change these options, a password will be generated at the top. And helpfully, numbers and symbols are color-coded to make them stand out and avoid ambiguity.

The image shows the Bitwarden password generator settings. At the top, the word "Generator" is displayed. Below it, a text box shows a generated password: "F7tNPRS3kq@Bki#jNNKY". Under the heading "What would you like to generate?", the "Password" radio button is selected, and the "Username" radio button is unselected. Under the heading "Password type", the "Password" radio button is selected, and the "Passphrase" radio button is unselected. There are three input fields: "Length" with a value of 20, "Minimum numbers" with a value of 1, and "Minimum special" with a value of 1. Under the heading "Options", there are five checked checkboxes: "A-Z", "a-z", "0-9", "!@#\$\$%^&*", and "Avoid ambiguous characters". At the bottom, there are two buttons: "Regenerate password" and "Copy password", and a small circular icon with a clock symbol on the right.

Figure 5-14. Bitwarden password generator settings

2. Now that we have the default settings configured, go to the website for which you'd like to change your password and log in (either manually or using Bitwarden).
3. Every website is different here. You'll need to figure out how you change your password for each site. It's usually in your "account" or "profile" or "security" settings. Click whatever links/buttons you need to bring up the form for changing your password. If the password change form requires it, fill in your current password.

4. To generate a new password, click the Bitwarden blue browser plugin icon, and then select “Generator” at the bottom (Figure 5-15). This will tell Bitwarden to generate a kick-butt random password for you.

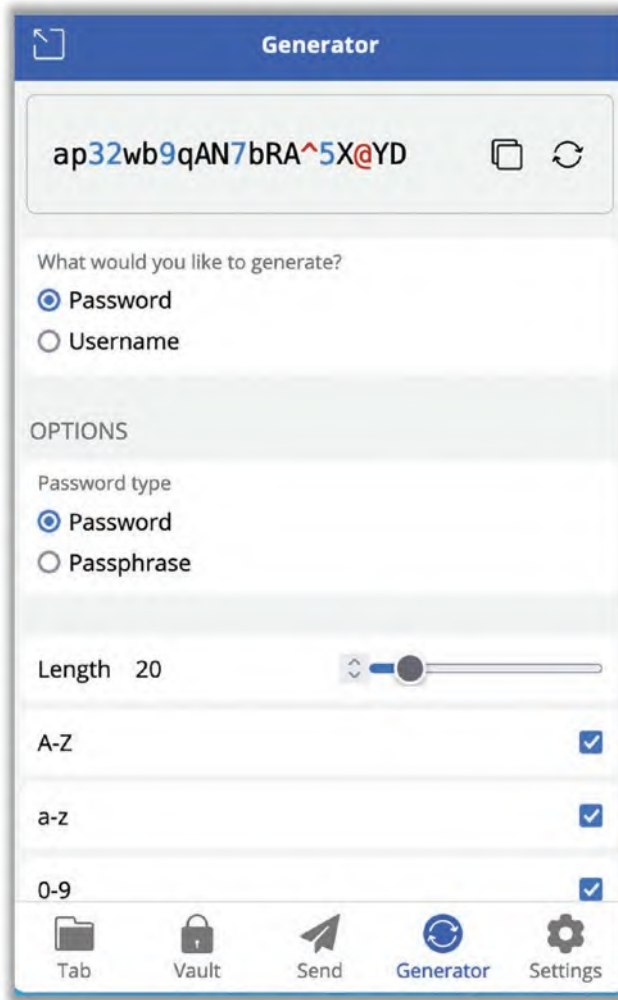


Figure 5-15. Bitwarden password generator for a web form/account

5. If you are unlucky enough to be on a website that does not allow certain types of characters or passwords of a certain length, you can make adjustments here to the settings. This should not change the default settings, but you still might check that the next time you use the generator.
 - a. Note: If this password is something you know you will have to sometimes enter by hand, either on a smartphone or worse yet something like a streaming TV box, smart TV, or some other device without a full keyboard, you might want to consider unchecking that last box for symbols—they can be a real pain to get to on smartphone keyboards or using a remote control. You might even want to remove capital letters. If you do this, you might want to increase the length of the password to offset the smaller password character alphabet.
6. If you changed any settings, the password should automatically regenerate. But if not or if for some reason you want to create a different one, just click the little circular arrow button to generate another password. Do this as many times as you want.
7. When you have a password you like, first click the little copy button to the right of the generated password (Figure 5-16). This will copy the generated password to your computer clipboard.



Figure 5-16. Copying a generated password to your clipboard

8. Now paste your new password into the password change form and confirm the password change.
9. Bitwarden *should* then pop up a little banner at the top of the web page to ask if you want to save this password. You will obviously want to do this. If it does not do this, you should manually edit this entry and again paste in your new password.

Tip 5-15. Generate and Store Offline Passwords

There will be some situations where you need to generate a strong, random password for things besides websites. We'll have such a situation in the checklist of the next chapter, in fact. So you need to know how to generate and save passwords without having a corresponding web password form to fill out.

You can do this using the Bitwarden menu on your browser like we did in the previous tip. But once you create this password, you'll want to copy it and save it in a secure note.

1. Using the Bitwarden browser menu, generate a secure password. Then use the copy button to save it to your clipboard, like we did in the previous tip.
2. Now, in your Bitwarden browser menu, select the button to add a new entry and then select "Secure note" as the type. The password was saved by your computer clipboard in the previous step, so just paste it in the big open space. I would put the password on a line all by itself, to avoid any confusion. Give the note a descriptive name and feel free to add more info in the note with the password; you want to be *sure* you know what this is for, and you also want to make it easy to search for (Figure 5-17). Then click "Save."

ADD ITEM

What type of item is this?

Secure note

Name

Backup hard drive encryption key

Folder

No folder

Notes

YbP55n%6MWYACNbbEtHS

CUSTOM FIELDS

New custom field

Text

OPTIONS

☐ Master password re-prompt

Save

Cancel

Figure 5-17. Saving generated passwords in a Bitwarden secure note

Tip 5-16. Pepper Your Passwords

Fair warning: This one is tricky. Most people will not want to do it, but I’m including it for completeness.

If you want the convenience of a cloud-synced password vault, but don’t fully trust your vault holder, there is an interesting but tedious technique that will let you have the best of both worlds. It will take a little work, but I think it’s an interesting compromise. This method goes by different names: double-blind passwords, Horcruxing,¹² or peppering.

¹² This is a Harry Potter reference: https://en.wikipedia.org/wiki/Magical_objects_in_Harry_Potter#Horcruxes

At a high level, you split your password into two parts: a crazy, random base password that you store in your password manager and a short secret suffix that you either remember or store separately.

When setting or updating a password, use your password manager to generate a strong password, as usual. Have the password manager fill that in for you. Then, *before submitting your password change*, tack on a short suffix of your choosing. That is, extend the password with another, short secret. For example, if your password manager generates “o35F@CuW0%”, you can then add “6J9D” to make “o35F@CuW0%6J9D”. That’s your actual password. But *you only save the first part in your password vault*.

If your password vault is somehow stolen and cracked, the bad guys will only have part of each of your passwords. They wouldn’t have the “pepper” —they’ll still have to guess that, assuming they figure out why none of your passwords are working. (Salt and pepper are actual cryptographic terms, by the way.¹³)

This means you have to somehow remember that “6J9D” suffix part. You’ll either need a separate password vault or commit it to memory. But you could come up with a formula for deriving the suffix too. For example, for “amazon.com” you could make the suffix “amaz” or “AmAz” or “-amaz”... You get the idea. That’s predictable, but the bad guy would somehow have to guess the crazy base password and then figure out your pattern.

Here’s a major drawback to this method: your password manager is now going to constantly ask you, “Do you want to update your password?” every time you log in. Why? Because it’s smart enough to see that what you submitted isn’t what it has stored, so it assumes you must have changed your password. Crucially, *you can never accidentally say “Yes”* as this will now store the entire password. This is precisely what you’re trying to avoid with this peppering technique.

If this sounds interesting but too difficult, consider maybe only using this technique for the really important passwords.

¹³ [https://en.wikipedia.org/wiki/Salt_\(cryptography\)](https://en.wikipedia.org/wiki/Salt_(cryptography)), [https://en.wikipedia.org/wiki/Pepper_\(cryptography\)](https://en.wikipedia.org/wiki/Pepper_(cryptography))

Tip 5-17. Guard Your True Identity

This may seem like an odd thing to say, but you should avoid identifying yourself (giving out your real identity) where you can. Don't give out uniquely identifying information like your full name, home address, birthdate, email address, phone number, or government ID number unless you really need to do so. When filling out forms or signing up for accounts, ask yourself these questions:

1. Do they have the right to know who you are?
2. Do they have a valid need to know who you are?
3. Do you want them to know who you really are?
4. Do you specifically want to pretend to be somebody else?

For low-key stuff, you can often just lie—as long as you're not defrauding them in some way by doing so. I will often give out fake names or birthdates, for example.

However, if you're creating an account with fake info, you should be sure to note the false information that you gave (like maybe save this in the password manager entry for this account) so that you can faithfully regurgitate the lie(s) if asked to verify that information later.

CHAPTER 6

Raise the Drawbridge!

Now it's time to really get into the meat of the book—computer security! This chapter covers the topics that most people probably associate most with security: Macs vs. PCs, antivirus software, and operating system security settings. This chapter will cover those topics and more, with a slew of top-notch tips to make sure your desktop or laptop is locked down tight.

Macs Are Safer Than PCs

Let's start this chapter by stirring up some controversy: Macs are safer than PCs. That's right, I said it. However, I had to seriously resist the urge to put “air quotes” around the word *safer*. So, let me be a little more specific. Macs are “safer” than PCs...because most people who write malware are looking for the largest market, and that would be Windows. Despite the recent resurgence in popularity of Macintosh computers, they still make up only a small percentage of the computers on the Internet. According to GlobalStats “statcounter”, Macs account for just under 14 percent of all desktop operating systems as of April 2022, while Windows holds about 74 percent. If you were going to try to design some sort of computer virus, which operating system would you focus on?

This is a form of what we call *security through obscurity*, which I mentioned in Chapter 3. Macs are more “secure” because they are more “obscure.” Security through obscurity means that you try to lie low and not draw attention. If they don't see you, they won't attack you. As a security practice, it's horrible. It's sorta like hiding the key to your house under your doormat. Sure, your house is technically locked, but if someone goes to the trouble of looking around for a key, then it may as well not be locked.

Modern operating systems have included lots of great security features over the last decade or so, and I think you'd be hard-pressed to argue that the latest Mac OS is significantly more secure than the latest Windows OS. However, there are a lot more PCs

out there running really old versions of Windows than there are Macs running really old versions of Mac OS. Again according to GlobalStats “statcounter,” as of the December 2021, 13 percent of Windows PCs were still running Windows 7, which was released in 2009 and cut off from all support in 2020. Despite a period where Microsoft offered free updates to Windows 10, only 23 percent of PCs are running Windows 11, according to Adduplex. If you’re one of those people still running Windows 7, you need to upgrade to something newer—and if that means getting a newer computer, then you should do that, if you can.

In 2013, Apple shifted to a policy of free upgrades for its operating system, which is a huge plus for Mac users and their security—and it allows Mac users to upgrade to the latest OS as soon as the new version is available.

So, on some level, you’re marginally safer with a Mac than with a PC. But I’m not going to leave that to chance. Let’s talk about the things you can do to really make yourself safer, regardless of what operating system you’re running.

Non-admin Accounts

One of the most fundamental principles of security is the practice of *least privilege*. This is sorta like the “need to know” that we’re familiar with in our spy novels and movies (and of course, it’s a real thing in security agencies). Benjamin Franklin once said, “Three can keep a secret, if two of them are dead.” The idea here is that the fewer people who have access to the truly important stuff, the more likely it is that the important stuff will remain safe.

Let’s look at the castle analogy again. You might give everyone on your guard the keys to the front gate, but you would give the keys to the main castle only to your elite guards. Why? Because the guard at the front gate doesn’t need access to the castle. Likewise, the king might keep the keys to the gold vault on his person, not even trusting the castle guard with that level of access. At the end of the day, the only person who really needs to access the coffers is the king. If every member of your castle guard had a copy of the castle and vault keys, then what happens when one of the guards is knocked over the head and his keys are stolen? All of a sudden, your most precious items are at risk. Guards don’t have any need to access the gold in the vault to do their job. They just need to protect it. So, guards don’t get that key.

Who has a key to your house? Probably everyone in your family. Maybe you will give a key to a house sitter while you're away because for that limited period of time, they actually need to be able to get into your house. When you get back, you take back your keys. But who has keys to your safe deposit box or the combination to your house safe? Probably just you. You would probably never give that access to anyone else, at any time, because the only person who *needs* to get in there is you.

The principle of least privilege says that people should be allowed to access only those things they need to access to do the things they're supposed to do, and no more. If necessary, you can grant temporary access and revoke it later.

You may already know that your computer allows you to set up multiple user accounts. You may never have used it, but you probably know that it's possible. What you may not know is that each of these user accounts can have different levels of privilege. That is, you can restrict the level of access—the power to make important changes—for each account. At first you might think that this feature is mainly for parental control, preventing kids from doing stuff they shouldn't be doing. Actually, it's for all users—even you! But wait...surely if you can trust anyone, you can trust yourself! Turns out you can't. It's not about trusting yourself; it's about preventing malware that gains access to your account from acting on your behalf. If you accidentally click a bad link, download a virus, or hit a website that installs malware, then whatever you are allowed to do, *the malware can also do*.

Let me drive this home with some chilling statistics. According to a 2017 report by a company called Avecto, 80 percent of all Windows security vulnerabilities that were considered “critical” could have been prevented or significantly mitigated if the user had not had full administrator (or “admin”) privileges. Furthermore, removing admin rights could have mitigated 95 *percent* of the critical vulnerabilities in Edge.

Great. Now I can't even trust myself! Now what?

The solution to this problem is to always create at least two accounts on your computer: an admin account, which you use only when necessary, and a regular, non-admin account for everyday use. When you first pull your shiny new computer out of the box, you're going to need that admin account to install your software and tweak all your system settings. But after that, you need to create and use a more restricted account for day-to-day stuff.

I would go further, however. I believe strongly that each person in the household should have their own account. It's easy to set up, and there's really no excuse for not doing this. It's not about keeping secrets—everyone deserves their own space, their own settings and preferences, and some basic privacy. It lets everyone express their individuality—but it also compartmentalizes risk. As an added benefit, this function will allow you to use parental controls to restrict access for young children, without affecting your ability to...uh...do parent things. And if something goes horribly wrong with one of the user accounts, you can just delete that account and create a new one without affecting anyone else or having to completely wipe and reinstall everything on your computer.

There are other interesting reasons to have multiple accounts. If you're a hard-core gamer or have some other intense application that requires some system tweaks to be efficient, you can create a second account for this purpose. This other account will be stripped down and dedicated to the special task at hand.

If you regularly give presentations for work using your computer, you can log in to a special account for when you're presenting. You can have a special desktop picture, avoid sharing your cluttered desktop, and also avoid annoying pop-up notifications from all your personal accounts.

You can also set up a special guest account so that when someone just wants to check their mail or look something up on your computer, you don't have to worry about giving them access to your personal stuff (including your password vault).

Microsoft announced a feature with Windows 10 called "Controlled folder access." The purpose of this feature is to restrict access to your personal files to only a few authorized applications. You select the files as well as the approved applications. While this may seem odd, it's really just another form of least privilege. If configured properly (and I'll walk you through this later in the checklist for this chapter), this tool would prevent ransomware from encrypting your irreplaceable files and demanding money to unlock them.

Likewise, Apple has added several security features to macOS, including restricted access to key folders, as well as access to your computer's location, camera, microphone, contacts, photos, and much more.

I expect that we'll see more and more features like this as time goes on from both Apple and Microsoft. As things get worse out there, the balance between security and convenience will necessarily move in the direction of security.

iCloud and Microsoft Accounts

Get ready for a big dose of “good news, bad news.” In the old days (like 2004), your computer was more likely to access the Internet via dial-up modem than always-on broadband. Around this same time, smartphones came on the scene, and suddenly people had not one but two devices that were always connected to the Internet. It was only a matter of time before people wanted their address book, web bookmarks, calendars, and to-do lists to be kept in sync across their various devices.

Apple and Microsoft heard the call and launched services to meet this growing need. The current versions of these services are iCloud and OneDrive,¹ respectively. While these services offer limited Internet-based file storage and sharing, in this chapter I’m focusing on the data synchronization aspects. You can’t argue with the convenience factor here. When you update your vagabond sister’s home address for the umpteenth time or add little Johnnie’s complete Little League spring schedule to your PC calendar, it’s really nice to have those changes automagically appear on your smartphone and your work computer. Oh, and you can probably also access all of this info from the Web by logging in to your cloud account, even from a computer or device you don’t own. Finally, you can use these same services to share this information with the rest of your family. What’s not to like?

Well, that was the good news—arguably great news. It’s a killer feature. Here’s the bad news: you’re not just sharing that all that juicy information with all your devices and your family members, but you’re also sharing it with Apple and/or Microsoft. Here’s the worse news: you’re probably sharing that information with many other companies too. Apple and Microsoft will argue that this is a feature, not a bug—they’re giving you the opportunity to access this information from within other applications, saving you the trouble of having to manually transfer things like contacts and calendar events to some third party. But you need to stop and think about what all that data is revealing about you. Your address book probably contains more than friends and family. It may also contain embarrassing contact information—maybe your AA sponsor, herpes doctor, or mistress. And if you’re like most other people I know, you put lots of other info in your address book like social security numbers, PINs and passcodes, account numbers, and who knows what else.

¹These marketing names change all the time. Apple’s service used to be called Me.com and MobileMe. OneDrive used to be called SkyDrive. No matter what they’re called, these are Apple and Microsoft accounts.

That said, it's almost impossible to avoid signing up for these services today. Both Apple and Microsoft have deeply embedded these services into their products to the point where many key features simply won't function without them. Furthermore, you pretty much need to have one account for each person in your family, not just one shared account. These services are not just about synchronizing data across your devices, but it's about personalization of the experience on these devices for each individual. For example, it allows parents to control what each of their children can access—what's right for your elementary school son is different than what's right for your teenage daughter.

Of course, all of these hyper-personalized settings are a gold mine for marketers. If you dig around in the end-user license agreements (EULAs) you “sign” by clicking that “agree” button, I'm sure you'll find references to how you consent to sharing some of your information with “partners.” I guarantee you'll find language about how Apple and Microsoft will hand over this information to law enforcement authorities “in accordance with the law” too. That may or may not require a warrant, by the way.

This is the world we live in now. We're offered enticing and often very valuable services, usually at no (monetary) cost—we just have to sign away our privacy. And this is increasingly becoming unavoidable as these services are tightly integrated with our computer and mobile operating systems. In Chapter 10, I'll show you how to enhance the privacy settings for these accounts.

Built-in Security Features

Computers are meant to make our lives easier and richer by offering all sorts of valuable functions, taking over the drudgery of tedious tasks, helping us to organize our increasingly complex lives, and giving us powerful tools to create documents, presentations, greeting cards, images, and so on. In the early days, before the advent of the Internet, computers were wide open—they were ready and willing to accept instructions from other computers on the home or work network. Our operating systems and software applications were happy and naive, gladly offering their help to anyone who asked. Then came the Internet. It was like transporting Mary Ann from Gilligan's Island to the Island of Dr. Moreau. The cheerful eagerness to help without question went from being an asset to a serious security liability.

Modern computers have lots of built-in security features, though until recent years, many features were not enabled by default. Security is frequently at odds with convenience, and both Microsoft and Apple want to avoid causing their customers undue grief. Thankfully, however, as computer security has become more important, computer and software makers are finally enabling these features right out of the box.

One of the most important features in modern home computer networks is the *firewall*. Firewalls keep out unsolicited connections from outside your network but allow you to initiate connections from inside your home to the broader Internet. They also allow you to set up specific rules that explicitly allow certain types of connections from outside your home. It's sort of like a phone that can only call out by default but will let you give it a list of people who you allow to call you. (Why no one sells such a phone is beyond me. I'd buy it in a heartbeat.) You probably have multiple firewalls in your network. Your ISP's modem might have a built-in firewall. If you have a Wi-Fi router, it almost surely has a firewall function, enabled by default. Finally, your operating system also has a built-in firewall. These firewalls do an excellent job of protecting your computer. (We'll talk more about firewalls in Chapter 8.)

These features may sound nice on paper, but you'd be surprised how well they work—all by themselves—to thwart Internet attackers. Because unprotected computers are so vulnerable, hackers and other bad guys are constantly scanning the Internet for computers without these basic protections. Multiple studies² have shown that unprotected computers (particularly older models without these modern, built-in protections) connected directly to the Internet are routinely and easily hacked. In fact, if you connect an older, unprotected Windows machine directly to the Internet, it will be subverted, on average, *within ten minutes*. Before this computer can even download the system updates that would probably protect it, it will be hacked³ by some automated bot. The firewall functions as an excellent first line of defense, and luckily these features are standard in home networks now.

So far, we've talked only about features that are already in place and working for you right now, and these features tend to be enabled by default. But there are other built-in security features in modern operating systems that are just sitting there, waiting to be used.

²Such as this one: <https://isc.sans.edu/survivaltime.html>

³Hackers refer to this as being “p0wned” or “pwned.” It rhymes with *owned*, and the meaning is that the computer has been hacked and subverted to the hacker's will.

Full hard drive encryption is a feature that's been built into recent versions of macOS and Windows. While Apple's drive encryption utility (FileVault) is available on all of its recent OS variants and enabled by default, Microsoft's encryption utility (BitLocker) is unfortunately only available on the Pro and Enterprise versions of Windows. Encrypting your entire hard drive might seem like overkill, but it's so easy to do; there's just no reason not to do it. As a user, you won't even notice it. The operating system takes care of decrypting all the files (and applications and even the OS itself) on the fly and in the background. What this means is that if someone were to have physical access to your hard drive, they would be unable to read any of the data, unless they were somehow able to guess your encryption password. While this may not be that important for desktop computers that stay inside your house, it can be important for laptops and other devices that you carry around with you—particularly if you travel to foreign countries⁴ with these devices. If your laptop were to be lost or stolen, you'll be happy to know that your data is perfectly safe, even if they were to pry open the case and attempt to directly access the hard drive. But even for desktops, this feature is important when it comes time to sell or donate the computer.

One last free feature deserves special mention: Apple's "Find My" service, which works with a Mac, iPhone, or iPad. Offered with Apple's iCloud service, this feature allows a person to track the location of all their devices and control them from afar. When you register your device with the Find My service, Apple uses the various wireless technologies (mainly Wi-Fi and cellular signals) on the device to help you communicate with the lost device, send remote control commands to it, and, as a last resort, remotely erase the data from the device. It's truly a marvelous feature, and everyone with an Apple product should take advantage of it.

Let me demonstrate the usefulness of this feature with a personal story. My family and I went to Los Angeles a couple years ago for a big vacation, and part of our trip included Universal Studios. I normally carry my iPhone in my shirt pocket, and I do *not* normally ride theme park rides. However, on this day, we rode several—and at one point when I went to pull my iPhone out to take some pictures, I realized it was gone. It must have fallen out, but I had no idea where. This park is massive, and it could be anywhere. I alerted our tour guide, and she said she would put in a call to their lost-and-found

⁴By the way, the danger here for US citizens is at the US border crossing. US law currently allows law enforcement to inspect and even seize your electronics for any reason: <https://www.eff.org/issues/know-your-rights#5>

department, but that they probably wouldn't be able to look for it until after the park closed at 10 PM. We got home around 9 PM, and I jumped on my laptop to check Find My iPhone on iCloud...and there it was, in the Jurassic Park ride building! As it hit 10 PM, I was able to actually send signals to my iPhone to make alerting noises and post a message on the main screen with contact information. As I watched the map update, I finally saw it move! Someone had found it! It stopped moving at the building where the lost-and-found office was. I went first thing the next morning and retrieved it.

The Pros and Cons of Antivirus Software

When people think of computer security, they invariably think of antivirus (AV) software. That's no accident. Companies that make this software spend lots of money marketing their wares and convincing you that you'd be foolish not to buy them. Most Windows PCs come preloaded with all sorts of trial software that claims to protect you from the big bad Internet—for just a small (ongoing, hard-to-quit) service fee! This is a perfect example of what we call FUD, which stands for “fear, uncertainty, and doubt.” Computer malware is a very real problem—don't get me wrong—but in many cases today, the cure can be worse than the disease. Let me explain.

In simpler times, AV software did a good job at finding malware on your computer. Generally speaking, the core function of AV software is to recognize known malware and automatically quarantine the offending software. Some AV software is smart enough to use heuristic algorithms to recognize malware that is similar to the stuff it already knows is bad or recognize suspicious behavior in general and flag it as potentially harmful. A popular feature for a lot of AV software is to monitor your web traffic directly, trying to prevent you from going to malicious websites or from downloading harmful software.

That all sounds good, but the devil (as always) is in the details. First, in the ever-connected world of the Internet, malicious software is produced so frequently and is modified so quickly that it's really hard for AV software to keep a relevant list of known viruses. Also, the bad guys have moved to other techniques like phishing to get your information, attacking the true weakest link: *you*. AV software just isn't as effective as it used to be.

But the problem is much worse than that. In many cases, the AV software *itself* is providing bugs for hackers to exploit. Not long ago, Symantec/Norton products were found to have horrendous security flaws⁵ (which it claims to have since fixed). Increasingly, AV products are offering to monitor your web traffic directly, but this means inserting themselves into all of your encrypted (HTTPS) communications, which has all sorts of ugly security and privacy implications.

This comes back to the concept of least privilege. In order to properly protect you, AV software must be given the highest (and more dangerous) levels of access to your computer and your data. Think of it like hiring a bodyguard—to protect you, they need full, unfettered access to you and your stuff—even the embarrassing stuff. But while you can have a bodyguard sign a nondisclosure agreement, you probably agree to quite the opposite when agreeing to the terms of service for your AV software. Furthermore, you can sue a bodyguard who allows you to come to harm due to negligence, but you can't sue Norton if you get a virus.

So, I strongly believe you don't need to pay for an antivirus service today. That is, I don't personally believe that the benefits of the various for-pay services warrant their cost for most people. There are totally free alternatives from the operating system creators that do a very good job (which I will be helping you install later in this chapter). Furthermore, if you just do the things I outline in this book, you will significantly reduce your risk. It's like debating the value of buying a bulletproof vest. While walking around wearing Kevlar is inarguably safer than walking around wearing only cotton, your better option is just to avoid places where bullets are likely to be flying.

Sticky Bits

Did you ever wonder what happens when you delete a file on your computer? On Windows and Mac OS, this is represented by putting the file or folder in the “Trash” or “Recycle Bin.” Most of you probably realize that the file isn't actually deleted until you “empty the trash.” What you may not realize is that even then, the data associated with that file is not really gone. It's still there on your hard drive. While your file system no longer shows it to you, the actual bits and bytes are still there, and special software can be used to recover that information.

⁵<https://www.us-cert.gov/ncas/alerts/TA16-187A>

This is sort of like the difference between throwing away a document and shredding it. Just because you threw your old legal will into the garbage and the trash collector took it away doesn't mean that it can't be salvaged and read. You can't see it anymore, but it still exists in a landfill somewhere. It will slowly decay over time, but until then, someone could dig around and find it. This is why you should always shred documents that contain personal information.

When your operating system "deletes" a file on your hard drive, all it really does is forget about it. It treats that part of the hard drive as if it were empty. When you want to save a new file, the operating system will put that file in the space on your hard drive that is marked as empty. Someday it will eventually overwrite part or all of your old "deleted" file, but until that day, the data is actually still there and capable of being read by special tools.

So, if you really want to delete a file from your computer, you need to digitally "shred" it. I'll show you how to do this in the checklist for this chapter.

Summary

- Macs are targeted less often than PCs by hackers and malware makers, mostly because Windows is a lot more popular than macOS. Apple computers are also much more likely to be running the latest version of the operating system than their Windows counterparts, largely because Apple has been giving away all updates to its OS for years. Major security features are added with each OS release, and therefore Macs tend to be more secure because they are more likely to be running an OS that has these new features.
- Having a separate non-admin account on your computer can significantly reduce the damage done by malware, particularly on PCs. It also makes sense to have separate user accounts for each person in the family—to provide a personalized space for everyone and also to compartmentalize exposure to malware.
- Cloud-based storage and data synchronization services have become ubiquitous and nearly impossible to avoid. It's important to understand what information you're sharing and do what you can to reduce your exposure. (We'll discuss this more in Chapter 10.)
- While there are many for-pay services and software tools out there to protect your computer from malware, they're probably not worth the money. There are free alternatives that do a very good job, especially if you follow the other tips in this book.
- To truly delete a file, you need to do more than just "empty the trash/recycle bin." You need to digitally "shred" it.

In the next chapter, we'll dig a little deeper into how your home network works and I'll tell you how to protect your "smart" devices from the bad guys.

Checklist

This chapter covers some key things you can do on your computer to reduce your “attack surface” and practice the policy of “least privilege.” That is, you need to reduce unnecessary risks, turn off features you don’t need that might be exploited, and set up some reasonable boundaries on who can do what on your computer.

Note Some of the tips in this checklist will require you to choose a password. In some cases, you will need a really strong password; in others, you will just need something moderately strong. I will make a recommendation in each case. But I want to be clear what I mean by “strong” and “moderate.”

- *Strong password:* Use BitWarden to generate a crazy, random password. It should be at least 20 characters long and include all the various types of characters. These passwords are used to protect really important things, specifically things that might be subject to a computerized (offline) attack.
- *Moderate password:* Use the techniques described in Chapter 5 for master passwords to come up with something at least ten characters long that you can easily remember. (You could also use a shorter passphrase, maybe four words.) These passwords will be used to protect your computer login and less important things and/or things that will require a human to sit there and guess them by hand (i.e., online attack).

If you have the option to specify a “password hint,” just use the phrase *BitWarden* or even *BW*. All of these passwords should be stored there, even the “moderately strong” ones that you should be able to memorize. You don’t actually want to give someone a hint that might allow them to make educated guesses.

Finally, note that many settings and changes on a PC will require admin access. I sometimes explicitly say this in the steps, but I’m sure I missed some. So be prepared periodically to be challenged for an admin ID and password. On Macs, you’ll often see padlock icons on settings—you’ll need to click this icon to unlock some settings, which will also require admin credentials.

Tip 6-1. Upgrade Your Computer

If your computer is so old that you can no longer install the latest operating system from Microsoft or Apple, then you should seriously consider getting a new computer. I know it's not cheap, but there are many low-cost options available, even from Apple.⁶

If you are a PC user, you might want to at least consider switching to a Mac the next time you upgrade your computer. While it's debatable whether Macs are inherently more secure than PCs, it's a fact that Macs are generally targeted less often by hackers—mostly because there are way more PCs out there than Macs. If you just use your computer for email and web browsing, you would probably not notice the difference. If you're a hard-core gamer or if you have some very specific applications you use that run only on Windows, then you're probably stuck with a PC.

If all you do on a computer is surf the Web and check email and you like the portability of a laptop, you might want to consider getting a Google Chromebook. A Chromebook is essentially a laptop that runs only Google Chrome (web browser) and some Google Play apps. They're affordable and not nearly as susceptible to malware. The downside to using a Chromebook is that you have to assume that Google pretty much knows everything you do on it.

Another great option for someone with simple needs is foregoing a computer completely and just using a tablet, like Apple's iPad. You can even use a physical keyboard and mouse with most tablets, making them almost like laptops. But the security features on tablets are usually much better than with regular computers.

Tip 6-2. ★ Require Passwords for Computer Accounts

I know this will seem like overkill, especially for desktop computers in your own home, but you should require some form of authentication to log in. If you live alone and never have other people in your house, I suppose you can let this slide. But if you have kids, guests, maids, contractors, or any other visitors, you should set your computer to require authentication to unlock. If you have the option to use biometric authentication, then it's really pretty easy.

⁶You can save a lot of money buying refurbished devices directly from Apple (I would avoid buying from others). They come with the same warranty and are indistinguishable from a new computer, other than the packaging. I've done this several times and have no regrets. You may need to keep an eye on what's in stock as it changes often.

Tip 6-2a. Microsoft Windows

Microsoft introduced Windows Hello several years ago and it's now the default for authenticating with a Windows device. Windows Hello allows you to sign in to a computer or device using a fingerprint or face scan (or a PIN code if you don't have a device with a fingerprint reader or camera that supports Hello). It's secure enough and I recommend it for most people. In this section, I'll show you how to set up Windows Hello using a PIN, which you should always have as an option in case biometric authentication is unavailable for some reason. If you have a biometric option, you can enable that in addition to the PIN method.

The instructions are very similar for both Windows 10 and 11. I'll show you screenshots here for Windows 11.

1. Open Settings and search for "sign-in requirements." Select "Change the sign-in requirements" and you should see your sign in options. Select the "PIN" option (Figure 6-1).

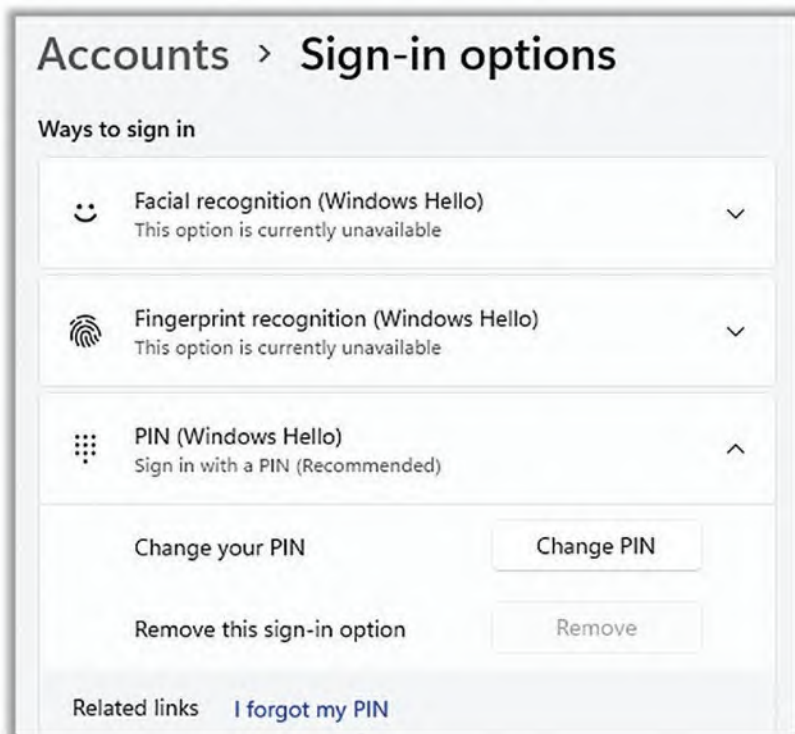


Figure 6-1. Windows 11 sign-in options

2. Windows has probably already forced you to set up Windows Hello at some point, but if not, you can set up or change your PIN here (Figure 6-2). If your PIN only contains numbers, you should change it to use letters and symbols, as well. Click “Change PIN” and check the box, as shown in Figure 6-2. Again, use a moderately strong password here.

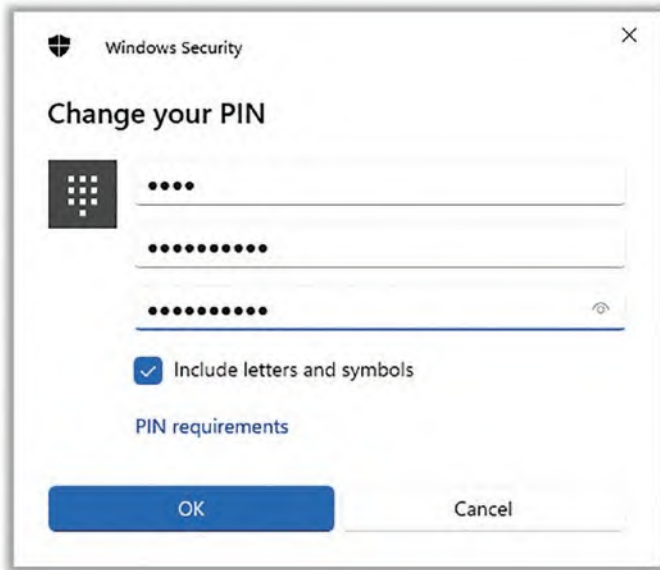


Figure 6-2. *Windows 11 Change your PIN*

3. Return to Sign-in options in Settings (as earlier). Scroll down and look for “Require sign-in.” Make sure “When PC wakes from sleep” is selected (Figure 6-3). Make sure it’s set to require sign-in when your PC wakes from sleep. Note: the Dynamic Lock feature is interesting—you can set your device to lock when you walk away from it, by pairing it with a device like your smartphone. If you’re interested in doing that, go ahead and click that option and follow the instructions.

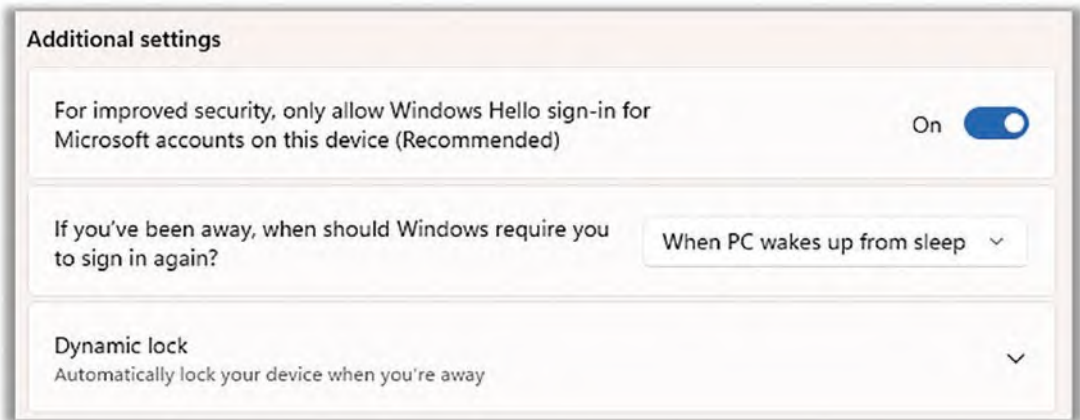


Figure 6-3. Windows 11 sign-in options, additional settings

4. Return to Settings and now search for “power.” Select “Power & sleep settings” (Windows 10) or “Power, Sleep & Screen Settings” (Windows 11). You’ll want to set these to some reasonable values that aren’t too long—maybe 10–20 minutes for a desktop computer and 1–5 minutes for laptops. The settings may look a little different for a laptop vs. a desktop, but it should look something like Figure 6-4.

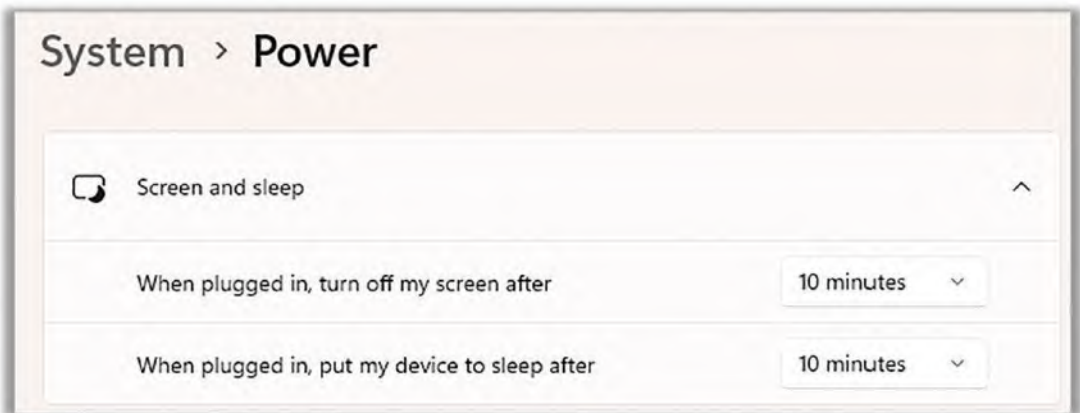


Figure 6-4. Windows 11 Power settings

Tip 6-2b. macOS Ventura

Mac OS requires passwords by default in most cases. If you can log in to your Mac without a password, follow the steps here to require a password (and disable automatic login). Also, make sure your computer is set to require a login after it goes to sleep.

1. Search System Settings for “users & groups.” Make sure “Automatic log in as” is set to “Off” (Figure 6-5).

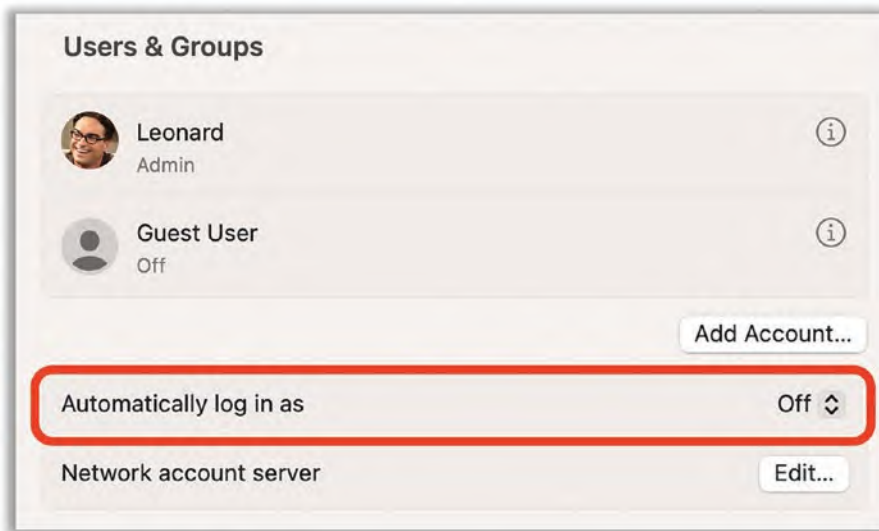


Figure 6-5. macOS Ventura Users & Groups

2. Now search System Settings for “lock screen.” You’ll want to set these to some reasonable values that aren’t too long—maybe 10–20 minutes for a desktop computer and 1–5 minutes for laptops. The settings may look a little different for a laptop vs. a desktop, but it should look something like Figure 6-6.

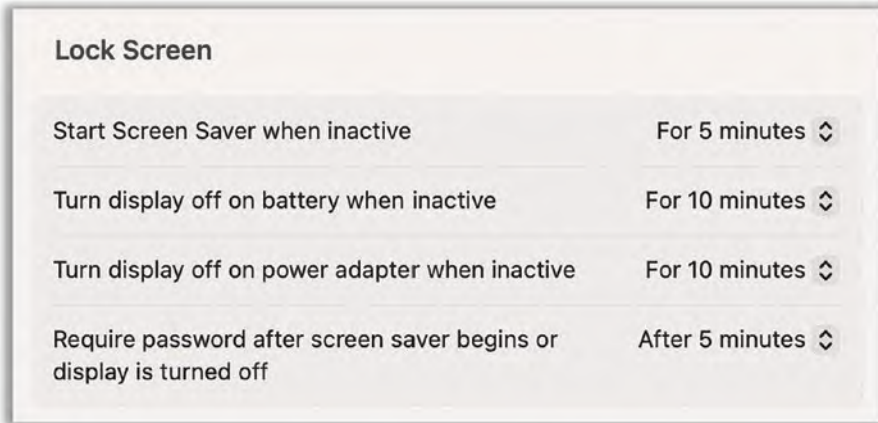


Figure 6-6. *macOS Ventura Lock Screen*

Tip 6-2c. macOS Monterey

Mac OS requires passwords by default in most cases. If you can log in to your Mac without a password, follow the steps here to require a password (and disable automatic login). Also, make sure your computer is set to require a login after it goes to sleep.

1. Search System Preferences for “users & groups.” Click the “Login Options” button at the lower left. Make sure “Automatic log in as” is set to “Off” (Figure 6-7).

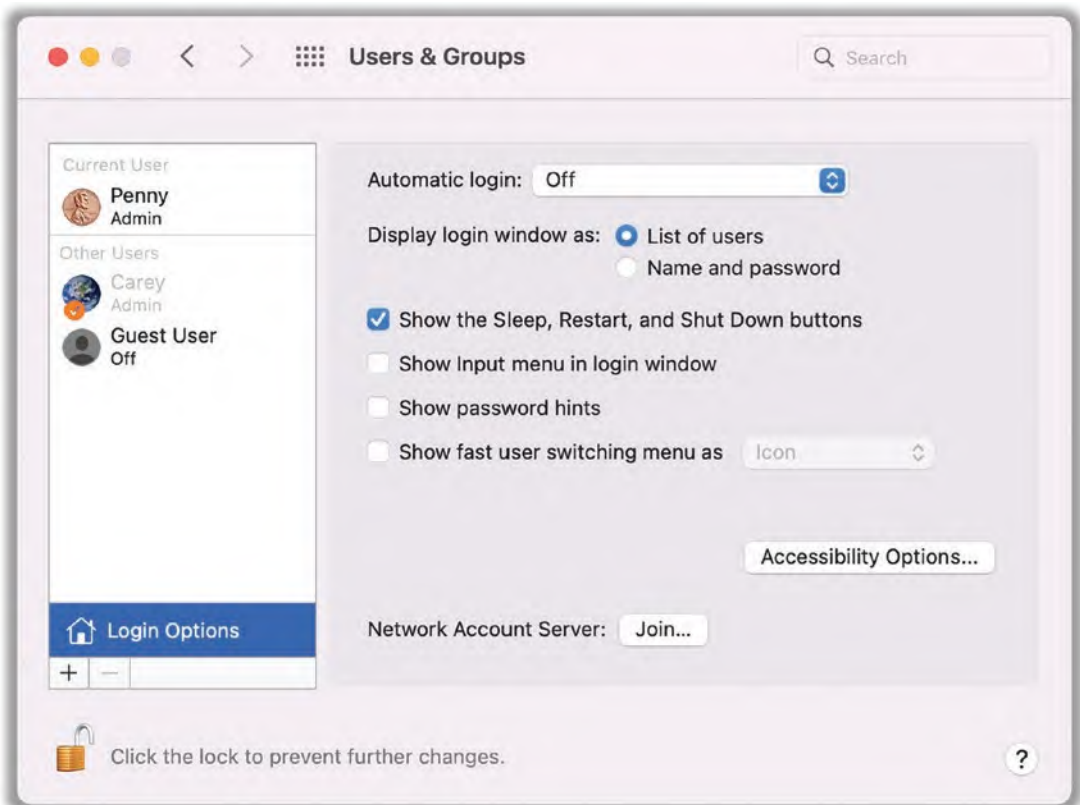


Figure 6-7. *macOS Monterey Users & Groups*

2. Now search System Preferences for “privacy & security.” You’ll want to set these to some reasonable values that aren’t too long—maybe 10–20 minutes for a desktop computer and 1–5 minutes for laptops (Figure 6-8). Also make sure “Disable automatic login” is checked.



Figure 6-8. macOS Ventura Lock Screen

Tip 6-3. ★ Create a Separate Admin Account

One of the best ways to limit the damage that can be done by malware is to limit yourself. Malware running on your computer can do whatever you can do. More accurately, malware running on your account will have the same permissions as your account does. Therefore, it’s best to have at least two accounts on your computer: an admin account for installing software and making system changes and a non-admin account for regular, day-to-day stuff.

We’re going to assume that you have only one account on your computer. (If you already have multiple accounts, then you just need to make sure that the special admin account is the only one with admin privileges.) This process is a bit tedious, but it’s not that hard. (This is probably the longest set of instructions in this book.) We’re going to do two main things here:

1. Create a new “admin” account with full administrative privileges.
2. Using this new admin account, we’ll *reduce the privileges* of your regular, day-to-day account

After you make these changes, you will need to enter the admin credentials whenever you install software or make certain system changes. On Macs, this may mean clicking the padlock icon on some settings and then entering your admin creds to enable changes. On PCs, this may mean right-clicking some apps and selecting “run as administrator.” The key here is that malware will not be able to use your non-admin privileges to do anything really nasty. If the malware tries to do anything that requires admin-level privileges, you will get a pop-up message asking for your admin credentials, which gives you a warning that something’s going on that you may want to investigate before proceeding.

These accounts will require you to choose a password. While you could use BitWarden to generate a strong password, you really need something you can easily remember and type by hand (you won’t be able to copy and paste this password). So, you should generate a moderately strong password here using the techniques we discussed in the previous chapter. If this computer is a desktop computer that will be used only within your home, you really don’t need a crazy long password here—eight characters is probably enough. If this is a laptop or if for some reason many strangers might have easy physical access to this computer, then you should make it 10 to 12 characters. Note that for almost all of my password hints, I just use “BitWarden” or even just “BW”—because I store all these passwords as secure notes in my BitWarden vault.

Note I will suggest that you create an admin account that is purely a local account and does not have an associated Microsoft or iCloud account. This is mostly to keep these instructions a little simpler. However, you should be able to associate your existing iCloud or Microsoft account with this new admin account through your web browser, too, if you wish.

Tip 6-3a. Microsoft Windows 11

Microsoft has made it very difficult to create Windows accounts that are not tied to a Microsoft account—but for our admin account, we ideally want a purely local account.

1. Open Settings and search for “other users.” Select “Family & Other Users.” Under “Other users,” click the “Add account” button next to “Add other user” (Figure 6-9).

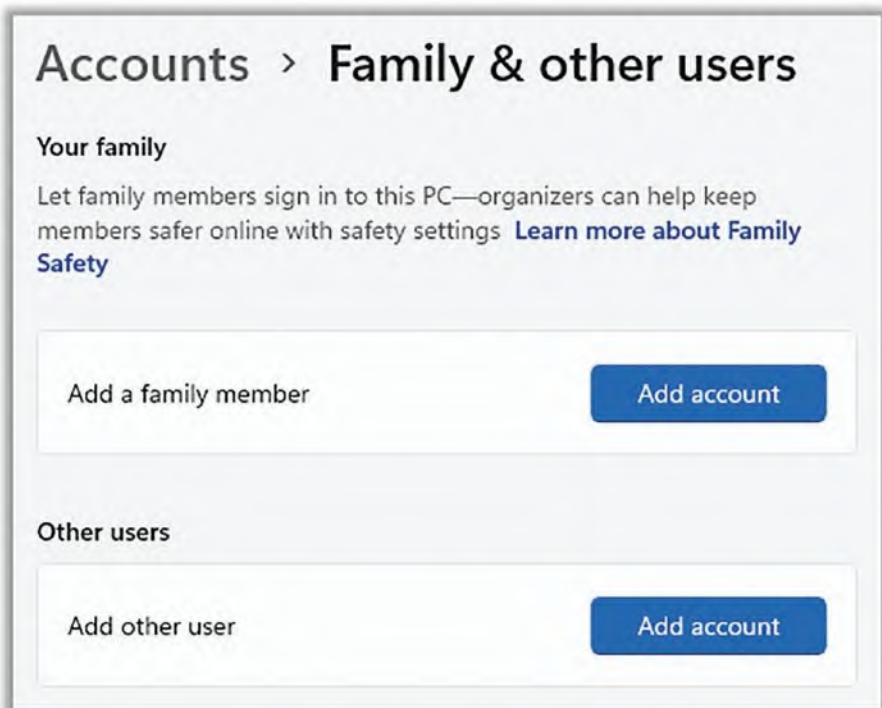


Figure 6-9. Windows 11 Family and other users settings

2. They make it hard to add a purely local account. Click the link at the bottom that says “I don’t have this person’s sign-in information” (Figure 6-10).

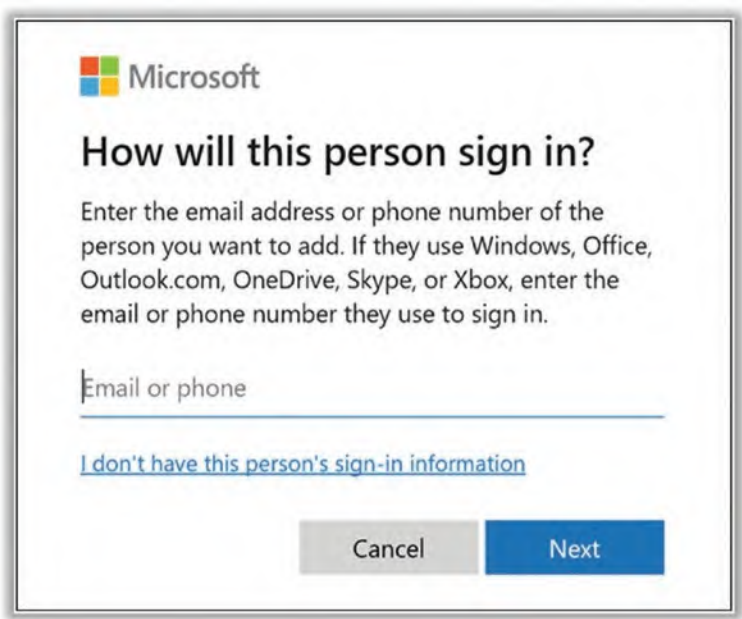


Figure 6-10. Windows 11 Create local account

- 3. At the bottom of the next page, click “Add a user without a Microsoft account” (Figure 6-11).

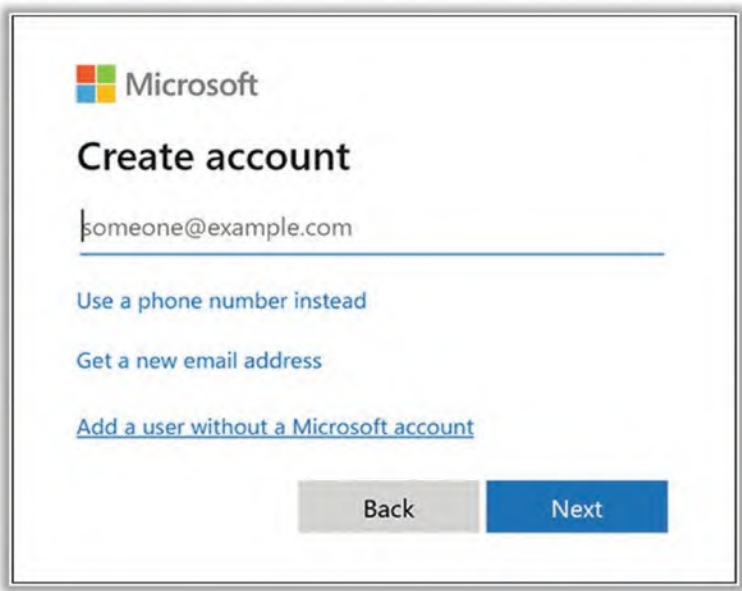
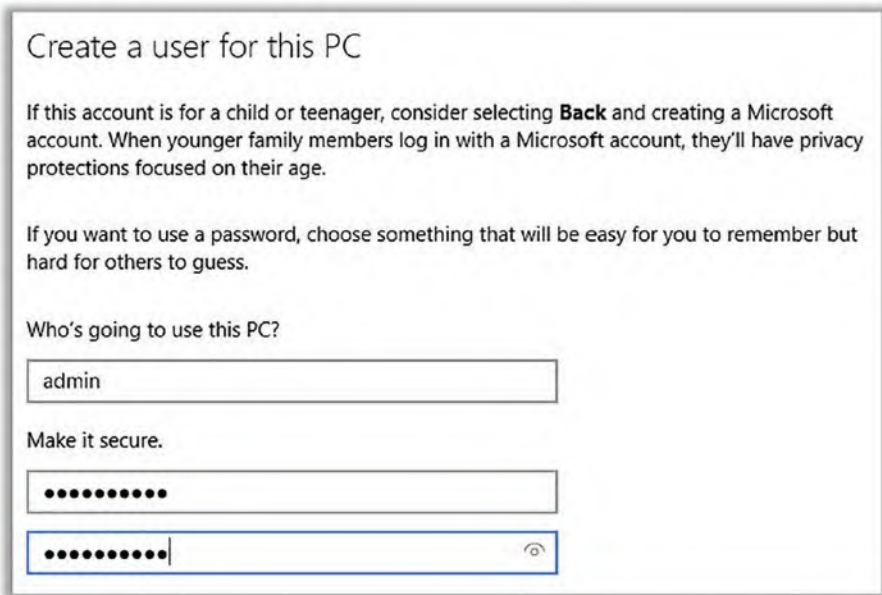


Figure 6-11. Windows 11 Add user without a Microsoft account

4. Create your account name. I personally prefer *admin*—short and to the point. Choose a moderately strong password and create a secure note in BitWarden, so you won’t forget it (Figure 6-12).



Create a user for this PC

If this account is for a child or teenager, consider selecting **Back** and creating a Microsoft account. When younger family members log in with a Microsoft account, they'll have privacy protections focused on their age.

If you want to use a password, choose something that will be easy for you to remember but hard for others to guess.

Who's going to use this PC?

admin

Make it secure.

.....

.....

Figure 6-12. Windows 11 Create account dialog

5. Below the name and password, Microsoft requires you to answer some security questions in case you forget your password. Choose your questions and enter your answers.⁷ I would also copy these questions and answers into the same BitWarden secure note as you saved the admin password in the previous step. Then click “Next” (Figure 6-13).

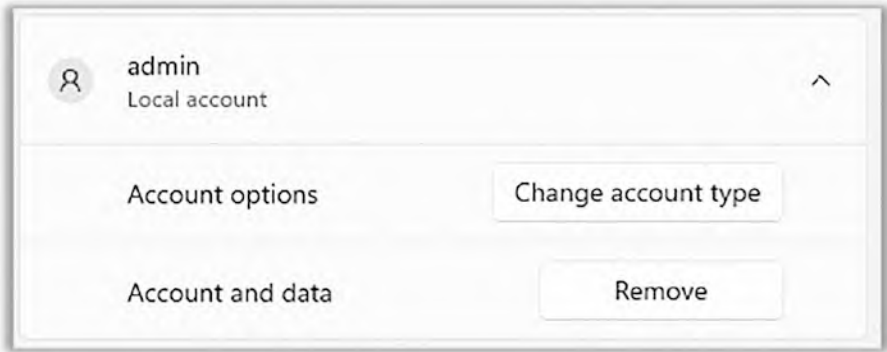
⁷I hate security questions for password recovery. It seriously weakens security—people that know you well (or check your Facebook account) can often answer them. In fact, for online accounts, I often recommend that you *lie*. We’ll discuss this in Chapter 10.



The screenshot shows a Windows 11 security questions dialog box. The title is "In case you forget your password". It contains four questions, each with a dropdown menu and a text input field. The first question is "What was your first pet's name?" with the answer "Fido". The second question is "What was your childhood nickname?" with the answer "Stretch". The third question is "What's the name of the city where your parents met?" with the answer "New Orleans". At the bottom right, there are two buttons: "Next" (blue) and "Back" (gray).

Figure 6-13. Windows 11 Answer security questions

- 6. You need to now enable admin privileges for this account. Once again, select “Family & other users” and then click the new admin account. When you click it, you should see the options as in Figure 6-14.



The screenshot shows the Windows 11 "Change account type" dialog box. At the top, it shows the account name "admin" and "Local account". Below this, there are two sections: "Account options" and "Account and data". In the "Account options" section, there is a button labeled "Change account type". In the "Account and data" section, there is a button labeled "Remove".

Figure 6-14. Windows 11 Change account type dialog

- 7. Click “Change account type.” On the next dialog, set the account type to Administrator (Figure 6-15).

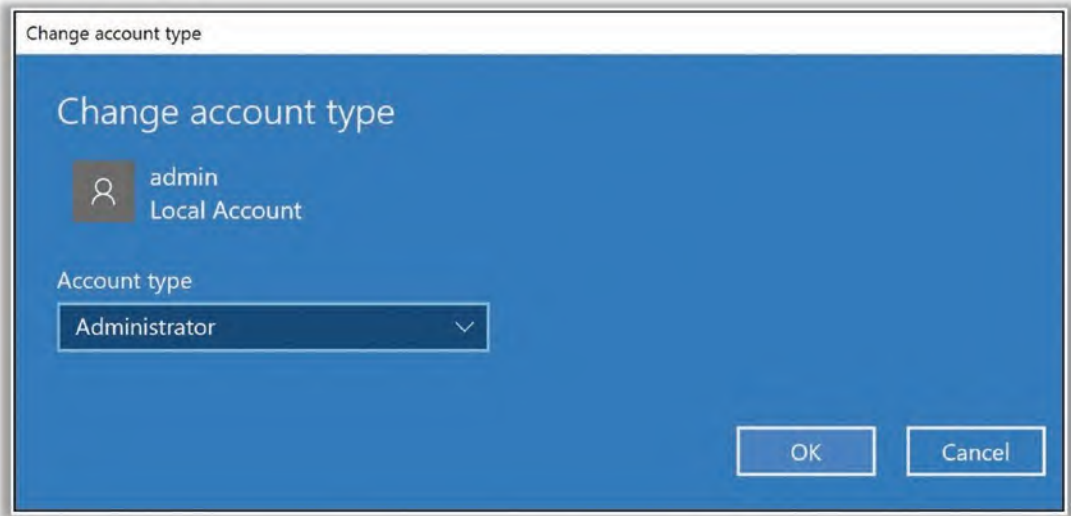


Figure 6-15. Windows 11 Change account type to administrator dialog

8. Log out of your current account, and log back in to your new admin account. Do this by clicking the Windows icon at the bottom and clicking your current account name. From this new menu, select “Sign out”. (Note: Don’t just switch directly to the new admin account—you need the current account to be logged out for the changes to take effect.) See Figure 6-16.

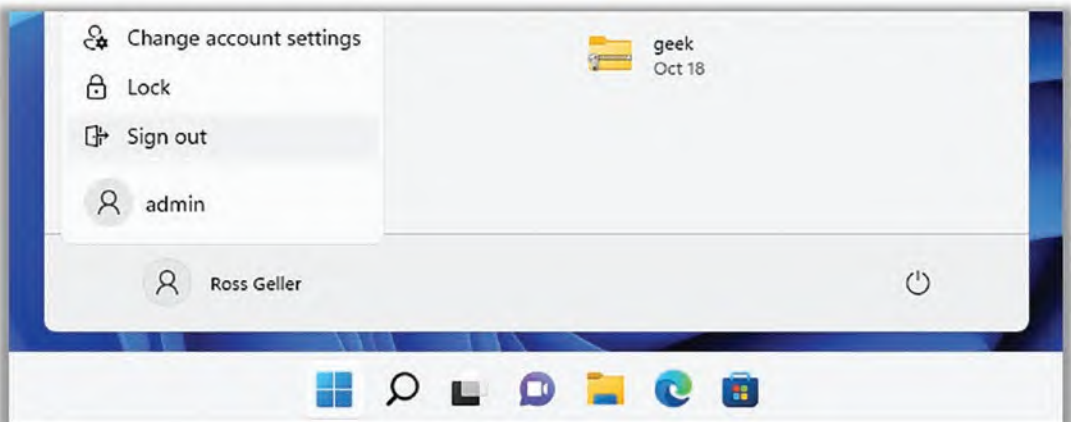


Figure 6-16. Windows 11 Sign-out menu

9. Now sign in to your new admin account. Click “admin” on the login screen at the lower left (Figure 6-17).

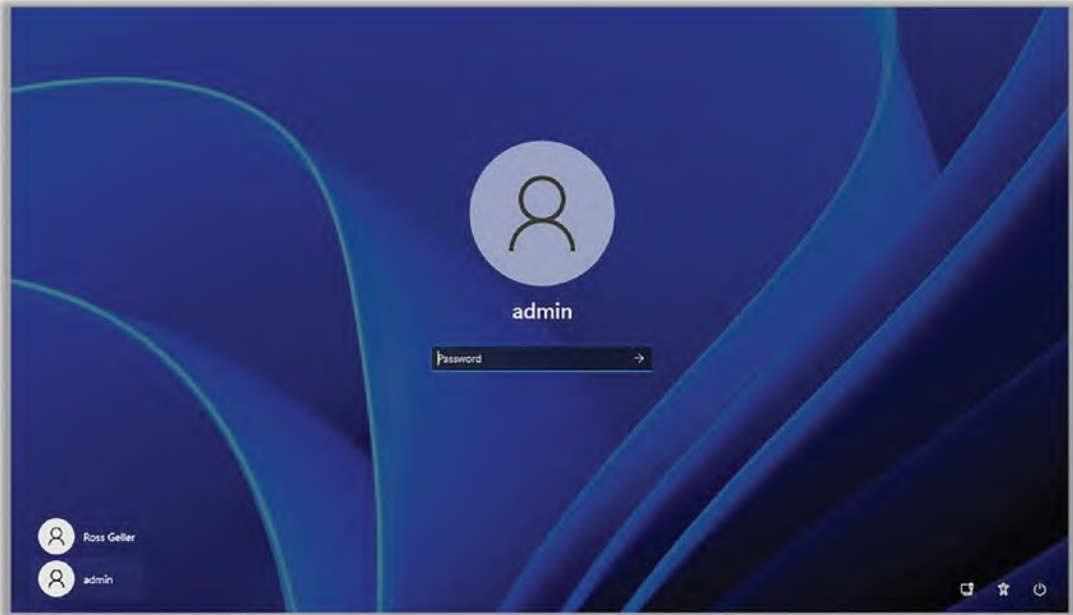


Figure 6-17. *Windows 11 Login screen*

10. You’ll have to sit through some welcome messages while your new account is set up. One of the windows will have privacy settings (Figure 6-18). I suggest you disable everything (scroll down through the entire list of options). Note that we’ll adjust some of these settings later in the book.

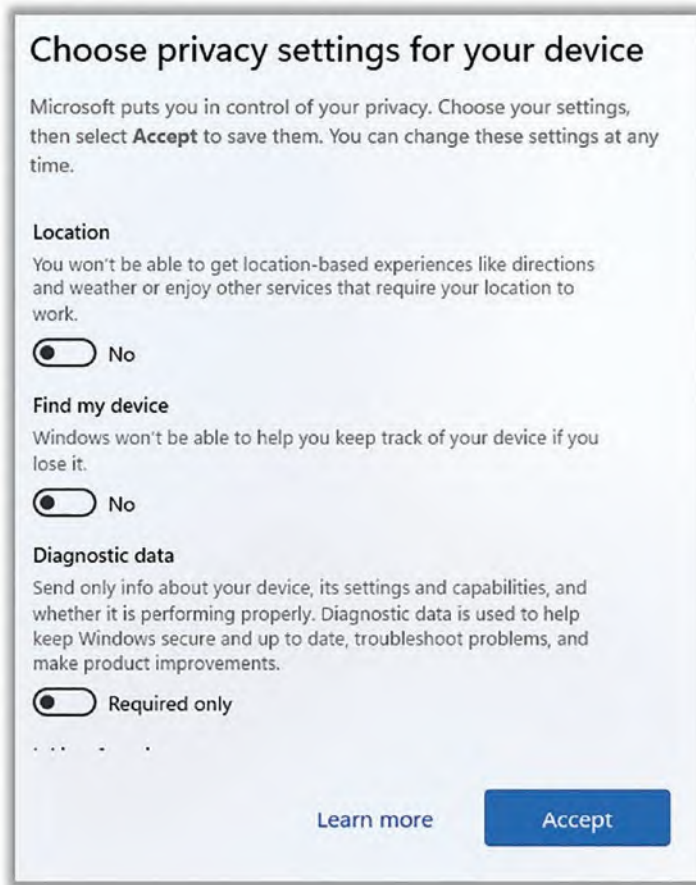


Figure 6-18. Windows 11 New account privacy settings

11. When account setup completes, open Settings and search for “other users” and select “Family & Other Users” (as we did earlier). This time click your personal account (“Ross” in our example). Then click “Change account type” (Figure 6-19).

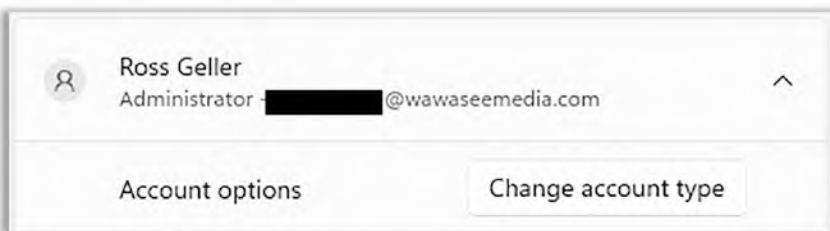


Figure 6-19. Windows 11 Change account type dialog

12. Change the account type to Standard User and click “OK” (Figure 6-20).

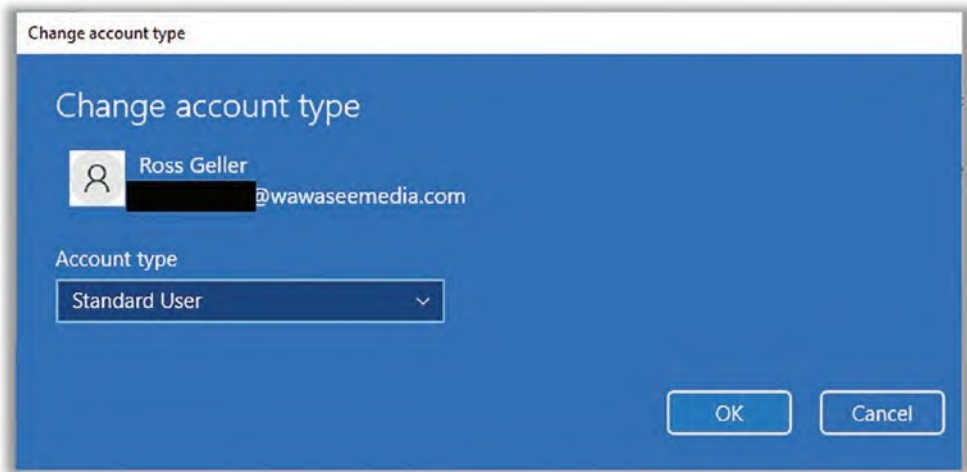


Figure 6-20. *Windows 11 Change account type to standard user dialog*

13. Repeat the logout and login procedure, switching back to your regular account. Your regular account is now restricted, which will prevent malware that gets by your other defenses from doing too much harm. If you run into a situation where you need admin privileges, you can log in to your admin account or simply enter the admin account credentials when asked.

Whew! That was a long one! But this one step will make you a lot more secure, particularly on Windows!

Tip 6-3b. Microsoft Windows 10

Microsoft has made it very difficult to create Windows accounts that are not tied to a Microsoft account—but for our admin account, we ideally want a purely local account.

1. Open Settings and search for “accounts.” Select “Add, edit, or remove other users.” Under “Other users,” click the plus sign next to “Add someone else to this PC” (Figure 6-21).



Figure 6-21. Windows 10 Family and other users settings

2. They make it hard to add a purely local account. Click the link at the bottom that says “I don’t have this person’s sign-in information” (Figure 6-22).



Figure 6-22. Windows 10 Create local account

3. At the bottom of the next page, click “Add a user without a Microsoft account” (Figure 6-23).

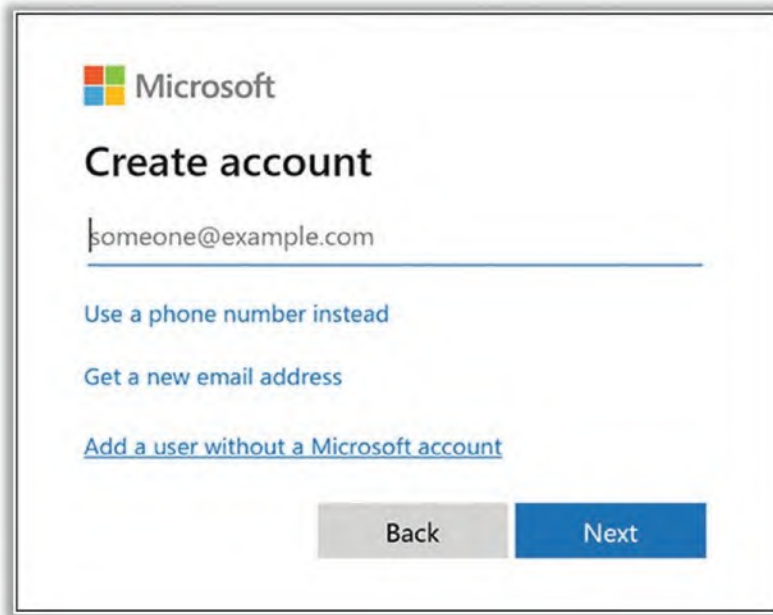
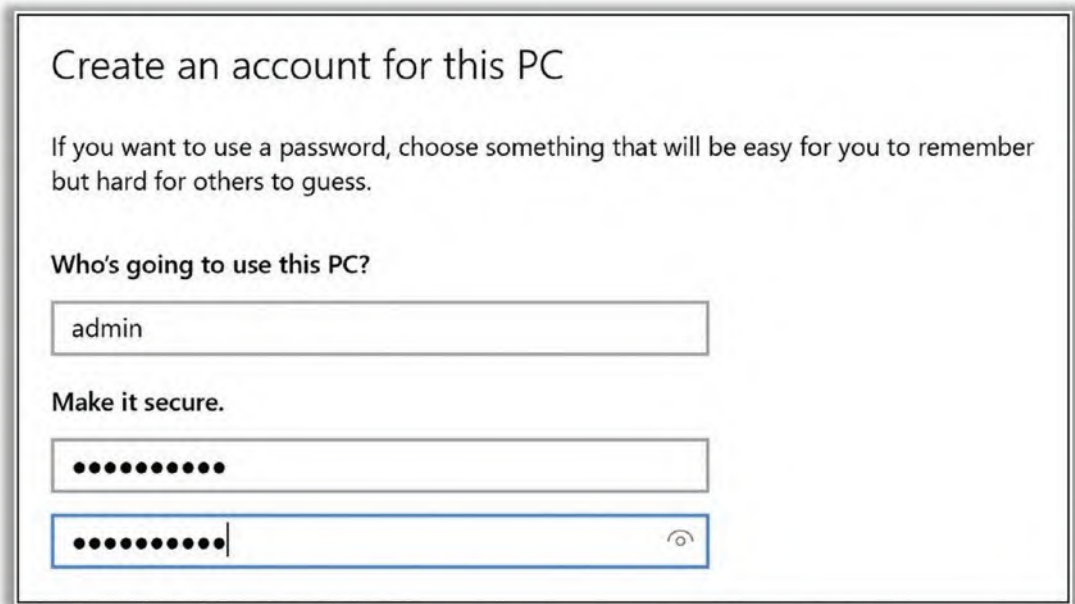


Figure 6-23. *Windows 10 Add user without a Microsoft account*

4. Create your account name. I personally prefer *admin*—short and to the point. Choose a moderately strong password and create a secure note in BitWarden, so you won’t forget it (Figure 6-24).



The screenshot shows the 'Create an account for this PC' window. At the top, it says 'Create an account for this PC'. Below that, a message reads: 'If you want to use a password, choose something that will be easy for you to remember but hard for others to guess.' The first section is 'Who's going to use this PC?' with a text box containing 'admin'. The second section is 'Make it secure.' with two password fields. The first password field is filled with dots. The second password field is also filled with dots and has a blue border, indicating it is the active field. To the right of the second password field is an eye icon, which is currently closed (represented by a diagonal line through the eye).

Figure 6-24. *Windows 10 Create account dialog*

5. Below the name and password, Microsoft requires you to answer some security questions in case you forget your password. Choose your questions and enter your answers.⁸ I would also copy these questions and answers into the same BitWarden secure note as you saved the admin password in the previous step. Then click “Next” (Figure 6-25).

⁸I hate security questions for password recovery. It seriously weakens security—people that know you well (or check your Facebook account) can often answer them. In fact, for online accounts, I often recommend that you *lie*. We’ll discuss this in Chapter 10.

In case you forget your password

What was your first pet's name?

Fido

What was your childhood nickname?

Stretch

What's the name of the city where your parents me

New Orleans

Next

Back

Figure 6-25. Windows 10 Answer security questions

- 6. You need to now enable admin privileges for this account. Once again, select “Family & other users” and then click the new admin account. When you click it, you should see the options as in Figure 6-26.



admin

Local account

Change account type

Remove

Figure 6-26. Windows 10 Change account type dialog

7. Click “Change account type.” On the next dialog, set the account type to Administrator (Figure 6-27).

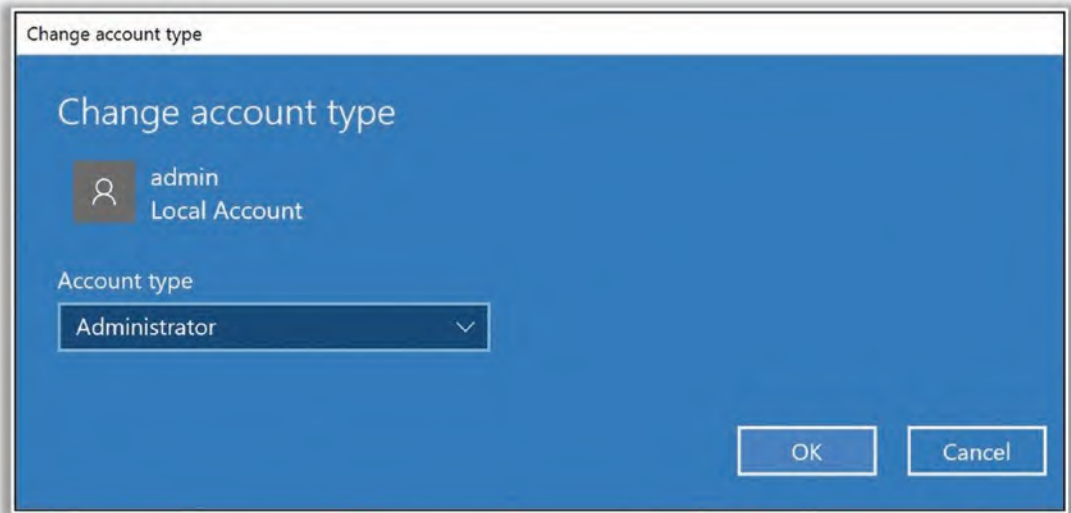


Figure 6-27. *Windows 10 Change account type to administrator dialog*

8. Log out of your current account, and log back in to your new admin account. Do this by clicking the Windows icon at the lower left and clicking your current account name. From this new menu, select “Sign out.” (Note: Don’t just switch directly to the new admin account—you need the current account to be logged out for the changes to take effect.) See Figure 6-28.

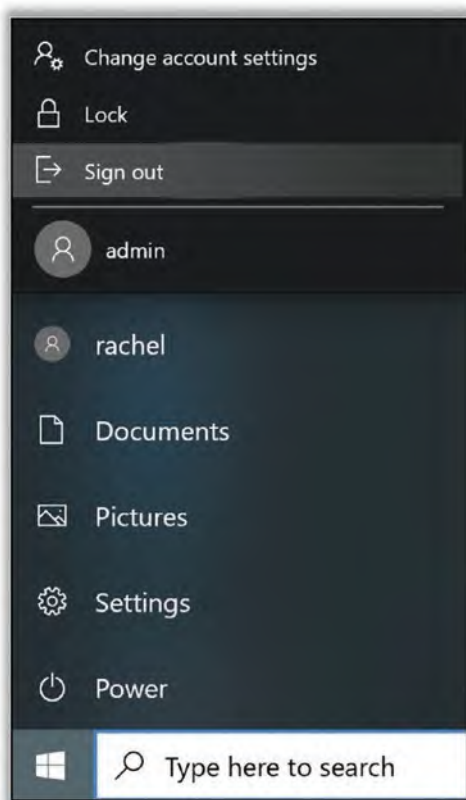


Figure 6-28. *Windows 10 Sign-out menu*

9. Now sign in to your new admin account. Click “admin” on the login screen at the lower left (Figure 6-29).

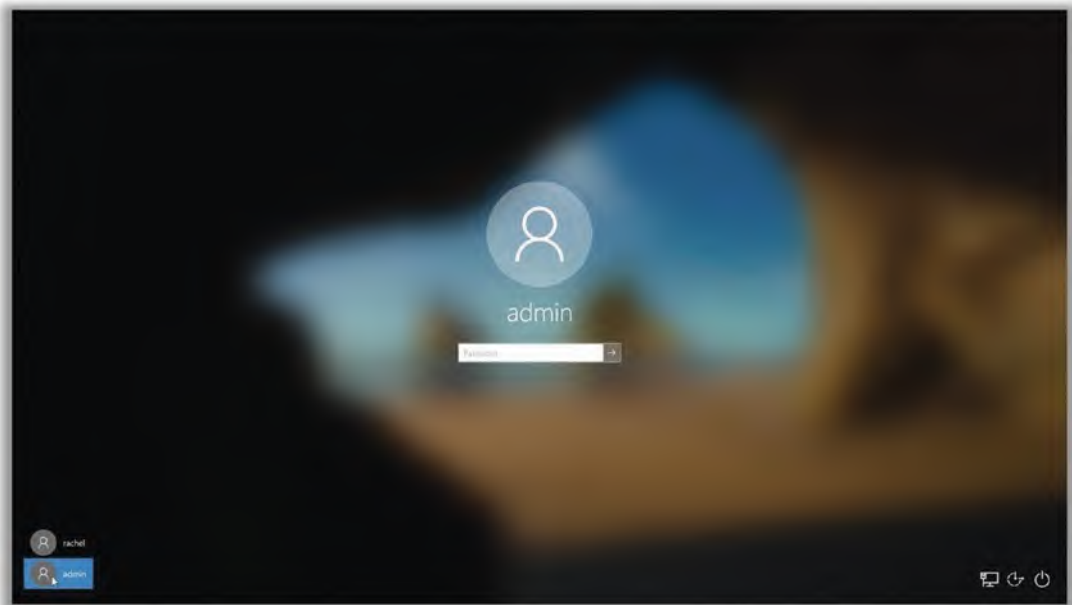


Figure 6-29. *Windows 10 Login screen*

10. You'll have to sit through some welcome messages while your new account is set up. One of the windows will have privacy settings. I suggest you disable everything as shown in Figure 6-30. Note that we'll adjust some of these settings later in the book.

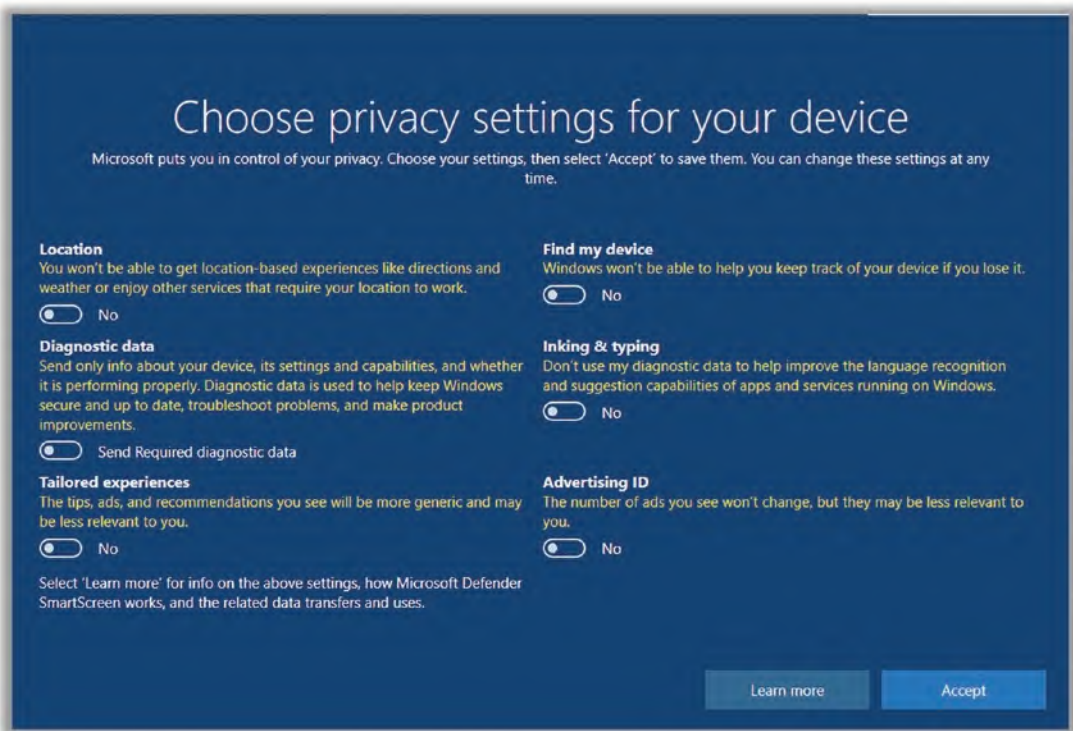


Figure 6-30. Windows 10 New account privacy settings

- 11. When account setup completes, open Settings and go to “accounts” and select “Add, edit, or remove other users” (as we did earlier). This time click your personal account (“rachel” in our example). Then click “Change account type” (Figure 6-31).



Figure 6-31. Windows 10 Change account type dialog

12. Change the account type to Standard User and click “OK” (Figure 6-32).

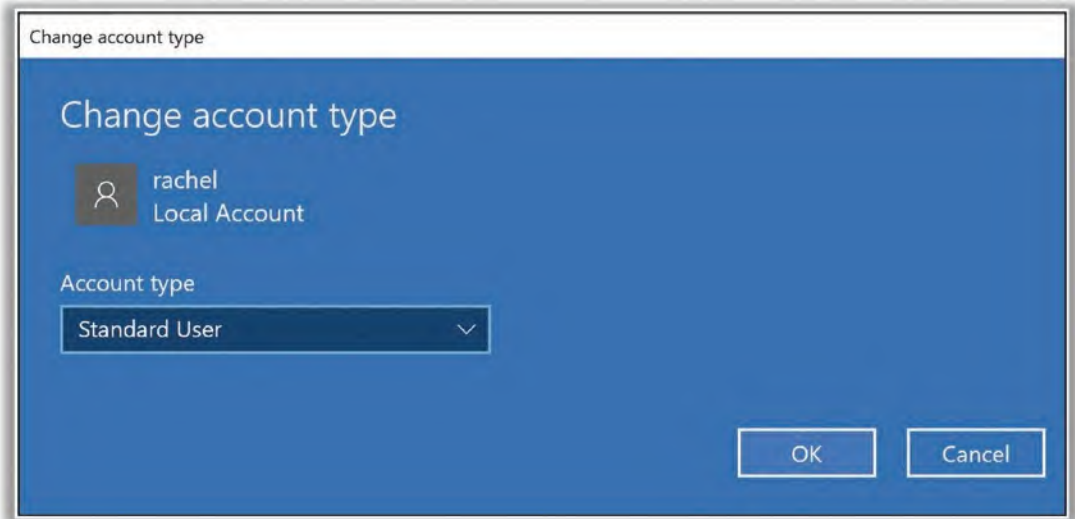


Figure 6-32. Windows 10 Change account type to standard user dialog

13. Repeat the logout and login procedure, switching back to your regular account. Your regular account is now restricted, which will prevent malware that gets by your other defenses from doing too much harm. If you run into a situation where you need admin privileges, you can log in to your admin account or simply enter the admin account credentials when asked.

Whew! That was a long one! But this one step will make you a lot more secure, particularly on Windows!

Tip 6-3c. macOS Ventura

1. From the Apple menu, open System Settings and search for “users & groups,” and then open this settings panel (Figure 6-33).



Figure 6-33. macOS Ventura users & groups

- 2. Click the “Add Account” button under the list of accounts. If asked, enter your computer account credentials. Choose an account name. I personally prefer *admin*—short and to the point. You can add a password hint. I usually just use *BitWarden* because that’s where I’ll store a copy of this info for future reference. Click Create User to finish (Figure 6-34).

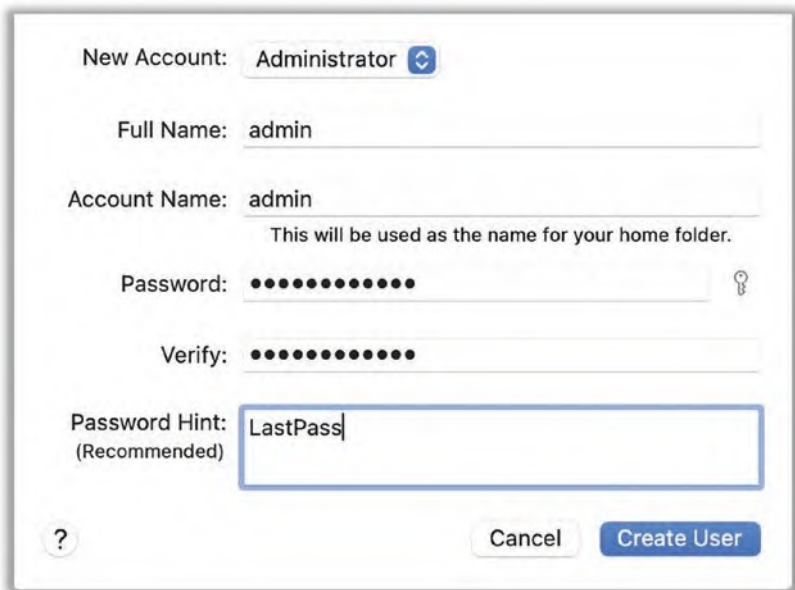


Figure 6-34. macOS Ventura Administrator password dialog

3. Now we need to remove admin privileges from your regular account—in this example, Leonard. To do this, you need to log out of your current account and log back in as the admin account. In the Apple menu, select “Log Out Leonard” (Figure 6-35).



Figure 6-35. *macOS Ventura Logout menu*

4. You should now see a list of your accounts (the login screen). Select your admin account and log in using the password you just chose. You will have to go through some initial account setup questions. You can skip most of these by clicking the “Skip” or “Set Up Later” link toward the bottom of each window. You will rarely log in directly to this account, so many of these won’t matter.
5. Once you’re logged in to the new admin account, go back to the Users & Groups settings, as we did earlier. Click the little “i” in a circle icon next to your regular account (in my example, Leonard—see Figure 6-36). Then uncheck the box that says “allow this user to administer this computer.” If asked, enter your new administrator credentials.

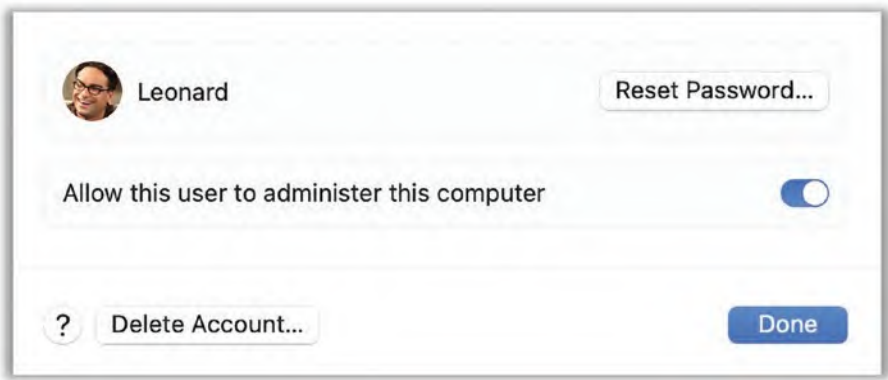


Figure 6-36. *macOS Ventura Disable administrator privileges*

6. You should get a dialog like Figure 6-37. Click OK.

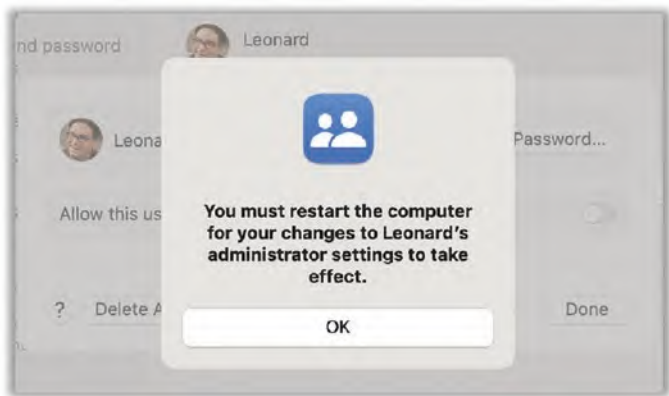


Figure 6-37. *macOS Ventura Remove administrator confirmation dialog*

7. From the Apple menu, restart your computer to make the changes take full effect. See Figure 6-38.

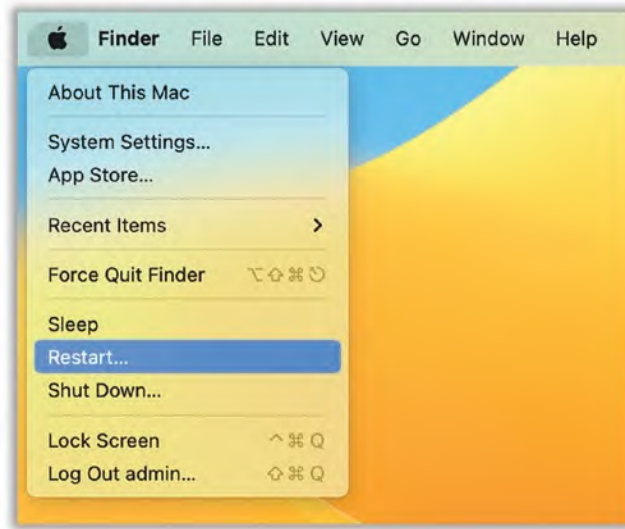


Figure 6-38. *macOS Ventura Restart menu*

8. You can now log back in as your original user (“leonard” in our example). If you try to install new software or change key system settings, you will be prompted for the administrator credentials. Whenever you need to unlock the settings padlock icon, you’ll also usually need admin credentials.

Tip 6-3d. macOS Monterey

1. From the Apple menu, open System Preferences and search for “users & groups.” If the lock icon at the lower left is locked, click the icon and enter your password to unlock these settings. Click the little + (plus) sign under the list of accounts to create a new account (Figure 6-39).

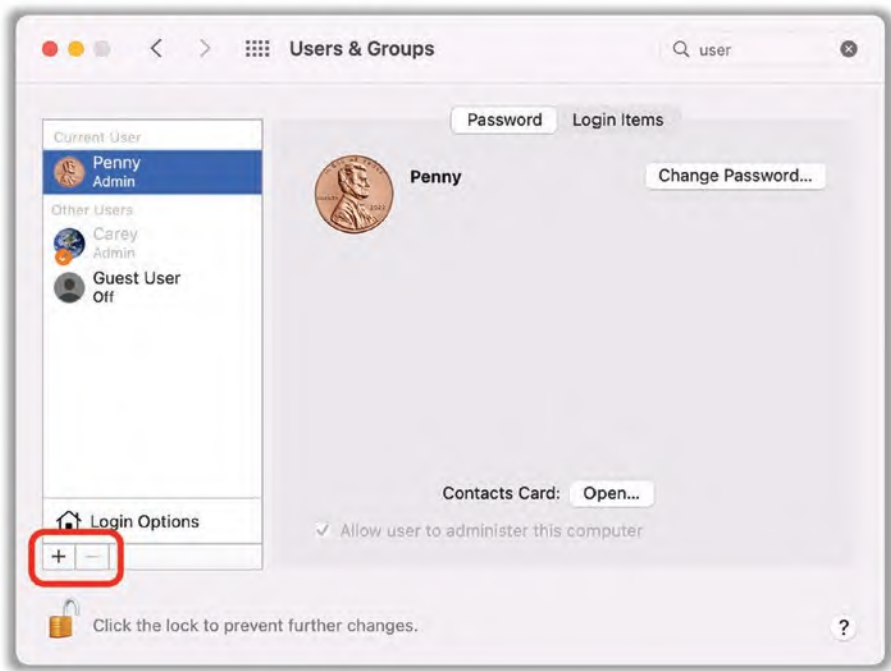


Figure 6-39. macOS Monterey users & groups

- 2. Choose an account name. I personally prefer *admin*—short and to the point. You can add a password hint. I usually just use “BW” or “BitWarden” because that’s where I’ll store a copy of this info for future reference. Click Create User to finish (Figure 6-40).

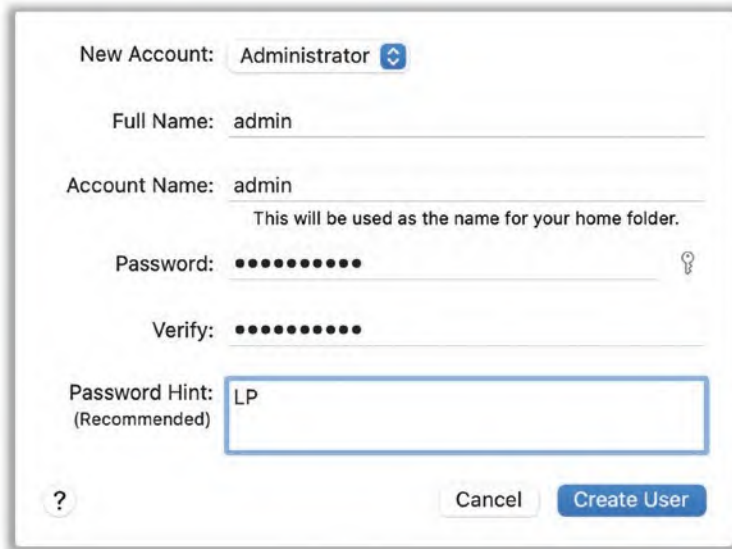


Figure 6-40. macOS Monterey Administrator password dialog

3. Now we need to remove admin privileges from your regular account—in this example, Penny. To do this, you need to log out of your current account and log back in as the admin account. In the Apple menu, select “Log Out Penny” (Figure 6-41).

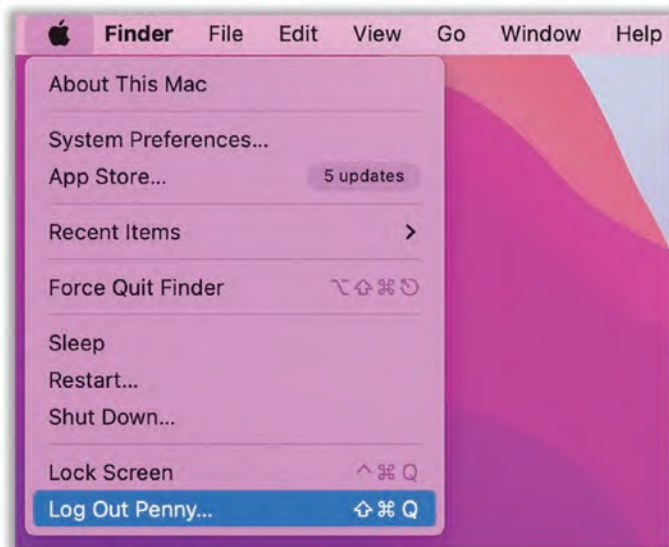


Figure 6-41. macOS Monterey Logout menu

4. You should now see a list of your accounts on the login screen. Select your admin account and log in using the password you just chose. You will have to go through some initial account setup questions. You can skip most of these by clicking the “Skip” or “Set Up Later” link toward the bottom of each window. You will rarely log in directly to this account, so many of these won’t matter.
5. Once you’re logged in to the new admin account, go back to the Users & Groups settings, as we did earlier. Again, click the lock icon to unlock the settings.
6. Click the entry for your original Mac account at the left (“penny” in the example here). Then uncheck the “Allow user to administer this computer” box. You should get a dialog like Figure 6-42. Click OK.

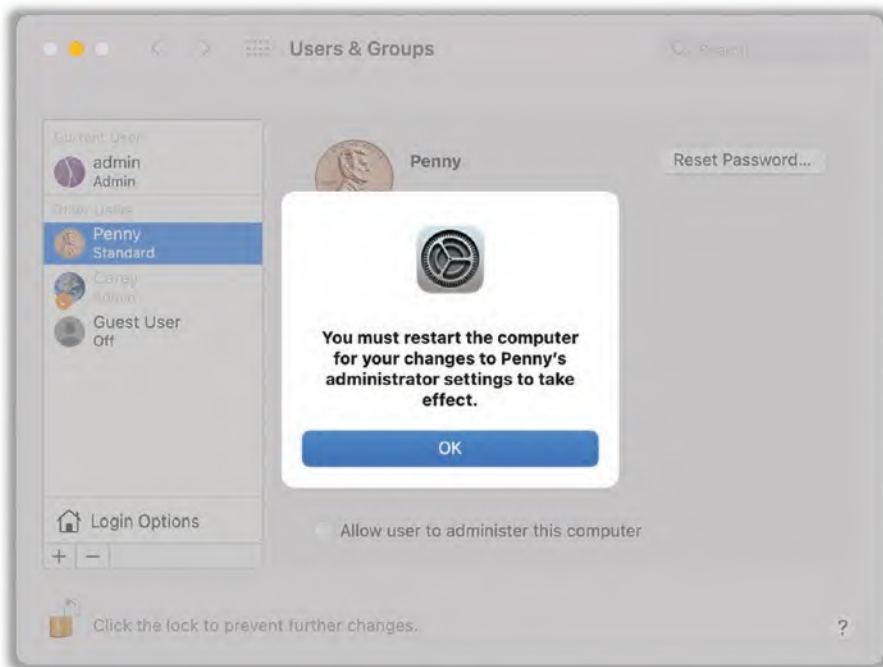


Figure 6-42. macOS Monterey Remove administrator confirmation dialog

7. From the Apple menu, restart your computer to make the changes take full effect. See Figure 6-43.

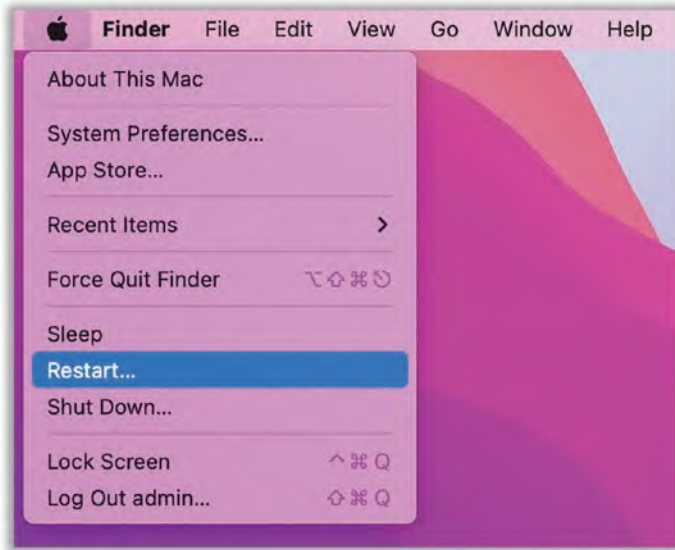


Figure 6-43. *macOS Monterey Restart menu*

8. You can now log back in as your original user (“penny” in our example). If you try to install new software or change key system settings, you will be prompted for the administrator credentials. Whenever you need to unlock the settings padlock icon, you’ll also usually need admin credentials.

Tip 6-4. Install Free Antivirus Software

Antivirus (AV) software used to be a must-have for any computer owner. But lately, the effectiveness of AV software has become questionable. Furthermore, many AV products have become overzealous in their protection schemes by embedding themselves deeply into your operating system so that they can monitor network traffic and inspect all files. In doing this, they often do more harm than good—in some cases, it’s been shown that AV software itself is either causing problems or creating new vulnerabilities for hackers to exploit.

For these reasons and others, I feel that most people should forego expensive antivirus software products. You'll do a better job protecting yourself using all the other tips in this book. However, there are good and totally free software utilities for protecting your computer that I can recommend, if you feel you'd like to have some sort of AV software installed. (If you have a teenager in the house, it's probably best to have AV software installed at least for their account.)

Note If you already have another antivirus program installed, you should disable and remove it before installing new AV software. If you've subscribed to this service, be sure to unsubscribe!

Tip 6-4a. Windows

Windows 10 and 11 come with Windows Defender preinstalled, and it should be enabled by default. You just need to verify that it is enabled and configured properly. The screenshots for Windows 10 and 11 look very similar.

1. Open Settings and search for "security" and select "Windows Security." You want to see green check marks on all of these, as shown in Figure 6-44. In particular, right now we're concerned with "Virus & threat protection." If this item doesn't have a green check mark, click it and check the settings. (Note that if there's a yellow warning sign asking you to set up OneDrive, you can click "Dismiss." We'll discuss better options later.)

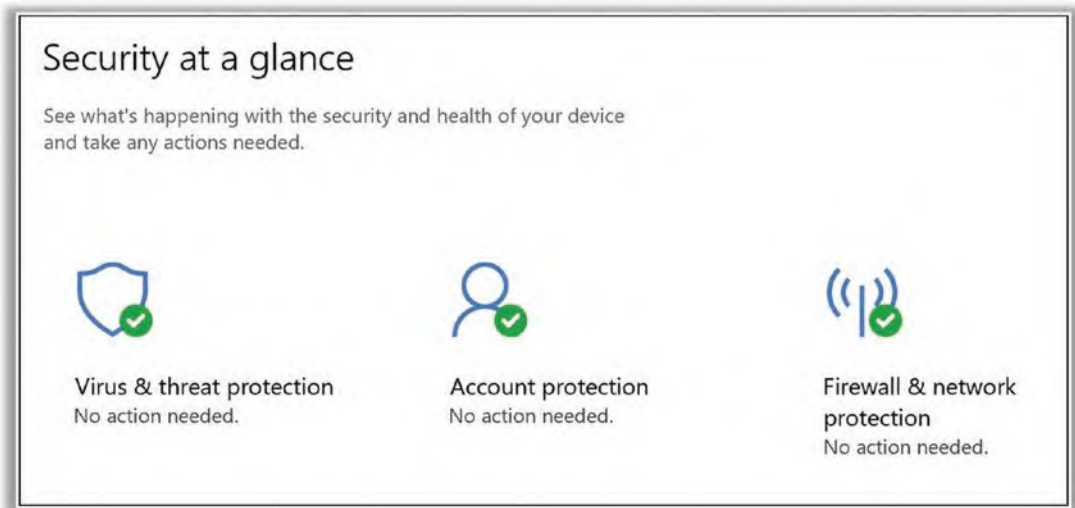


Figure 6-44. Windows Security status

2. Click "Virus & threat protection," and then scroll down to find the "Virus & threat protection settings" section. Then click "Manage settings" (Figure 6-45).

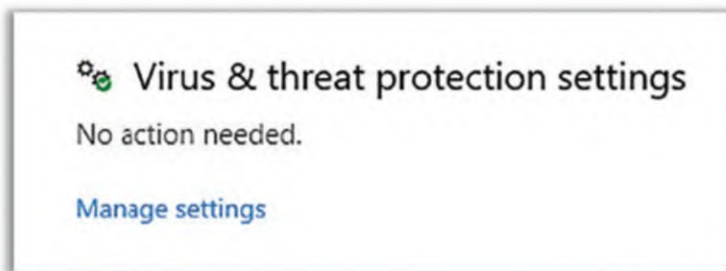


Figure 6-45. Windows Virus and threat protection settings

- 3. Make sure the top 4 items are on, as shown in Figure 6-46. (We'll talk about "Controlled folder access" in the next tip.)

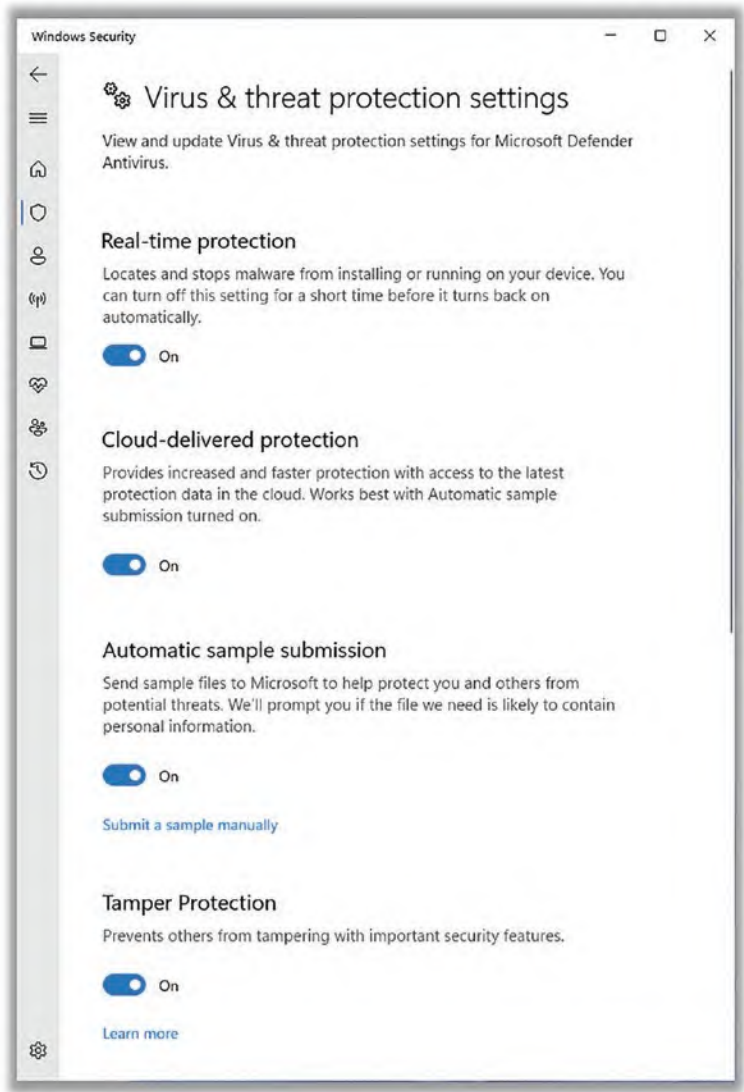


Figure 6-46. Windows Virus and threat protection settings detail

Tip 6-4b. macOS

Modern Mac computers come with some basic anti-malware protection built in to the operating system, but it's not a full-fledged antivirus program. In most cases, this is all you really need, if you follow the other tips in this book.

There are a few decent, free applications for Mac. Unfortunately, the capabilities and efficacy of these applications change constantly. These third-party programs are often adding features that break your encrypted Internet connections in an attempt to see everything you're doing. These techniques are dangerous and can lead to some severe vulnerabilities.

The other issue is that AV software online reviews are horribly biased due to “affiliate programs” that give sites a kickback for referrals. Even if you trust these review sites, they all have different recommendations as to what's best. It's hard to pick a winner.

If all of that weren't bad enough, AV software is horrible for privacy. Like a bodyguard, to do their job they need full, unfettered access to all your files and all your web surfing. Unlike a bodyguard, they will gather and resell your information. They'll claim it's all anonymous or aggregated, but even if that's true, mistakes will happen.

Honestly, I've personally decided not to install AV software at all on my Macs. But if you decide you really want this, I would look at the free version of Malwarebytes. You can also find some interesting free security tools from Objective-See, like Block Block and RansomWhere.

<https://objective-see.org/tools.html>

Tip 6-5. Restrict Access to Important Files

Both Microsoft and Apple now have built-in mechanisms to restrict access to key folders and files. In both cases, the feature is aimed at blocking ransomware and other malware from adding, changing, or deleting files in selected folders and system files. Some already-trusted applications (like the built-in apps) will automatically be given access, but other applications will need to be explicitly “whitelisted” in order to access your files. This will probably mean you'll get some pop-up messages asking whether to allow this or that app access to your protected folders, but you should only have to do this once per application. In my opinion, with ransomware as prevalent and devastating as it is, I think this is a good trade-off of security over convenience.

Tip 6-5a. Windows

Microsoft has a nice feature called “Controlled folder access” to protect your files.

1. To enable this feature, go to the same security settings area we went to in the last tip, under “Virus & threat protection settings.” Scroll down to “Controlled folder access” and click “Manage Controlled folder access” (Figure 6-47).

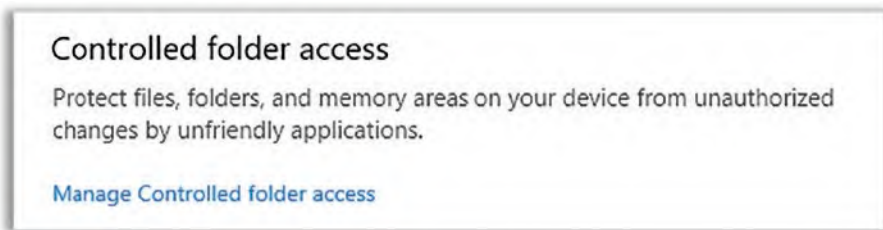


Figure 6-47. Windows Controlled folder access

2. Enable “Controlled folder access” (Figure 6-48).



Figure 6-48. Windows Controlled folder access settings

3. You can see what folders are protected and add other folders by clicking “Protected folders.”

4. If you already know of some applications you want to add to the approved list, you can add it using the “Allow an app through Controlled folder access” here. Otherwise, you will be prompted to approve each application when they try to access your files.

Tip 6-5b. macOS Ventura

Apple has built-in protections for many key aspects of your computer—not just important files and folders but also your built-in microphone and camera, location, and other privacy-oriented settings. These security settings are enabled by default, and you’ve probably already seen pop-up dialogs asking for you to give permission to access this or that. But it’s still good to know where these settings are in case you want to revoke any of these privileges.

1. Open System Settings and search for “security,” and then open “Security & Privacy” settings. You’ll find a long list of security and privacy settings (Figure 6-49). It’s good to periodically review these settings to make sure that you haven’t accidentally granted permission to some application, or you want to rescind your permission. But for now, we’ll focus on files and folders.



Figure 6-49. macOS Ventura Privacy & Security settings

2. The two settings to check here are “Files & Folders” and “Full Disk Access” (Figure 6-50).

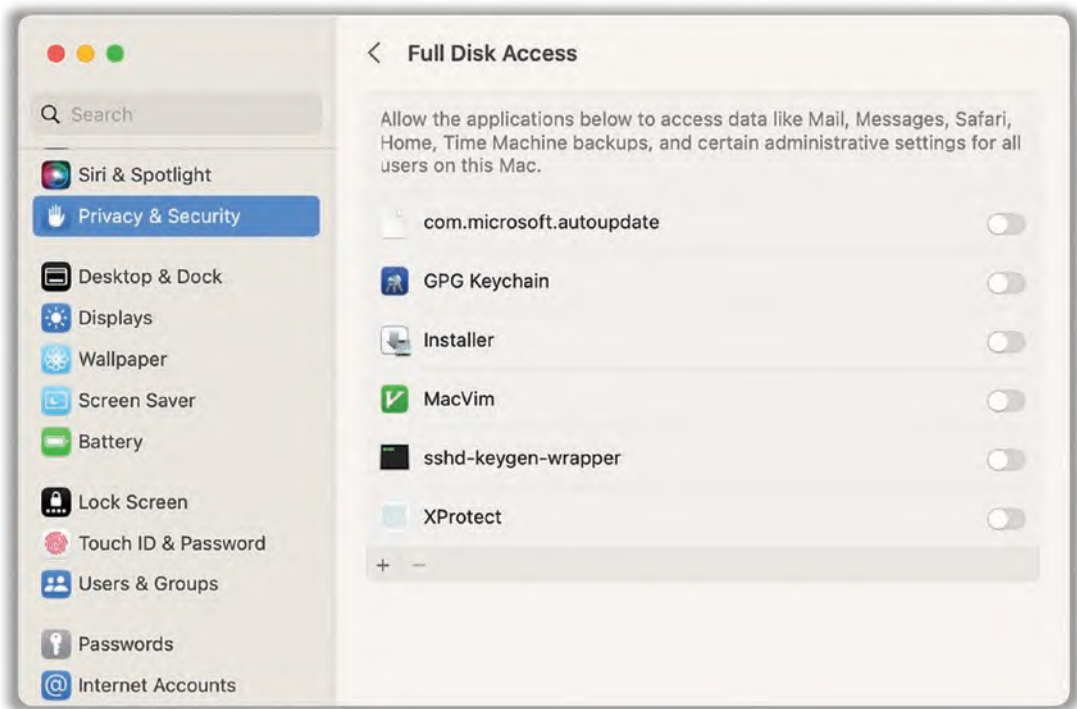


Figure 6-50. *macOS Ventura Security and Privacy, Full Disk Access*

3. You’ll want to look at all the applications in both of these areas to make sure you want to allow those applications to have access. Full Disk Access is pretty much what it sounds like—access to every file and folder. This is necessary for backup apps like Backblaze, but most apps will only need access to specific folders like Documents. To remove an app (i.e., remove their access privileges), select it by clicking it and then click the little “minus” button at the bottom of the list.

Tip 6-5c. macOS Monterey

Apple has built-in protections for many key aspects of your computer—not just important files and folders but also your built-in microphone and camera, location, and other privacy-oriented settings. These security settings are enabled by default, and

you’ve probably already seen pop-up dialogs asking for you to give permission to access this or that. But it’s still good to know where these settings are in case you want to revoke any of these privileges.

1. Open System Preferences and search for “security,” and then open “Security & Privacy” settings.
2. Under the Privacy tab, you’ll find a long list of security and privacy settings. It’s good to periodically review these settings to make sure that you haven’t accidentally granted permission to some application or you want to rescind your permission. But for now we’ll focus on files and folders. The two settings to check here are “Files & Folders” and “Full Disk Access” (Figure 6-51).

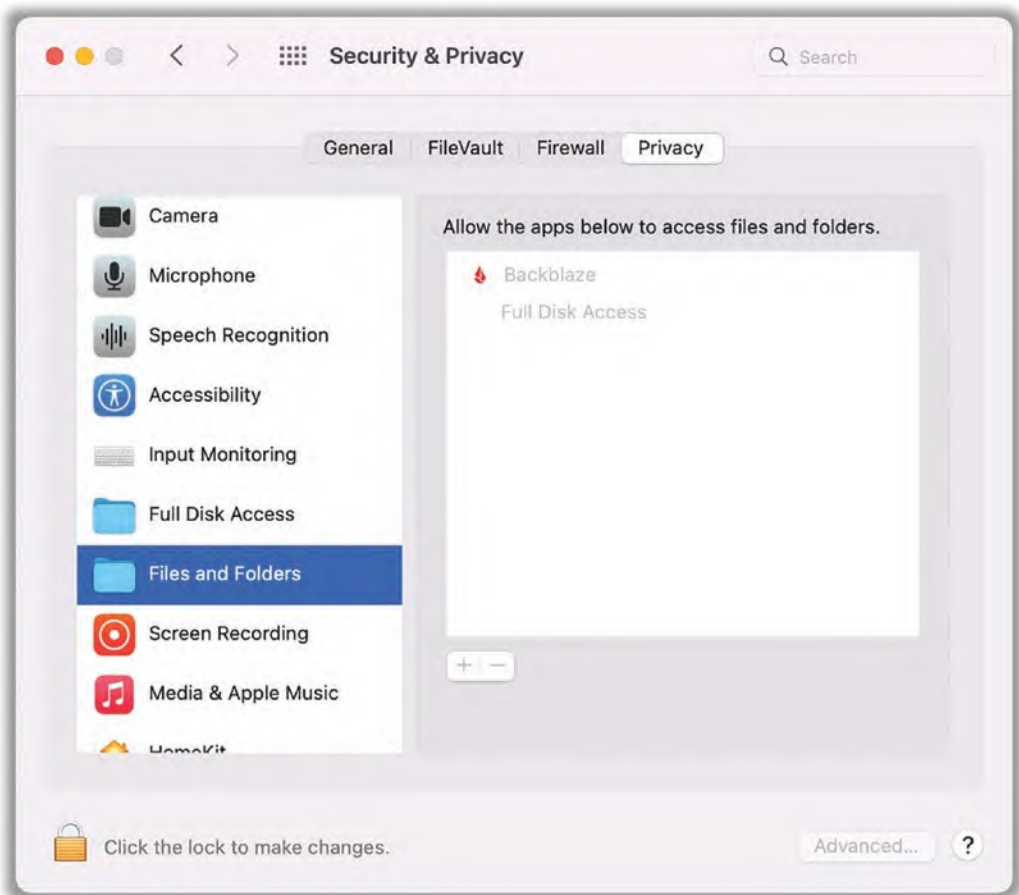


Figure 6-51. macOS Monterey Security and Privacy, Full Disk Access

3. You'll want to look at all the applications in both of these areas to make sure you want to allow those applications to have access. Full Disk Access is pretty much what it sounds like—access to every file and folder. This is necessary for backup apps like Backblaze, but most apps will only need access to specific folders like Documents. To remove an app (i.e., remove their access privileges), select it by clicking it and then click the little “minus” button at the bottom of the list.

Tip 6-6. Disable Unneeded Startup Software

Your operating system will sometimes start up some software applications automatically every time you start your computer. This can be helpful (if there's some app you *always* start every time you log in), but I'll bet there are some apps you don't actually want to start automatically. These apps take up precious resources and can slow down your start up, so it's good to review these items periodically.

Note that there are also system services that are started up every time you log in too. On Windows, several of these services have been shown to be vulnerable to hacking (like the print spooler and Remote Desktop server). The process for dealing with system-level services is rather arcane and can really screw up your computer, if you're not careful. I'll give you links for further information, but I won't cover that in this book.

Tip 6-6a. Windows

Search your Windows settings for “Startup apps” and open the settings window (Figure 6-52). Disable any applications there that you don’t need to start automatically.

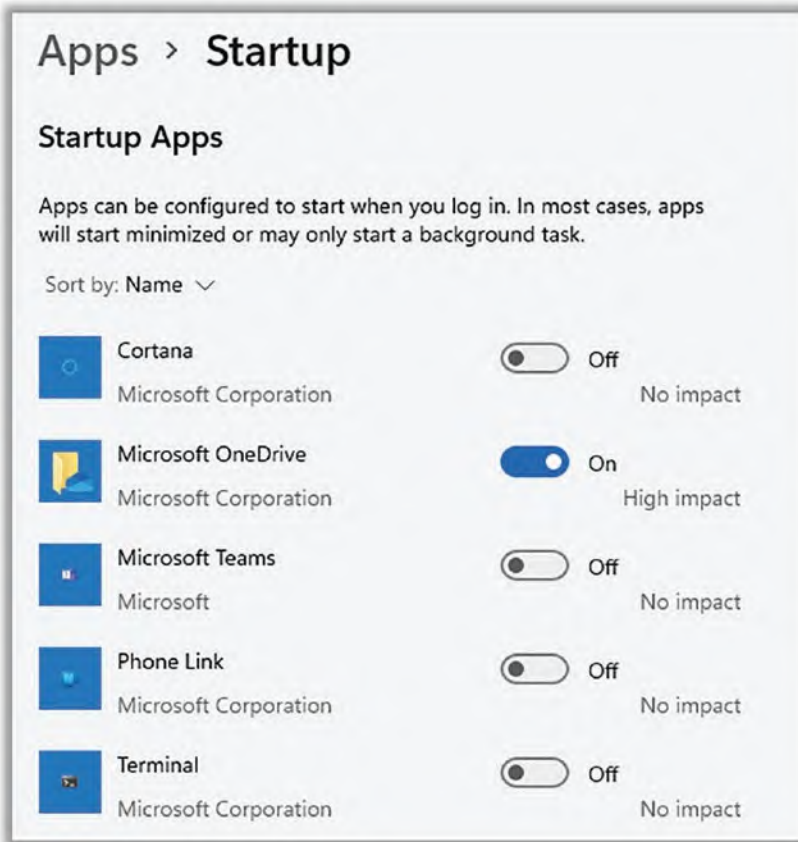


Figure 6-52. Windows Startup Apps

Windows has some particularly nasty services that you might want to consider disabling. Unfortunately, there are weird situations where they are needed. The following article has a good review of the services you might want to consider disabling and will tell you how to do it. However, if you’re the least bit unsure, I would leave this alone.

<https://www.thewindowsclub.com/which-windows-10-services-safe-to-disable>

Tip 6-6b. macOS Ventura

Search System Settings for “login items” and open the settings window (Figure 6-53). Disable any applications there that you don’t need to start automatically.

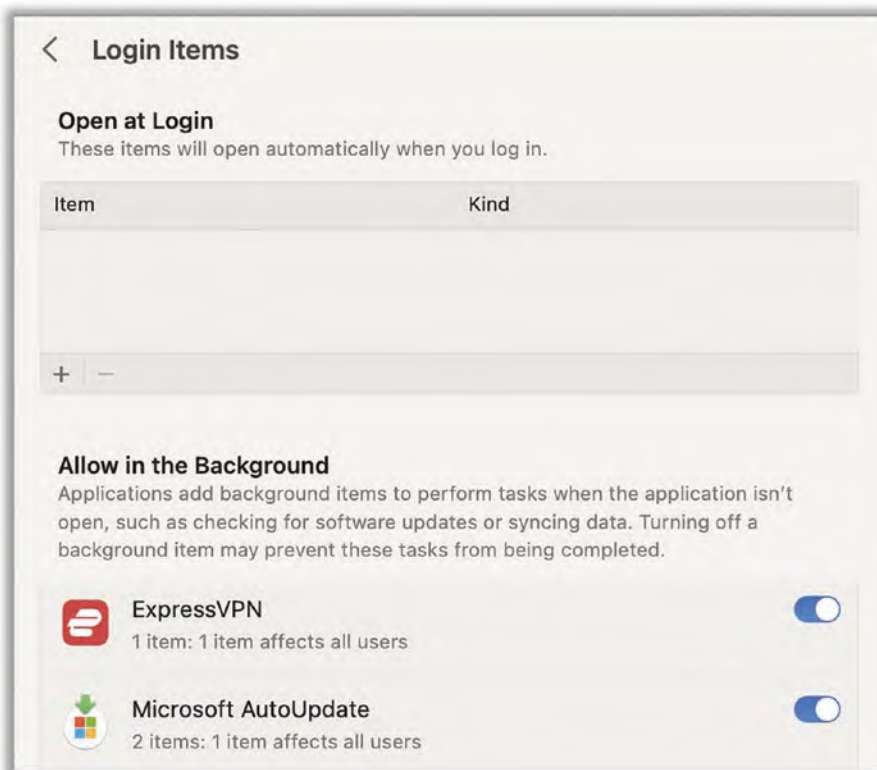


Figure 6-53. macOS Ventura Login items

Tip 6-6c. macOS Monterey

Search System Preferences for “login items” and open the settings window (Figure 6-54). Disable any applications there that you don’t need to start automatically. To do this, select the item by clicking it, and then click the little minus button at the bottom of the list.

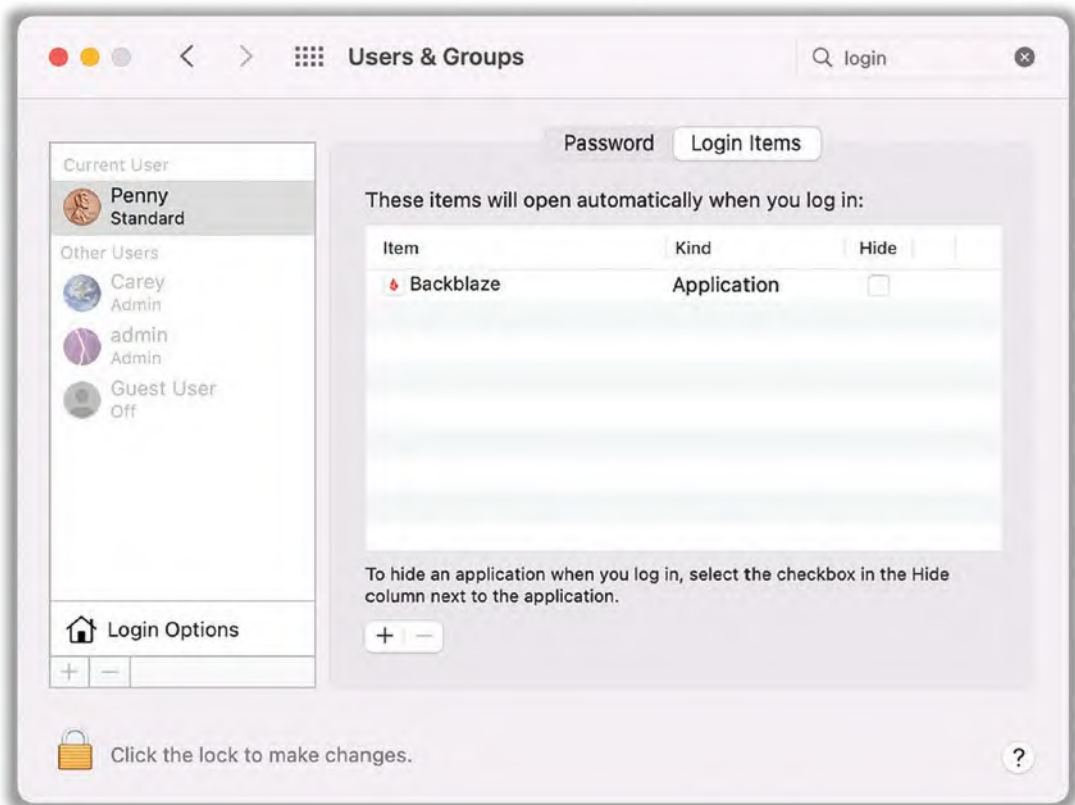


Figure 6-54. macOS Monterey Login items

Tip 6-7. Don't Install Apps That Come with Peripherals

Many computer peripherals (monitors and printers, especially) come with software, usually on a CD or thumb drive that's included in the box. External hard drives, because they're already storage devices, usually come with software on the drive itself—and some installer app may even launch when you first plug it in. In almost all cases, you should *not* install this stuff. Your computer already has drivers built in that will work just fine, or your OS will automatically fetch the drivers from Apple or Microsoft. The software that comes with these peripherals is often “crapware” or “bloatware” that will bug you to start free trials and show you ads for other stuff you don't want. Some of this software will also mine your data. I would just avoid it. (For external drives, I usually reformat the drive to erase all the crap that came with it.)

Tip 6-8. ★ Turn on Disk Encryption

Turning on full-disk encryption is an easy step to protecting your precious data, and you won't even notice it. The process itself can take quite a long time, but you can use your computer while the encryption is going on in the background. There's basically no reason not to do this (if you can). If your computer is ever stolen, the data on the drive will be unreadable unless they can guess your password.

Tip 6-8a. Windows

Windows Pro and Enterprise have a built-in tool called BitLocker that will encrypt your entire hard drive. Unfortunately, BitLocker is not available in Windows Home, which is frankly ridiculous (and will hopefully change some day).

Windows Home edition does come with an option called "Device Encryption," but there are two key drawbacks. First, it's not available for all Windows computers—it requires certain support hardware, which you may or may not have. Second, it requires a Microsoft account, and Microsoft gets to keep the encryption keys—you have no other choice (currently). This is probably billed as a convenience feature for average users who don't want the responsibility of securely storing the encryption key. (Mac OS does this by default, too, but at least gives you the option to control the key yourself.)

In this book, I'll show you how to enable device encryption, if your PC supports it. If you would like more privacy, or if your PC doesn't support device encryption, you should check out VeraCrypt. It's secure, it's free, and it's mostly open source.

<https://www.veracrypt.fr>

Note If you have put your user account home directory on a Windows drive partition other than the standard C: partition (e.g., a new D: partition), *you should not encrypt the partition with the user account*. One reader warned me that doing this prevented him from logging in to that user account and that it was quite difficult to remedy.

To enable device encryption in Windows Home edition, follow these instructions. They are nearly identical for Windows 10 and 11, so I show Windows 11 here.

1. First, we need to see if your computer supports device encryption. Search for “system information” and select it. Then click “Run as administrator” (Figure 6-55). Enter your admin password, if asked.

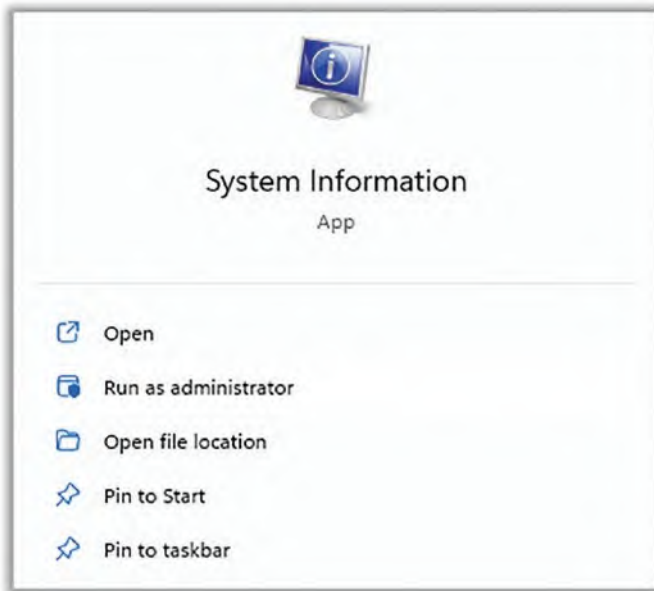


Figure 6-55. Windows 11 System information app

2. This information can be hard to read but look for “Device Encryption Support”—it’s usually toward the bottom of the long list. If you see “Meets prerequisites,” then you can continue; otherwise, your PC doesn’t support it.
3. Go to Settings and search for “Update & Security.”
4. Select “Device Encryption.” If device encryption isn’t turned on, click the “Turn on” button.

Tip 6-8b. macOS Ventura

Note When enabling FileVault on one account, it will automatically encrypt the entire hard drive, which affects all accounts on the Mac.

1. Open System Settings and search for “filevault,” and then open those settings (Figure 6-56).



Figure 6-56. *macOS Ventura FileVault settings*

2. Click the button “Turn On.” It will offer to save the key in iCloud or let you create a recovery key and save it yourself (Figure 6-57). For privacy reasons, I prefer to keep sole control over this key, but it’s more convenient to save it to iCloud. You can make the call.



Figure 6-57. *macOS Monterey Recovery key choice*

3. If you choose to use iCloud, clicking Continue is all you need to do. Otherwise, when you click Continue, you will be shown your recovery key (Figure 6-58). *This step is absolutely crucial!* If you lose this key, you will not be able to recover any of your files if there's some problem with your computer down the road. *Carefully* select the text from the screen, copy it, and then paste it to a secure note in BitWarden (see the previous chapter for instructions). I would label this BitWarden note with “FileVault recovery key” (or at least put this text in the note itself), so you can search for it easily later. You might want to also paste this key into a document, print it off, and then save that printout somewhere very safe (like a safe deposit box). Triple-check it to be certain you copied the entire key faithfully. (After you print the document, delete it.) Then click Continue.

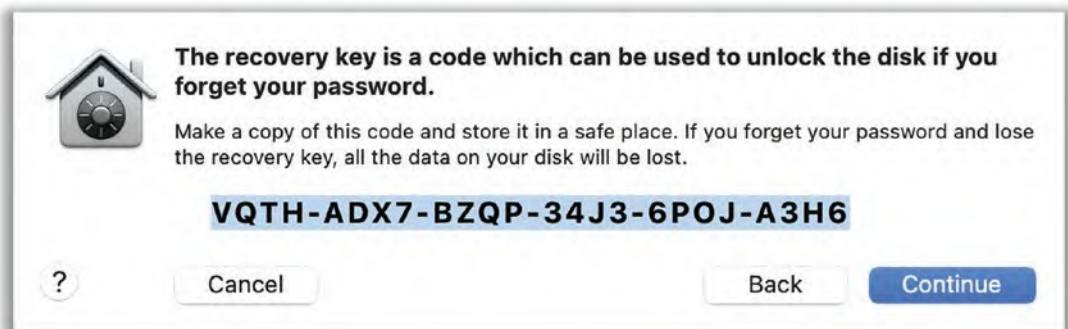


Figure 6-58. macOS Ventura FileVault recovery key—*SAVE THIS!!*

4. FileVault will then start encrypting your drive in the background. You can close the System Preferences window at any time (you don't have to wait for it to complete).

Tip 6-8c. macOS Monterey

Note When enabling FileVault on one account, it will automatically encrypt the entire hard drive, which affects all accounts on the Mac.

1. Open System Preferences and search for “Security & Privacy,” and then open those settings. Click the “FileVault” tab (Figure 6-59).



Figure 6-59. macOS Monterey FileVault settings

2. Click the lock icon at the lower left and enter your administrator account credentials. Click the button “Turn On FileVault.” It will offer to save the key in iCloud or let you create a recovery key and save it yourself (Figure 6-60). For privacy reasons, I prefer to keep sole control over this key, but it’s more convenient to save it to iCloud. You can make the call.



Figure 6-60. macOS Monterey Recovery key choice

3. If you choose to use iCloud, clicking Continue is all you need to do. Otherwise, when you click Continue, you will be shown your recovery key (Figure 6-61). *This step is absolutely crucial!* If you lose this key, you will not be able to recover any of your files if there's some problem with your computer down the road. *Carefully* select the text from the screen, copy it, and then paste it to a secure note in BitWarden (see the previous chapter for instructions). I would label this BitWarden note with “FileVault recovery key” (or at least put this text in the note itself), so you can search for it easily later. You might want to also paste this key into a document, print it off, and then save that printout somewhere very safe (like a safe deposit box). Triple-check it to be certain you copied the entire key faithfully. (After you print the document, delete it.) Then click Continue.



Figure 6-61. macOS Monterey FileVault recovery key—*SAVE THIS!!*

4. FileVault will then start encrypting your drive in the background. You can close the System Preferences window at any time (you don't have to wait for it to complete).

Tip 6-9. Securely Erase Sensitive Files

If you want to throw away a sensitive file, you need to do more than simply put it in the virtual trash or recycle bin and “empty” it. As discussed in this chapter, when the operating system “deletes” a file, it doesn't actually erase the bits and bytes; it just forgets about them. That means that the file's data is technically still there, until it's eventually overwritten by new files. With the right software tools, these files are recoverable. So, if you really want sensitive files to be erased, you have to take some extra precautions.

There's one big gotcha, though: you can't reliably erase a file if you have a solid-state drive (SSD)—and most modern computers come with an SSD drive. Because of the way SSD drives work, the bits that represent your files are moved around constantly to improve performance and balance the usage of the memory sectors. That means there are potentially several places on the drive where copies of your file's bytes may be lying around, waiting to be overwritten—or *recovered* using special software. So, for SSD drives, your best protection is just encrypting your entire drive (the previous tip). Even if there are remnants of the file floating around the disk, they're not readable by someone who's not logged in to the computer.

To put that another way, if you want the files you delete to really be unrecoverable, you should turn on full hard drive encryption. You can do this after the fact.

Neither Windows nor macOS has a way to securely erase a single file (possibly due to the odd nature of SSD file storage). There is another option, though: you can securely erase all the “free” space on your hard drive. This will effectively “shred” all files that have already been deleted. Note that this process can take quite a while, so it's not something you will do often. If you're not worried about someone getting into your account and trying to resurrect deleted files, then you can skip this step. Just make sure your drives are fully encrypted (previous tips).

Tip 6-9a. Windows

To securely erase all the free space on your hard drive, you'll need to use the Microsoft PowerShell utility. Note that this may take a while once you start it. This will only affect already-deleted files and will not touch anything else. Nevertheless, before you do this, *make sure you have all your files backed up*.

1. To get the most out of this procedure, you should quit all other applications. This allows any temporary files created by applications to also be cleaned up.

2. Search for “Powershell” and select “Run as administrator” and enter your admin password when prompted (Figure 6-62).



Figure 6-62. Windows 11 Powershell

3. In the PowerShell window (Figure 6-63), type the following at the prompt and hit Enter. Again, this may take a long time to complete, but when done, all your deleted files will be securely erased from your hard drive.

`cipher /w:C:`

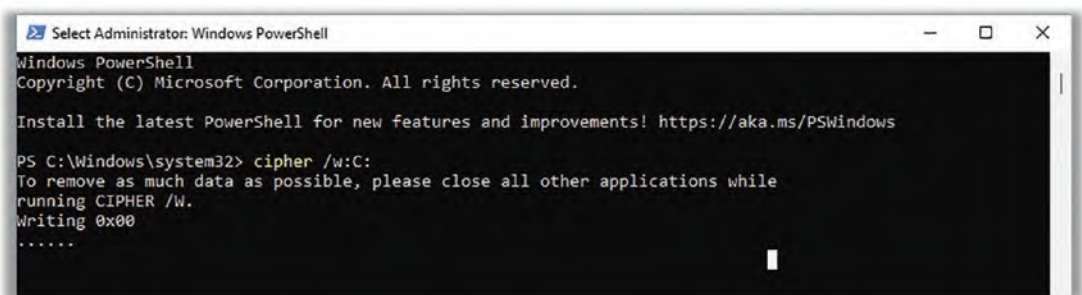


Figure 6-63. Windows 11 Powershell cipher command

Note You can also use a tool from Microsoft SysInternals called SDelete. This free set of Windows tools has a lot of really neat system utilities. You can check it out here:

<https://learn.microsoft.com/en-us/sysinternals/>

Tip 6-9b. macOS

If you have an SSD drive, I don't believe the following is possible. Again, your best security measure is to turn on full-disk encryption. But if you have an older spinning drive (HDD), this may still work.

To securely erase all the free space on your hard drive, you'll need to use the macOS Terminal utility. Note that this may take a while once you start it. This will only affect already-deleted files and will not touch anything else. Nevertheless, before you do this, *make sure you have all your files backed up*.

1. Run the Terminal app. The easiest way to do this is to click the little magnifying glass at the upper-right corner of your screen (Spotlight) and search for “terminal.” When found, click “Terminal” to launch the app (Figure 6-64).

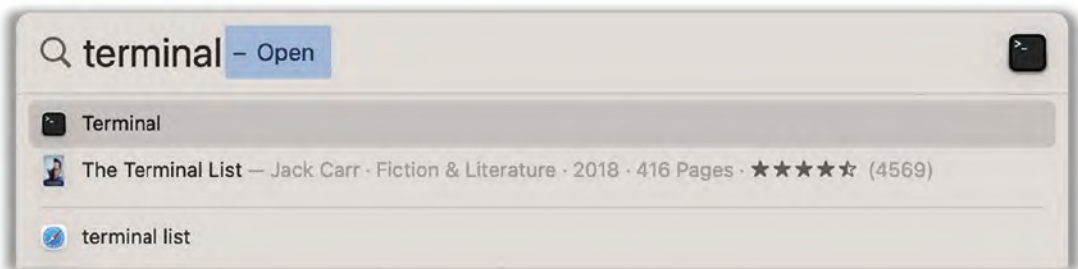


Figure 6-64. macOS Ventura Spotlight search for terminal

2. At the Terminal prompt, type the following. The spaces are important. Be *sure* to include the “freespace” part. Note that this assumes your main drive has the default name “Macintosh HD.” You can try higher levels of security by increasing the 1 to 2 or 3. This will also take a lot more time. When ready, hit Return. See Figure 6-65. If you get an error message, then this command will not work on your Mac.


```
diskutil secureErase freespace 1 /Volumes/Macintosh\ HD
```



Figure 6-65. *macOS Ventura Terminal secureErase freespace command*

Tip 6-10. ★ Prepare a Computer for Sale, Donation, or Recycle

Your computer probably contains a lot of juicy information about you. Before you get rid of it (sell, donate, or even recycle), you should make sure that no one else can get to your data. A recent study⁹ found that most people aren’t taking the time to properly wipe data off their hard drives before they resell them. The researchers bought 200 used hard drives and found that a whopping 59 percent of the drives still had data that was accessible, including “employment and payroll records, family and holiday photos (along with intimate photos and sexualized content), business documents, visa applications, lists of passwords, passport and driver’s license scans, tax documents, bank statements, and lists of students attending senior high schools.” While this study was rather limited, I have no doubt that people are not properly scrubbing data from the devices they trade in, recycle, resell, or throw away.

Now, if you’ve fully encrypted your hard drive like I’ve recommended, then you don’t need to bother trying to erase everything. Your data is completely inaccessible—total gibberish, even to the NSA. All you need to do is delete your accounts. (If you really want to be sure, look at the final chapter of the book for tips on how to securely wipe any hard drive.)

Tip 6-10a. Windows

Here’s how to prepare a Windows computer before you get rid of it. Obviously, before you do this, you’re going to want to back up all your important files first. Once you follow

⁹<https://www.zdnet.com/article/study-shows-that-majority-of-second-hand-hard-drives-contain-previous-owners-data>

these steps, all that data will be *gone*. So, make *sure* you’ve backed everything up before you do this!

Do the following steps from the admin account on your PC:

1. Open Settings and then Update & Security.
2. Click Recovery.
3. Under “Reset this PC,” click “Get started” button.
4. Select “Remove everything.”
5. On the next screen, click “Change settings.”
6. Turn on the “Data erasure” switch. Click “Confirm.” Then click the “Next” button.
7. Finally, click the “Reset” button.

Once this is complete, it will start the process to set up the PC, as if you had just pulled it out of the box. There’s no reason to complete this—you can leave this to whoever buys the computer. Simply shut down the PC.

Tip 6-10b. macOS

Here’s how to prepare an Apple computer before you get rid of it. Obviously, before you do this, you’re going to want a full backup of your computer. If you use the Time Machine method, you can easily use this back up to transfer all your data to your new computer—and I would do this before you erase this computer to make sure everything transfers okay. Once you follow these steps, all the data on the computer will be *gone*. So, make *sure* you’ve backed everything up first!

There are several steps to this process, and it will depend on the type of Mac you have, what iCloud accounts you have, if you’ve backed up to Time Machine, and what OS version you’re running. Apple has excellent help articles that cover all of these angles, and I think it’s safest to point you there:

<https://support.apple.com/en-us/HT201065>

If this link fails, search Apple Support for “What to do before you sell, give away, or trade in your Mac.”

Tip 6-11. Prepare Printers for Sale, Donation, or Recycle

Here's something I'll bet you didn't think about: many modern printers have built-in memory. This allows them to reprint documents you've scanned, for example. This is more common for workplace printers, but it's possible that your home printer has this capability too—especially if it's a fancier, more expensive all-in-one-type printer. That means that whoever has your printer next may be able to recall some of the things you've printed.

Because all printers are different, I recommend checking the manual for your specific make and model. You can usually download a PDF copy of the manual from their website if you didn't happen to save the one that likely came in the original box with the printer.

If your printer has a screen on it, you can try poking around in the settings and look for the option to do a “hard reset” or “factory reset” to wipe all the internal data.

Tip 6-12. Enable Laptop Location Tracking

This is a very nice feature for laptops, which are portable and can be lost or stolen. When this feature is enabled, you will be able to track your computer, send messages to the screen, and even remotely lock or erase it, if you believe it was stolen. You will need to sign up for a free iCloud or Microsoft account, if you haven't already. Note that I'll talk more about iCloud and Microsoft accounts in Chapter 10. If you haven't created an iCloud or Microsoft account yet, you might want to wait till we cover that topic and then return here.

Tip 6-12a. Windows

There's one major gotcha to setting this up on Windows—it requires a Microsoft account for the administrator, which we avoided. If you want to enable this feature, you'll need to set up your Microsoft account. You should be able to reuse your regular Microsoft account (i.e., you can use one Microsoft account for both your admin login and regular login).

1. To make these changes, you'll need to log in to your PC using an admin account. For some reason, there doesn't seem to be a way to right-click the Settings app and “run as administrator,” so you'll

- need to actually log in to your computer using the administrator account.
2. Once running as admin, search settings for “Find My Device.” If necessary, enable location services (there will be a warning there if you need to do this and a button to do it).
 3. Turn on “Find My” (see Figure 6-66).



Figure 6-66. Windows 11 Find My Device

4. You can now monitor the location of your laptop (and any other Microsoft devices that you’ve registered for Find My) by going to the following Microsoft website. You can also lock this device remotely, if it’s lost or stolen.

<https://account.microsoft.com/devices>

Tip 6-12b. macOS Ventura

There’s one gotcha to setting this up on macOS—it requires an iCloud account. You don’t have to be the administrator, however, so you probably already have an iCloud account set up for your main account.

1. Search System Settings for “iCloud account,” and select it. You should see “Find My Mac” listed in the top section (Figure 6-67).



Figure 6-67. *macOS Ventura iCloud account settings*

2. Click “Find My Mac” (Figure 6-68). Click the “Turn On” button.



Figure 6-68. *macOS Ventura Find My Mac dialog*

3. You'll be asked to allow the Find My Mac feature to access your location. Click "Allow" (Figure 6-69).



Figure 6-69. macOS Ventura Find My Mac location allow

4. When done, you should see the following (Figure 6-70).



Figure 6-70. macOS Ventura Find My confirmation

5. You can now monitor the location of your laptop (and any other Apple devices that you've registered for Find My) by going to the following iCloud website. You can also lock this device remotely, if it's lost or stolen.

<https://www.icloud.com/find>

Tip 6-12c. macOS Monterey

There's one gotcha to setting this up on macOS—it requires an iCloud account. You don't have to be the administrator, however, so you probably already have an iCloud account set up for your main account.

1. Search System Preferences for “iCloud account,” and select it. You should see “Find My Mac” listed in the right section (Figure 6-71).

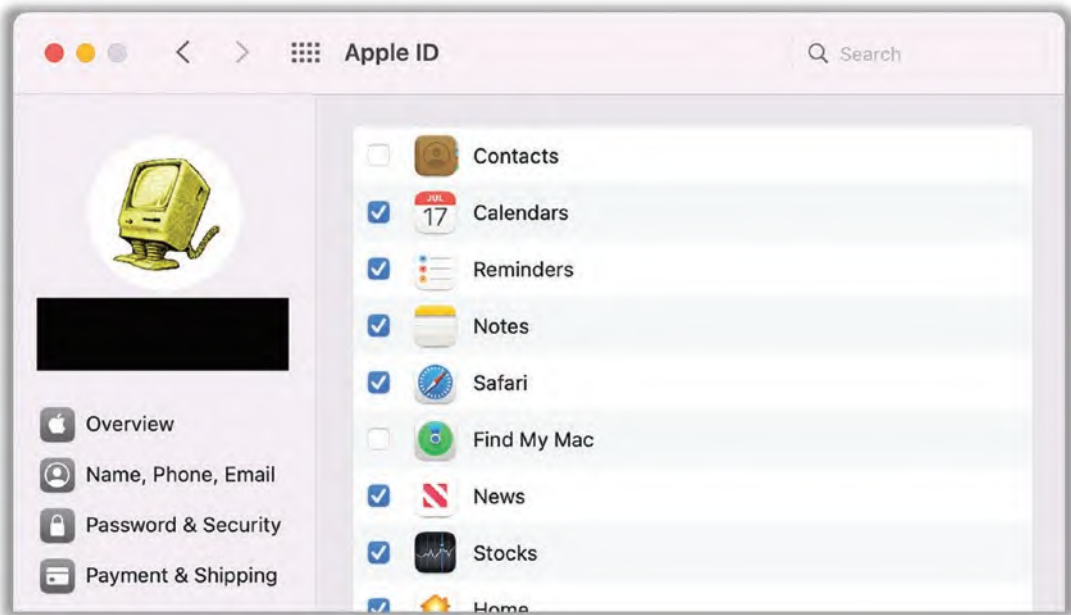


Figure 6-71. macOS Monterey iCloud account settings

2. Check the box next to “Find My Mac”—you should get a pop-up like in Figure 6-72. Click the “Allow” button.



Figure 6-72. *macOS Monterey Find My Mac location allow*

3. When done, if you see an error message right under “Find My” that says you need to enable location services with a button, click that to go to the Privacy settings for Location. You’ll want to enable location services and specifically enable it for Find My. (You’ll need to unlock this setting first.) When do, it should look like Figure 6-73.

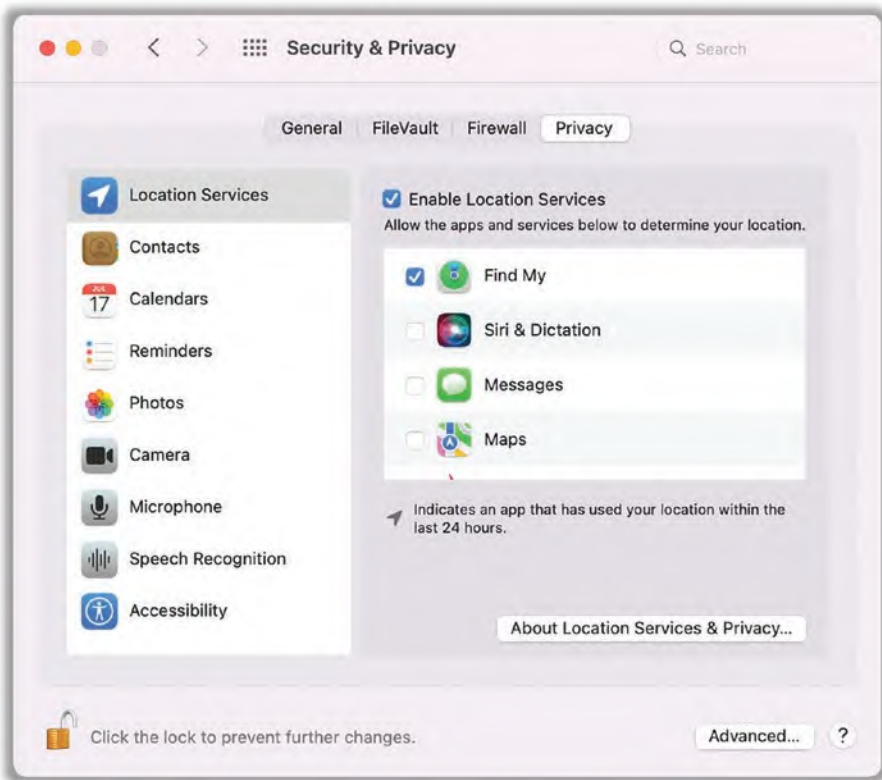


Figure 6-73. *macOS Monterey Privacy Location Services*

4. You can now monitor the location of your laptop (and any other Apple devices that you’ve registered for Find My) by going to the following iCloud website. You can also lock this device remotely, if it’s lost or stolen.

<https://www.icloud.com/find>

Tip 6-13. Use Lockdown Mode (macOS Only)

With macOS Ventura, Apple introduced a special security feature called Lockdown Mode. It’s specifically designed for high-profile spying targets like dissidents, activists, journalists, politicians and so on to prevent malware and spyware infections. In this mode, Apple disables a lot of fancier convenience features that have been exploited by top-tier hacking tools often used by nation state intelligence agencies and the like.

However, I personally think this might be useful for “normal people” in some situations, too – like maybe when traveling abroad, attending a political protest, or in any situation where you might be arrested.

In this mode, your Messages app won’t show you web link previews and most attachment types will be blocked. Some website technologies will be blocked, which may cause some sites to load slowly or even break completely. Incoming FaceTime calls will be blocked unless you have previously called them. There are several other changes, but in my mind they’re not that severe. You can read more here:

<https://support.apple.com/en-us/HT212650>

To enable this mode:

1. Open System Settings, tap Privacy & Security.
2. Under Security, turn on Lockdown Mode.
3. This will require a phone restart.

You can disable Lockdown by reversing the above process.

Tip 6-14. Don’t Trust Other Computers

Whenever you’re using a computer that is not your own, you need to be very careful what you do—particularly public computers at hotel business centers, cybercafes, libraries, and so on. Sometimes bad guys will install software on public computers that can record every single keystroke from the keyboard—these are called *key loggers*. Some malware can also take snapshots of everything shown on the screen. If you’re just doing some web searches and accessing websites that don’t require you to log in, then you don’t need to really worry because you’re not typing in or viewing anything that’s secret. However, you should never enter sensitive data like passwords, social security numbers, and credit card numbers on any computer you don’t own. It doesn’t matter if the website is secure; the information is being captured before it even gets to the form on the web page.

Tip 6-15. Avoid Strange USB Devices and Ports

We don't think much about all the USB peripherals we attach to our computers—mice, keyboards, printers, webcams, thumb drives, and so on. These devices seem simple enough, but *every* USB device can contain software—and often, our computers will automatically read and run that software when the device is first plugged in. The point of this is for these devices to have built-in driver software, allowing most devices to “just work” when we plug them in.

To save money, many manufacturers will make this software updatable after manufacture. That is, instead of making this software read-only, they give themselves the option to retroactively change the software—so that if there's a problem with it, they can simply change the software without having to throw away the hardware and start over.

The bottom line is that it's possible to install malware on a USB device. Therefore, you treat any foreign USB device as suspect.

While spreading malware via infected USB devices is not that common, you should still be aware that it's possible. If you want to be 100 percent safe, here are some things you can do to avoid catching a virus from a bad USB device or plug.

1. Never pick up a USB flash drive that you find lying around and plug it into your computer.
2. Get your USB devices from a reputable retailer. Make sure they're new and unopened.
3. Avoid buying or borrowing USB devices from people you don't know.
4. Set your computer screen to lock right away and require a password to unlock. Don't leave it alone with others present while it's unlocked. It's already been shown that bad guys can completely hack your computer in less than a minute by plugging in a specially configured USB device. You'll never even know they were there.

Note that this also applies to charging your smart device on a public USB port (charging stations, airplane USB ports, charging ports in taxis, etc.). See Chapter 12 for how to protect yourself when charging.

Tip 6-16. Restart Your Computer Periodically

There's honestly no real need to turn off your computer these days. The most common thought is that it will save energy, which it will. But most modern computers will automatically go into a deep sleep mode when not in use and draw very little power. Also, the automatic software update features tend to do their thing in the middle of the night when their masters are sleeping. For these reasons, I would leave your computer running most of the time.

However, your computer can build up some cruft over time—applications that don't quit cleanly, data that isn't flushed properly from RAM, services that get hung in the background, and so on. It's therefore a good idea to restart your computer periodically. How often? I probably do it once or twice a month, or whenever my computer seems to be sluggish or acting funny.

Tip 6-17. Don't Use Adobe Reader to Read PDF Files

The popular PDF¹⁰ viewing app called Adobe Reader is known for its share of security bugs. This isn't an issue with macOS since Apple provides an excellent PDF viewer called Preview (though some Adobe products will still install Reader, which will automatically supplant Preview for opening PDF files). On Windows, however, you should consider downloading and installing a new PDF reader app.

Most web browsers can open PDF files now. You can drag and drop the PDF file onto your web browser or right click the PDF file and select your browser to open the file.

If you just want a simple, quick application for reading PDF files, try Sumatra PDF reader:

<https://www.sumatrapdfreader.org>

If you would like a full-featured PDF reader that will also let you create PDFs, try Nitro PDF reader. You'll get a free trial of Nitro Pro, and then it will revert to the (perfectly useful) free version:

<https://www.gonitro.com/free-pdf-software>

¹⁰ Portable Document Format (PDF) is a popular format for creating documents that can be read on a variety of devices and operating systems.

Tip 6-18. Unplug or Cover Webcams When Not in Use

This is going to sound paranoid, but it's for real. It's actually possible to remotely enable some webcams and watch what people are doing, in some cases even without turning on the little light that indicates that the webcam is active. This would usually require that your computer has already been compromised with malware—which is to say that if you have this problem, you probably have others too. Nonetheless, I would unplug webcams if you're not using them or put a sticky note over the lens if the webcam is built-in. (Mark Zuckerberg, CEO of Facebook, was famously seen doing this.)

Tip 6-19. Beware Cold Calls for Computer Support

If someone calls you out of the blue and tells you that your computer is having problems and offers to remotely debug your computer for you, just hang up. Real computer support companies will never do this. While this company may actually offer computer support services (at a low, low subscription cost of \$199/year), you probably don't need them.

Likewise, if you're getting a weird pop-up on your computer warning you that you're infected (from something other than the antivirus program you've already installed) or your computer's performance could be optimized or even that some scanner has detected illegal materials on your hard drive, just close the window without doing anything. This is almost surely a scam.

If the pop-up messages continue or you're just worried that something really is wrong, contact a tech-savvy friend or relative and get their advice. If that's not an option, call a reputable computer store or call your computer's support line (even if you're out of warranty).

CHAPTER 7

Guard the Castle Gate

In this chapter, we're going to discuss your home network—the main gate for your digital castle. Everything that comes in or goes out of your home network goes through your modem and router. We'll also discuss some common devices on your network, VPNs, and more.

Even if you have only one computer connected to the Internet, you still technically have a network. A network is something that allows two or more devices to communicate and share resources. The Internet is the most famous network; it's the network that connects us to computers and services all over the globe. But most of us also have an *intranet* within our homes, and how we allow our personal network to communicate with the public network is crucial to our security and privacy.

Network Overview

Let's start by identifying the parts of your home network—called a *local area network* (LAN). For your computer to connect to the Internet (referred to as a *wide area network*, or WAN), you first need to have Internet service—often called *broadband* or *high-speed Internet* service. For most people, this is provided by their cable or phone company.¹ In rural areas, you might get your Internet service from a satellite company. In many metropolitan areas, you can get Internet service over fiber-optic cable or via cellular data. But regardless of the specific way in which you connect to the Internet, the company that provides you with this service is called your *Internet service provider* (ISP). Somewhere in your house (or condo or apartment), you will have a box that this

¹Service from your cable company uses technology called Data over Cable Service Interface Specification (DOCSIS); service from the phone company usually uses technology called Digital Subscriber Line (DSL) or Asymmetric DSL (ADSL).

company provided to which you connect your computer. This box is usually called a *modem* (which is short for “modulator-demodulator”). A typical modem looks something like Figure 7-1.



Figure 7-1. *Cable modem*

The modem converts the common Internet Protocol (that your computer understands) to some sort of special protocol that allows the communication to flow over the phone lines, cable line, fiber-optic cable, or satellite link. This device is assigned an Internet Protocol (IP) address, and like the address on your house, it’s associated specifically with you (or your account). When your computer talks to the Internet, the return address on all its packets is your IP address.

In the simplest case, you just connect your computer directly to this modem and you’re done. That’s your entire network. But most of us today have more than one device in our homes that wants to access the Internet, and in that case, you need another piece of equipment called a *router*. Your ISP gives you only one IP address. If you have multiple devices, then you need some way to give those devices their own addresses—at least within your home—so that each one of those devices can carry on their own conversations with other things on the Internet. (We discussed how this works in Chapter 3.)

It’s important to note that if you have multiple devices on your home network, they often talk to each other, as well. That is, they send information between themselves that’s not meant to leave your house. Maybe you’re streaming some music from your computer to your home theater system or printing a document from your laptop to a printer. In this case, all the data travels completely within your network. It’s like someone in marketing sending a package to the sales department via internal company mail. The US Postal Service never sees or knows about this; it’s completely internal and private. We’ll see why this is important in the next section.

Most routers today are wireless routers. This is a little box that often has one or more antennas on it and is directly connected to your modem via a cable called an *Ethernet cable*. It will look something like Figure 7-2.



Figure 7-2. *Wi-Fi router*

Ethernet cables are like phone cables—they usually have little clippy things on the end that snap into place. Ethernet cables are the most common cords that are used to connect things to a network directly. The router box is then connected to all the other devices in your house that need to access the Internet—either hardwired with an Ethernet cable or connected virtually over the air, wirelessly. The wireless connection is called *Wi-Fi* or sometimes by its technical spec name, 802.11. Networks created by Wi-Fi routers are commonly referred to as *wireless LANs* (WLANs). (I know...couldn't they come up with something a little less confusing? LAN, WAN, WLAN—really? Don't shoot the messenger, folks.) There are many versions of Wi-Fi. Over the years they improved things and gave the spec different names like 802.11n and 802.11ac. Realizing that this naming is rather cumbersome, the Wi-Fi Alliance has moved to a simpler naming scheme: “Wi-Fi” followed by a number. The latest version is Wi-Fi 6 (which would have been called 802.11ax in the old naming scheme). But all you really need to know is that the router acts like an internal, private mail room—the router allows all the devices in your house to have private addresses inside your home to talk with each other and to share a single public Internet address for communications with the outside world. Many hotels, cafes, restaurants, airports, and libraries provide free Wi-Fi Internet access for customers. These locations are referred to as *Wi-Fi hotspots*.

That's pretty much your home network in a nutshell. You have a modem, a router, and a bunch of devices that are connected to that router (either wired or wirelessly). Those devices include desktop computers, laptops, smartphones, printers, and tablets. With

the explosion of “smart” devices (the so-called Internet of Things), we also have several other devices wanting to connect to the Internet, including TVs, streaming boxes (like Apple TV, Fire TV, or Roku), video doorbells, home appliances, thermostats, and even light bulbs.

Now that we know the pieces to the home network puzzle, let’s take a look at the security and privacy issues associated with your home network and how to deal with them.

Modem

The modem provided to you by your Internet service provider is generally something you cannot control, and that makes a security- and privacy-conscious person nervous. Many ISPs are now providing a combo product: a modem and Wi-Fi router all in one—how convenient! That’s even worse. Why? Because what’s best for your ISP is not the same as what’s best for you.² Your network router is doing two crucial things: it’s a wall between your network and the rest of the wild, woolly Internet, and it’s the hub for all the data traffic within your home network. There’s just no reason to trust your ISP to perform those critical functions. While ISPs will usually try to protect your home network from bad actors on the Internet, they have no reason whatsoever to protect your privacy or to insulate you from their own meddling. Furthermore, you want to have full control over the configuration of your Wi-Fi router, and your ISP may not give you that access. For these reasons alone, I strongly suggest you always insert your own router between your computer and your ISP’s modem. Basic models are pretty cheap, and this book can help you get it set up.

Here’s an interesting story that will help to illustrate my point. A few years ago, Comcast (one of the largest ISPs in the United States) began rolling out a service for its customers called Xfinity Wi-Fi. This service allows Comcast customers to use “millions” of free Wi-Fi hotspots around the world. Sounds great, right? What’s not to like? Well, the company accomplished this by turning people’s private cable boxes into public hotspots—that is, Comcast enabled this feature on your home combo modem/Wi-Fi box so that its customers near (or in) your home could connect to the Internet using your equipment. While I’m sure Comcast customers somehow implicitly gave Comcast permission to do this somewhere in their licensing agreement, I’m willing to bet most people had no

² According to the 2017 American Customer Satisfaction Index (ACSI) survey, cable companies and Internet service providers are tied for last place in the United States, well below even health insurance companies and airlines.

idea they were doing this. Your modem is, after all, Comcast's equipment—not yours. It provides you with a service, and that contract surely allows Comcast to offer other services using its equipment.

When this became widely understood, people rightly had serious questions about this service. Won't this slow down my Internet connection (having to share it with others)? Will this give strangers access to my home network? What if someone uses my Internet connection to do illegal things using my network—won't that appear as if I did those things? Comcast has some partial answers for these concerns, and there does exist a way to opt out of this program by changing your account preferences online. But the real question is: do you trust your ISP to do what's best for you (as opposed to what's best for them)? If Comcast changes its strategy or decides to offer another feature like this in the future, how likely are you to be properly informed of this? And will you be given the choice to opt out? (Two customers in San Francisco filed a class action lawsuit against Comcast over this, but it was thrown out because all Comcast customers agreed to settle disputes via arbitration in their terms of service.)

The simplest solution to this is to just use your own router. If your ISP provided you with a combo modem and Wi-Fi router, I would call them up and ask them to disable the Wi-Fi service entirely. If you're a Comcast customer, I would also opt out of the Xfinity public/shared Wi-Fi program, if possible.

Since your modem is usually provided to you by your ISP, there's usually not much else you can do here. However, you can buy your own modem—see the tips at the end of this chapter.

Wi-Fi Router

Your Wi-Fi router is arguably the most important part of your network in terms of your overall Internet security. It's also probably the most complicated one because it performs several important functions. Understanding how to properly configure a Wi-Fi router is not easy, but that's why you bought this book! I'll walk you through the primary settings you need to worry about and show you how to configure them properly. Before we get to the specifics, let's discuss the key functions of your Wi-Fi router.

As I mentioned in earlier sections, your router acts as a barrier between your private, home network and the wider, public Internet. Most networked devices today still use the old but venerable Internet Protocol version 4 (IPv4) standard. As we discussed earlier,

there are about four billion possible IPv4 addresses—and the world now has way, way more than four billion networked devices. However, there are subsets of those addresses which are reserved for “internal use only.” These ranges of IP addresses can be reused over and over in people’s home networks, as long as they’re only used once within a given home network. Regardless of how many devices you have inside your house, the external world sees all your packets as coming from a single address—your public IP address, the one assigned to you by your ISP. Your router takes care of delivering all inbound traffic to the proper device inside your home.

Your router is in charge of assigning local, internal IP addresses for all the devices in your home network. It does this using *Dynamic Host Configuration Protocol* (DHCP). When you plug a device into the network or allow a new device to connect wirelessly, that device needs to have a unique IP address to communicate with anything else on the network. The device finds your router and asks it for an IP address that it can use. The router chooses a unique IP address from the range of reusable IPv4 addresses (usually something in the 192.168.x.x range) and keeps track of which address is assigned to which device³.

Network Address Translation (NAT)

This brings us to a very important function of home routers: *Network Address Translation* (NAT). As we discussed earlier in the book, communication with the Internet is like mailing letters: the information you send is chopped up into a letter-sized payload, stuffed in an envelope called a packet, and shipped out with a destination and return address written on it. But to the outside world, every smart device on your home Wi-Fi network looks the same—that is, all the communications appear to come from the same address. This is because your router acts as a sort of local mail delivery system. Think of a large company. When you send a package to someone in that company, you probably just address it to the person at the general company address. You don’t know the specific building and/or mail slot within the company; you just trust the company’s internal delivery service to find them. So, your home router maintains a mapping for all the

³If you’re interested, networked devices have fixed, preassigned hardware addresses called a media access control address, or MAC address. The initial setup works with these addresses, and then once DHCP happens, the device uses the IP address that the router assigned to it.

current open connections, making sure that the right incoming packets get routed to the proper internal device. Since there's only a single IP address that's given to the external world, we need a second piece of information: a port number.

It's not crucial that you understand this, but let me explain this with an example. (If you're really not curious, skip this paragraph.) Let's say your public IP address is 11.22.33.44. The internal IP addresses which your router can give out range from 192.168.0.1 up to 192.168.0.255. Your router usually gets the first one, so in this case 192.168.0.1. Your router actually has two addresses: the internal one that it uses to talk to your other home devices (192.168.0.1) and the external one assigned to it by your ISP (11.22.33.44). So, your laptop connects to the router and asks for an IP address—your router says “here, you use 192.168.0.2.” Now on your laptop, you point your web browser at amazon.com, which has an IP address of 54.239.28.85 (that's real, I looked it up). Your laptop picks a local port number, say 1000. An HTTPS request is sent from your laptop whose IP address is 192.168.0.2 using port 1000. The shorthand for this is 192.168.0.2:1000. It sends that request to 54.239.28.85:443—port 443 is the standard port for HTTPS connections. This goes through your router, which swaps out your internal return address on this outgoing request with a public address and port: let's say 11.22.33.44:2000. When Amazon responds, it sends the response to 11.22.33.44:2000, and your router (remembering the mapping) forwards the response internally to your laptop at 192.168.0.2:1000. Amazon never sees the internal IP address or port number. It talks to 11.22.33.44 on port 2000, and your router sends it to your laptop at 192.168.0.2:1000. That's how Network Address Translation works (at a very high level).

The result of this mapping—the NAT function—is that computers outside your home network have no direct way to contact an individual entity (computer, smartphone, or other Internet-connected device) within your home. The internal addresses aren't known. That's a very good thing. This is one form of security through obscurity that actually benefits you. (And we'll see later in this chapter how this handy hiding can be bypassed.)

Firewall

But there's one more very important router function that protects you from the bad guys on the Internet: a *firewall*. A firewall in a car separates the passengers from the engine compartment (and the heat it produces). In buildings, a firewall is used to prevent the spread of fire. In a router, a firewall keeps unsolicited web traffic from entering your

network⁴. It's sort of like a one-way data valve: requests from inside the home network can go out to the Internet, but requests from the Internet can't come in—at least without being “invited” (I'll come back to that in a second). Note that requests imply responses, which we discussed just a second ago. Your web browser (a client) sends a request out to somewhere on the Internet, like to amazon.com (a server), and then expects a response (like the contents of a web page). The firewall allows the request to go out and any responses to that request (there may be more than one) to come back in. As long as the initial connection originated within your home network, all subsequent traffic for that connection is allowed to flow back and forth freely.

You can configure your router to explicitly allow incoming connections. This is called “poking holes in your firewall,” which I do not recommend. You'll probably never do this yourself, but the *Universal Plug and Play* (UPnP) feature on home routers allows devices on your network—like a game console—to automatically open ports in your firewall for things like multiparty gaming. You should disable UPnP on your router, and we'll cover that in the checklist⁵.

Wireless Connections and Quality of Service

Wi-Fi routers allow you to connect to your home network wirelessly—as in, without wires or cables. This feature, while extremely handy, brings with it a lot of security issues. Instead of having to physically plug an Ethernet cable into your router to get onto your network, you can now connect your laptop or other smart device through the ether simply by changing a setting. Instead of having to be physically inside your house, with Wi-Fi you only have to be *near* your house—like next door or parked outside on the street. To protect your network, Wi-Fi has some security options that will restrict access to your network. These include adding encryption, authentication, and even some good ol' security by obscurity. However, there are also a lot of add-on features for convenience

⁴So, the title of this book intentionally plays fast and loose with the meaning of “firewall.” Dragons breath fire, right? But the real point of the title is that if a dragon-level attacker (think CIA, GCHQ, Russia, China) really wants to get into your home network, then common tools like the firewall in your router will not be sufficient defense.

⁵There is actually a public, free search engine for exposed Internet devices—it's called Shodan. With this tool, you can search for webcams, baby monitors, video doorbells, and other smart devices that have exposed themselves directly to the Internet, usually through holes poked in a firewall.

that have exposed some weaknesses. All of these will be discussed at length in the checklist at the end of this chapter.

Routers have one more interesting feature that is worth mentioning. Routers act as a sort of traffic cop, directing traffic in the network. The router can allow some traffic to have a higher priority than others—for example, allowing live video streams to flow freely while sending Google queries to the back of the line. Packets of audio and video information are very time-sensitive—if those packets are delayed or lost, you will have glitches in your music or your streaming movies. However, things like querying Google for local restaurants or checking your email can wait a bit, if necessary (and by “wait a bit” I’m talking fractions of a second). This is referred to as *quality of service* (QoS); some network packets are more “important” than others. Some routers will automatically detect important traffic and prioritize it, while others need to be configured for this feature. The quality of service flag on these packets is not required to be honored; it’s more of a suggestion. But it’s a mechanism that can be used to improve the performance of time-sensitive network traffic.

Keep Your Gatekeeper on Your Payroll

In most cases, your router is the only thing standing between your devices (certainly your IoT devices) and the open Internet. It’s also privy to all the networking traffic between your home devices. This makes it the ideal place to implement security and privacy functions—and the ideal place to subvert them. For this reason, you should own your router whenever possible, and you should buy a high-quality router from a reputable manufacturer.

If we go back to our castle analogy, this would be like hiring your own guards to watch the front gate and patrol the castle grounds—as opposed to allowing this job to be farmed out to a third-party security service guild...or whatever a medieval contracting company analogy would be. You shouldn’t be shopping security services around to the lowest bidder, no matter how convenient that might be.

The Internet of Things

The *Internet of Things* (IoT) refers to the popular tech trend of making all of our dumb devices smart—that is, connecting them to the Internet (which I’m not sure necessarily makes anything or anyone “smart”). What good is your refrigerator if you can’t query its

contents from the office before you come home? Who wants a dumb thermostat that you can't change from halfway around the globe? Who needs a Bluetooth speaker that won't respond when you ask it for today's weather? We're already spoiled by our smart devices, and we've frankly only scratched the surface of what's possible. Connecting things to the Internet has been a massive boon to makers of products—adding Wi-Fi to something means cool new features and ways to collect and monetize your data.

The problem with adding smarts to cheap devices like light bulbs, baby monitors, thermostats, and appliances is that it adds cost—in some cases, significant cost (compared to the equivalent “dumb” version). People pay for features they can see and experience—and they tend not to pay for other stuff, like security. Security in particular can cost a lot of time and money to develop and build into your products, especially if you're going to do it right. And many companies don't do it right or at all. We like to say that the S in IoT is for security... meaning there is none. That's not strictly true, but it's sadly not far from it. So, as we're bringing all these wonderful, connected devices into our homes, we also need to be very cognizant of the risks involved.

Let's look at both the security and privacy threats as they relate to the Internet of Things devices.

IoT Security (or Lack Thereof)

Internet-connected appliances tend to have horrible security (though things are starting to improve, mostly due to legislation), and the bad guys know it. There are two primary reasons that attackers might want to target your weak IoT devices: to establish a beachhead inside your LAN to get at other devices or to conscript your devices to serve in a zombie computer army (I'm not kidding). Let's take these one at a time.

If a hacker wanted to try to spy on you or score some personal data, they need to get onto your home network, meaning they need to get past your router's firewall. The best way to do that is to have a mole on the inside, and usually the easiest target is a vulnerable IoT device. Each of these devices contains a tiny computer. All computers run software and all software has bugs. If the hacker can take over that computer with malware by exploiting the weak security, they can now remotely poke around your home network at will. Maybe they'll try to infect other devices, including your computers. They could turn on microphones or cameras to spy on you or root around your files for sensitive information. While you might wonder why anyone would target you for this, you have to realize that many of these hacking programs are automated. It's like robotic burglars

roaming around neighborhoods looking for unlocked doors and windows and taking stuff that looks valuable.

But once they've compromised your devices, cybercriminals love to use these devices to do nefarious things. We call these groups of hacked computers and devices a *botnet* ("bot" being short for "robot," "net" being short for "network"—a network of robots). These compromised IoT devices are programmed to listen for instructions from remote command-and-control computers. The directive may be to attack other, higher-value computers or simply mining Bitcoin to make their masters some money. But once conscripted into this zombie army, they can be called upon to do anything at any time.

This might sound silly, but it's a serious problem. Remember the Target credit card breach in 2014? Hackers got into Target's payment system by first hacking the heating and air conditioning system. The system was on the same network as the credit card database. In another story, the CEO of cybersecurity company Darktrace revealed that a casino's high-roller data was exfiltrated by first compromising a smart aquarium thermostat in the casino's lobby.

Botnets are even more serious. When done well, a thousand compromised devices can bring down an entire website. The Mirai botnet was responsible for crippling Internet service of much of the United States and parts of Europe in 2016 by taking down the DynDNS service.

To make matters worse, IoT devices are often controlled via the Internet instead of just through your home network⁶. This allows them to be easily monitored and configured from anywhere on the planet. Of course, it also means that the bad guys can try to hack these cloud services and gain access to your data and maybe even to your devices. But you don't really have control over that, unfortunately.

IoT Privacy (or Lack Thereof)

Internet-connected devices can easily be spied in our midst. Some devices just have crappy security (as we just discussed) allowing bad guys to take them over remotely. But many of these devices are actually programmed explicitly to mine your data, so it can be in some way sold to others. Let me give you a creepy and nearly ubiquitous example.

⁶There are plans afoot to address this problem—basically, by creating a smart "hub" at home, which can centralize and standardize control of your IoT devices, with more security and privacy. See this article: <https://www.eff.org/deeplinks/2022/06/keeping-your-smart-home-secure-private>

We talked about a smart TV in Chapter 2 whose terms of service explicitly call out the use of built-in microphones to send recorded audio snippets out to the Internet somewhere. But there's another feature of modern smart TVs that will blow your mind. If you're properly paranoid, you probably assume that the built-in smart TV apps like Netflix, Hulu, Amazon Prime Video, and others are keeping track of everything you watch. But what you may not know is that the TV itself is also watching what you're watching and reporting it to the TV's manufacturer. It's called *Automatic Content Recognition* (ACR), though different TV makers have different proprietary names for this feature. If you're familiar with the Shazam app for recognizing songs just by listening to them, ACR does the same thing with TV shows, movies, and even ads. The software examines a snippet of the video and creates a sort of fingerprint of the content. It can then match this fingerprint to a database of known shows, and voila—your TV now knows what you're watching. And it wants to know this so that it can report and sell your viewing habits to others. They call it “post-purchase monetization” (I'm not kidding). I'll tell you how to stop this in the checklist.

A Note About Virtual Assistants

In recent years, Big Tech companies like Amazon, Google, Microsoft, and Apple have incorporated voice-activated virtual assistants into their various Internet-connected products: Alexa, Google Assistant, Cortana, and Siri, respectively. The idea is that you speak a “wake phrase” and then ask a question (“what's on my calendar today?”) or give a command (“remind me when I get home to bake a cake”). The virtual assistant, which presumably has access to things like your calendar, location, contacts, and so on, can give you a personalized response. This necessarily means that these devices have a built-in microphone which is constantly listening.

A common misconception about virtual assistants is that everything you say is transmitted to the company that owns the service—that these devices are glorified wiretaps or bugs. At least as they exist today, that's not true. The computers in these devices do listen constantly, but they're only listening for the magic word or phrase that triggers them to act. This sound processing is done locally on the device itself. Once you trigger the device with the wake word or phrase, then whatever you say next will be recorded and sent to the cloud for processing. These audio snippets are processed automatically by AI software, turning your speech into text and then analyzing this text to produce a response.

That's not to say that you shouldn't be wary about having these devices in your home. But know that, in most cases, no human will ever listen to these audio snippets and they will eventually be deleted⁷. For "quality control purposes," sometimes humans will listen to these snippets to make sure their systems properly interpreted your requests. This is done anonymously (i.e., they won't know who they're listening to). After some uproar, you can now opt out of this practice in the settings (usually in the associated smartphone app).

These devices currently require Internet connections, so they can send the snippets to powerful cloud computers for processing. As consumer devices get more powerful, this processing will eventually happen locally. Apple is already doing some Siri processing on your iPhone, so your requests don't have to go to Apple's servers at all.

BYPASSING THE BOUNCER

As we've just discussed, your home router does a lot to protect you—both from a security and a privacy perspective. It's the gatekeeper for your home network. However, there are two technologies that have the ability to bypass your bouncer, and they worry me greatly.

First, let's look at Internet Protocol version 6 (IPv6). Despite being around for decades, it really hasn't caught on yet. Because of Network Address Translation (NAT), we haven't really run out of IPv4 addresses yet. IPv6 has a nearly infinite number of addresses available, which is one of the main reasons for using it. If all our devices start using IPv6, then we won't need Network Address Translation—every single Internet-connected device can have a globally unique address. That means that your smart devices could be directly addressable from anywhere on Earth, if your router allowed this. In other words, bad guys could send malicious requests to your devices, hoping to hack them. I can only hope that routers will continue to implement this NAT function that effectively hides all your devices from the Internet, even though it's not technically necessary to do so with IPv6. We'll see.

Second, low-bandwidth cellular data plans (think LTE or 3G) and the cellular modem computer chips connected to these networks have become quite cheap. Given the penchant for "post-purchase monetization" by electronics manufacturers and the lack of regulation preventing data mining, I'm worried that newer IoT devices will bypass your home Wi-Fi all together

⁷One odd addendum to this... law enforcement agencies have subpoenaed these recordings for criminal investigations.

and just connect directly to the Internet over cellular. This would completely sidestep your home router. In fact, this is already happening with medical devices like CPAP machines. Insurance companies want to know that you're actually using these expensive devices that they're paying for, and so they require "compliance data" to be collected. In the old days, this meant storing data on an SD card and bringing that card to your doctor for verification of usage. But modern CPAP devices just automatically connect to the Internet using a built-in cellular modem—and you probably can't disable it. Also, all modern cars have built-in cellular modems, as well. They collect "telemetry" data on your vehicle, which I'm sure includes lots of personal information, too, including location, driving speed, and even potentially information from a paired smartphone. If this becomes really cheap, I expect IoT devices to all have this capability. And then your ability to control data collection is gone.

The Internet of Things is bringing us a ton of innovation and convenience, but device manufacturers have to step up their security game. Likewise, governments need to start requiring these devices to meet minimum security and privacy standards, including the ability to be remotely and automatically upgraded to fix software bugs as they're found.

Virtual Private Network (VPN)

Another network security tool you may have heard of is a *virtual private network*. Unfortunately, VPNs are widely misunderstood. VPNs have uses for security and privacy, but they're not the silver bullet that many VPN companies (and review sites) make them out to be.

As we've just discussed, the devices on your home network often make connections out to the broader Internet—to send and/or receive information from some server in the cloud. Until recently, many of those connections were unencrypted—that is, they used a plain HTTP connection⁸. This meant that the data itself was readable by anyone who could monitor the passing traffic, such as Internet service providers (ISPs), telecommunications companies, law enforcement, and cybercriminals. Thanks to a program called Let's Encrypt, created by a Big Tech industry consortium, the vast

⁸ HTTP stands for HyperText Transfer Protocol, which is the request and response language that I alluded to earlier in this chapter.

majority of Internet connections today are fully encrypted—they now use HTTPS connections, with the “S” standing for “secure.” This means that the contents of the data stream are unreadable by anyone other than the sender and the receiver. However, the metadata—things like “from” and “to” IP addresses, the time and duration of the connection, and the amount of data—are still visible and knowable.

Armed with this info, let me now explain what a virtual private network is and what it isn’t.

What a VPN Is

Using our analogy from Chapter 3, we know that sending data over the Internet is a lot like sending a letter through the regular postal system. But without encryption, it’s really more like sending a postcard. If you have a nosy mail carrier, they could read what you wrote. To prevent this snooping, you can encrypt your connection, which is akin to putting letters in a sealed envelope. But the mail carrier can still see who you’re sending it to—the envelope still has to have a valid “from” and “to” address. So let’s say you want to hide that, as well. How might you do that?

Well, you could engage a third-party carrier to act as an intermediary, say FedEx. You could then put your letters in a FedEx envelope and send it to the FedEx routing facility. Your carrier can’t see who your letter is going to, only that it’s going to FedEx. When FedEx receives your packet, it would open it and send the contained letter on to the final destination. Finally, to allow for a private response, FedEx would list itself as the return address on your letter. That way, if your recipient were to reply, it would go to FedEx first, and they would forward it on to you (in a private FedEx envelope). This has the added effect of hiding your real return address from the recipient. More privacy!

That’s all a VPN does. It wraps your digital traffic in an opaque virtual envelope (encrypts it) and funnels it through a third party (VPN provider) so that your ISP can’t see what you’re sending or who you’re communicating with. It also masks your return address from the recipient. That’s it.

What a VPN Isn't

But you wouldn't know this looking at the marketing language of many VPN services. A VPN doesn't protect you from viruses. It doesn't hide the amount and timing of your communications. It doesn't even encrypt your traffic all the way to its destination (though, again, most connections today are already encrypted end to end—just like most people send letters today and not postcards).

VPNs also don't prevent regular web tracking by the sites you visit. They have zero impact on tracking cookies, web redirect tracking, Referer header leaks, or browser fingerprinting (topics I'll discuss in the next chapter). That's because VPNs only hide your communications from outside third parties, not from the sites you're visiting. For example, in our analogy, there's nothing preventing you from revealing your real identity in the content of the letter you send (on purpose or by accident).

Also, you are just shifting your trust from your ISP to your VPN provider—in our analogy, from your local mail carrier to FedEx. Who's to say they're any more trustworthy? If FedEx offered to perform this service for you for free, then you should definitely be suspicious. How are they making money⁹?

You also need to understand that your traffic is only encrypted inside the VPN tunnel. It will eventually pop back out onto the regular Internet. Again, to relate this to our analogy, FedEx will eventually hand your package right back to the postal service to deliver it on the far end. And the mail carrier(s) can still tell how big/heavy your package is and when you sent it, which might leak some important information.

⁹The VPN market has gotten really slimy. Be very careful choosing your VPN.
<https://www.consumerreports.org/vpn-services/vpn-testing-poor-privacy-security-hyperbolic-claims-a1103787639/>

When Should I Use a VPN?

Using a VPN makes plenty of sense, in the right situations. Using a VPN will keep your ISP from keeping a record of the websites you visit and people you communicate with. (And make no mistake, they are doing this¹⁰.) It will also ensure that the contents of those communications are hidden, though again, most Internet connections today are already encrypted.

But be aware that some metadata is still visible. That includes when and for how long you send data and how much data you transmit. And remember that your Internet service provider is whoever is currently giving you access to the Internet. This includes your cell phone service provider when you're not on Wi-Fi and any public Wi-Fi hotspot host (coffee shop, restaurant, hotel, airport, etc.).

You may also be able to use a VPN to circumvent blocked websites and services—like watching US Netflix when you're traveling in Europe or getting to restricted websites from your corporate network or from a repressive country.

If you do choose to use a VPN, be ready for a lot of frustration. For example, VPN addresses are pretty well known and often blocked by sites that want to know who or where you are. You will likely trigger a lot of security checks, like CAPTCHAs and two-factor auth codes, too. And sometimes they just won't connect at all, forcing you to either disable your VPN or have no Internet connection.

¹⁰ Unfortunately, with the US privacy regulations being gutted in 2017, ISPs can legally track everything you do and sell that information to others. In the next chapter, we'll discuss another way to hide your Internet tracks from your ISP by using secure DNS.

Summary

- We reviewed the key parts of a home network and defined some common networking terms like *modem*, *router*, *Wi-Fi*, *LAN*, *WAN*, *WLAN*, and *VPN*.
- Your home router is the gateway to your home network and all of its connected devices. Built-in functions like the firewall and Network Address Translation (NAT) help to insulate your devices from the broader Internet, giving you both security and privacy.
- The Internet of Things (IoT) promises some amazing advances in connecting all of our electronic devices, but many of them are severely lacking in cybersecurity. This is already leading to threats from vast botnets and providing beachheads for cybercrime in otherwise well-protected networks.
- Virtual assistants are constantly listening, but they're not sending everything you say to the service in the cloud.
- Virtual private networks (VPNs) are becoming more important for everyday Internet users, providing security and privacy, as well as access to some region-restricted services like Netflix. But it's important to understand exactly what they do and don't do.

Now that we understand how the Internet works (Chapter 3) and we've reviewed the key components of your home network (this chapter), the next logical step is to talk about how to surf the Web securely and privately. I'll tell you all about it in the next chapter.

Going Further

- *Router security*: This website has a phenomenal amount of useful information. I'll cover all the key recommendations in the checklist for this chapter, but you can find more explanations and tips here:
<https://www.routersecurity.org/>
- *Blog articles*: I've written several articles about home network security, some of which I pulled into this book.

<https://firewallsdontstopdragons.com/be-my-guest-no-i-insist/>

<https://firewallsdontstopdragons.com/what-a-vpn-is-and-isnt/>

<https://firewallsdontstopdragons.com/stop-using-public-wi-fi/>

<https://firewallsdontstopdragons.com/the-s-in-iot-is-for-security/>

Checklist

One quick note before we start the checklist. If you have trouble with your home network or if you change some settings and all of a sudden you can't connect to anything on the Internet, you might want to reset your equipment. The proper way to reset your equipment is as follows:

1. Turn your equipment off including your modem, your router, and any other hardware devices like network switches, set-top boxes used for streaming music and movies, Internet telephony equipment (like Vonage or Ooma), and so on. (Computers and smartphones can probably be left on; they will usually sort themselves out on their own.) You can turn off these devices by unplugging them from the wall, or sometimes you can unplug the power cord from the back of the device itself. Give this about 30 seconds.
2. Turn the equipment back on starting at the point furthest “upstream.” In most cases, that will be your modem (the device you got from your ISP). Wait for your modem to come up completely. This usually means there are three to four solid lights and one rapidly flashing light.
3. Follow the chain downstream. The next device is probably your router. Power it back up and give it time to come up fully.
4. At this point, the next level downstream is probably the devices on your network. Turn them all back on.
5. If your computer or smartphone still can't connect after a few minutes, you might try restarting them, as well.

Many of the configuration items in this checklist require you to log in to your router. Unfortunately, every router is different—even routers from the same maker can have different configuration screens. There's really no way I can cover them all in this book, so you may have to do some searching around. Your best source is the manual that came with your router. If you can't find your manual, search the Web for it. Type in your router's make and model plus the word “manual”—that will usually find it. You can usually find your router's model info on a sticker on the router itself.

While you can use special software “wizards” to configure your router, you should also be able to access a special administration web page on your router that has the full configuration. In most home routers, there is a special IP address assigned to your router for this purpose—you can enter this IP address in your browser’s address bar to access the router’s admin page. Once you get to this web page, you’ll usually be asked to log in using the administrator credentials. Again, this will be in your router’s manual or maybe on a sticker on the router itself.

If you can’t find the manual, you try Table 7-1 for some common router info. If these fail, see the websites after the table. (In the table, [blank] means enter nothing; leave the field empty.)

Table 7-1. *Common Router IP Addresses and Admin Credentials*

Router make	Admin IP address	Default admin ID/password
Linksys	192.168.1.1	admin/admin
Belkin	192.168.2.1	admin/[blank], admin/admin, admin/ password
Netgear	192.168.0.1, 10.0.0.1	admin/password
D-Link	192.168.0.1	admin/[blank], admin/admin
Asus	192.168.1.1	admin/admin

For a longer list of router default IP addresses, try this:

<https://www.techspot.com/guides/287-default-router-ip-addresses>

For more default passwords, try this:

<https://www.routerpasswords.com>

Once you find this admin web page, spend some time looking around. Most of these special admin web pages will have helpful information right there to tell you what all the settings are for. Don’t let it overwhelm you, though—we will be tweaking only a few of these options.

Note Whenever you change administrative settings on your router, be sure to “save” and “apply” those changes. That is, sometimes you can change a setting, but nothing will actually happen until you save and apply the changes. Some changes may require your router to restart, which is fine—but you will lose Internet service for maybe a minute or two while the router comes back online.

Tip 7-1. Get Your Own Modem

Internet service providers will usually install their own modem for you to use, and that modem is often a combination modem and Wi-Fi router. They may also charge you a monthly fee to rent this modem, anywhere from \$5 to \$14 per month—which adds up quickly. However, in many cases, you can buy your own modem for as little as \$70 to \$90—it’s often the same make and model as the one your ISP gave you.

Note that ISPs don’t like this and sometimes will find ways to make this difficult. Be sure to check with them first to make sure they’ll let you hook up your own modem without any weird service charges or fees (this is supposed to be illegal now in the United States). You should also ask them which makes and models they support.

Modems use different types of communication protocols, and those protocol standards have versions. Generally speaking, the newer the version (i.e., the larger the number), the faster the connection speed. For example, cable modems use the DOCSIS standard. For most people, DOCSIS 3.1 will be good enough, but DOCSIS 4 is faster.

Tip 7-2. Get Your Own Wi-Fi Router

If you haven’t done this already, you should buy your own home router. Even if the modem given to you by your Internet service provider has a built-in Wi-Fi router, for privacy and security reasons, you should buy your own. Many of the tips in this chapter may be impossible if you don’t own the router.

- There are many good brands to choose from. I would go with a popular brand like Linksys, Netgear, Belkin, D-Link, or Asus.

- Wi-Fi routers are pretty easy to set up these days. However, you should *avoid using Wireless Protected Setup (WPS)*. While this technique is convenient, it's also fraught with security bugs. Just use the “old-school” method of setting a password on the router and entering this password on the Wi-Fi devices that you want to connect to the network.
- If you have a large home or “dead zones” where Wi-Fi signal strength is really low, you can look for a more expensive “mesh” network. Basically, you have multiple Wi-Fi boxes that work together to provide a bigger coverage area. If you do this route, I would avoid Eero, which was bought by Amazon. I wouldn't trust it for privacy reasons.

Tip 7-3. ★ Change Your Default Router Password

Your router will come with a preset user ID and password to configure the router through the admin web page (see Table 7-1). You should change this password as soon as possible, even if it looks like a good password. Malware will often try to log in to your router using well-known default passwords or predictable preset passwords, and if they get in, they can get up to all sorts of nasty business. You want to lock them out by changing the password to something the bad guys can't guess.

Generate a password using BitWarden and save it there. Since you'll access the router via a web page, BitWarden should fill it in for you, so it can be a truly strong random password. Don't be afraid to write this password down—you can even tape it to your router, if you want. The bad guys won't be in your house; they'll be trying to guess this password from some remote location.

Default passwords are so bad that California passed a law (SB-327) in late 2018 that bans this practice for all connected devices, which includes Wi-Fi routers. It wouldn't make sense for router manufacturers to sell something different in California from the rest of the world, so we should all benefit from this regulation. The law went into effect in January 2020, so if you bought a router recently, you may already have a unique admin password. However, I would still change it—sometimes these passwords are derived from knowable information, meaning they may be predictable.

Tip 7-4. ★ Update Your Router's Firmware

It's extremely important to keep your Wi-Fi router's software (sometimes called firmware) up to date. Using Table 7-1, you should log in to your router's admin interface and find the tab/page that lists the current version of the software installed (on appliances like this, the software is sometimes referred to as *firmware*). If you're lucky, this page will have a link or button to check for updates and install them if found. If not, you will need to go to your device's manufacturer website to see whether you're up to date. In either case, you may be asked to download a file and then upload it to your router for installation. (Note: If you can't update your router's firmware, it's time for a new router.)

If you've registered your router with the manufacturer, you should be notified of important software updates via email.

Tip 7-5. ★ Lock Down Your Wi-Fi

Always set a password for accessing your Wi-Fi network—that is, any device connecting to your network should require a password. (Your router admin page might call it a *key*, a *shared key*, or *passphrase*.) This password should be fairly strong, but it doesn't have to be crazy. People still need to be within Wi-Fi range to access it, so that limits the number of attackers. I would say use a short phrase that's easy to say and remember, maybe 12 to 15 characters long.

Use Wireless Protected Access (WPA) version 2 or 3 for your Wi-Fi encryption. This will be selectable on your Wi-Fi router's admin web page, usually as "WPA2-Personal" or "WPA3-Personal." WPA3 is the best option, which should be available on any modern Wi-Fi router. If your router still has WEP (Wireless Encryption Protection) or WPA (version 1 or no version listed), avoid them—they're not secure. If your router doesn't at least support WPA2, it's time to get a new router.

Tip 7-6. Use the Guest Network

If your router supports a guest Wi-Fi network, you should enable that. When enabled, your router will present to distinct network IDs (or SSIDs) for connecting—your main (private) network and the new guest network. This allows people who visit your house to have access to the Internet, but not to your regular home network. You might be

thinking: hey, I trust these people! But you never know what devices people are bringing into your home or where they've been. These devices may be compromised without them even knowing it. It's not worth the risk.

Be sure to set a password for the guest network, as well. You can put this password on your fridge or something, so your guests can easily see it and copy it to their smartphone or whatever. (See also the next tip.)

Tip 7-7. Create a QR Code for Easy Guest Network Access

You can make it easier for your guests to connect their smartphones to your Wi-Fi network by creating a handy QR code. This two-dimensional bar code embeds your Wi-Fi name (SSID) and the password into a little scannable image. Just open the camera app on an iPhone or Android smartphone and point it at the image. You can post this on your fridge or something. (You're going to want to use the guest network, though... see Tip 7-6.)

Unfortunately, many free QR code generators on the Web today are scams, particularly when it comes to creating web links. But to the best of my knowledge, this website is safe to use:

<https://qifi.org/>

Here's an example (Figure 7-3):



Figure 7-3. Sample QR code for guest network

Tip 7-8. Put Internet of Things Devices on the Guest Net

If you have smart devices in your home like thermostats, refrigerators, smart TVs, Wi-Fi digital picture frames, light bulbs, video doorbells, toasters, whatever... put them on your guest Wi-Fi network, not your regular Wi-Fi network. If these devices only need to talk to the Internet or to each other, then there's no reason to give them access to anything else within your home.

Note, however, that if you're not using the "smart" features, then don't bother connecting the device to the network at all—keep the devices "dumb." For example, if you're only using your TV for regular TV functions (and not for streaming services like Netflix), then there's no need to connect it to the Internet. Either don't configure the Wi-Fi settings or disable them. (If your device is connected using an Ethernet cable, just disconnect the cable.)

Tip 7-9. Disable External Admin

Some routers allow you to log in to their admin pages from *outside* your network—that is, from the public Internet or WAN. This is almost never necessary and extremely risky. If you find this feature on your router, make sure it's disabled. This also means not using smartphone apps to control/configure your router. If you can control or configure your home router from outside your home, then that means hackers will try to do the same. If you can't disable this feature on your router, I would seriously consider getting a different router. This is a security risk.

Tip 7-10. Disable WPS

People hate dealing with passwords, so someone decided to invent a way to make this easier: Wi-Fi Protected Setup (WPS). Sadly, "protected" was more of a marketing term—this technique was not truly secure. If your router has this feature, be sure to disable it. You can learn more about this, including how to verify that this feature has truly been disabled, here:

<https://www.routersecurity.org/wps.php>

Tip 7-11. Disable Universal Plug and Play (UPnP)

Some routers have a service called Universal Plug and Play (UPnP) that allows devices on your home network to open incoming connections. This was most often done with gaming consoles to allow for multiparty gaming over the Internet. This means poking holes in your firewall, which would allow hackers to get in from anywhere on the planet. That's bad. If your router has this feature, be sure to disable it.

While you're in this area of your router's configuration, look for any other external access features like telnet or SSH. Unless you really, truly need to control or configure your router remotely, you should disable any type of external access.

See the next tip for help testing your router's external vulnerabilities.

Tip 7-12. Probe Your Router for Vulnerabilities

One of my favorite security guys, Steve Gibson, has a website that will help you check to see whether your router or modem has any obvious weaknesses. It's a service called Shields Up (in reference to the Star Trek starship *Enterprise*). You might wonder if this is really necessary, but you need to realize that there are automated hacking systems on the Internet right now that are already doing these exact same port scans, continuously, looking for vulnerable systems. So your system has already been scanned, just not by you. You may as well find out what they found out.

1. Go to this website: <https://www.grc.com/shieldsup>
2. Read the little blurb in the box and then click Proceed.
3. The next few pages are a little hard to follow. First click the big yellow Instant UPnP Exposure Test button. This should verify that you've disabled external UPnP access.
4. Return to the previous page. In the following funny table, click the silver "Common ports" button, or if you want to go full tilt, click the All Service Ports button. It will scan your system to see whether any of these ports are accepting requests from outside, which they shouldn't be.

The ideal status here is “stealth” (green), meaning that your router completely ignored the request. The next best status is “closed” (purple), meaning that your router replied but denied the connection. If any of your ports are listed as “open,” then you need to go back to your Wi-Fi router’s admin page and find the setting for the listed service and disable it on the external (WAN) side. You can run the Shields Up test again to see if you succeeded.

Note that many ISPs will block these sorts of requests, too, trying to increase your security. So this test is actually testing both your ISP’s blocking and your router’s external port settings.

Just in case you don’t believe me, you can actually try to poke and prod your home router using some of the same tools the bad guys use. This website will show you how and even explain how it works:

<https://www.routersecurity.org/shodan.php>

Tip 7-13. Disable IPv6

Internet Protocol version 6 (IPv6) was built to replace version 4 (IPv4), mostly expanding the number of available IP addresses from four billion to effectively infinity. But your home network doesn’t need this, and I actually worry that it could be used to bypass security features in your router (see *Bypassing the Bouncer* earlier in this chapter). IPv6 can also be used to precisely locate you on a map (see the following article). For this reason, I would just disable it on your home router. This may not be a simple checkbox—if not, do some web searching on disabling IPv6 for your specific make and model of router.

<https://www.tomsguide.com/news/home-gateway-geolocation-bh21>

Tip 7-14. Change Your Default SSID

Your router will come with some default network name that it broadcasts, probably based on the model name. When you whip out your smart device and look at the available Wi-Fi networks, the names you see listed there are the service set identifiers (SSIDs) of all the Wi-Fi routers near you. Having a default name can be confusing, especially if your neighbors have similar names. But if the SSID contains information about what type of router you have, it can also give the bad guys a leg up on identifying known vulnerabilities.

I would change your SSID to be something more unique but also not obviously associated with you (like your name or street address). Note: If you change your SSID, you're going to have to reconfigure all of the wirelessly connected devices in your home that are using the old SSID. This can be painful if you have a lot of devices. The best time to change the SSID is when you're first commissioning a new router.

If you really want to get paranoid, you can prevent your router from broadcasting the SSID name at all. This might be some helpful security through obscurity if there are a lot of people near you, like in an apartment complex. Basically, you tell your router not to broadcast your network name SSID so that when people nearby scan for available networks, they won't see anything. To join your network, you will have to manually set up a connection by specifying the network name (SSID). (This is another great use for the QR code mentioned earlier.) However, a skilled hacker will still be able to find your Wi-Fi network, even if it's not broadcasting an SSID, so the more important protection is a strong password.

Tip 7-15. Register Your Devices

We all hate junk mail—electronic or otherwise. And we all know that when you register the products you purchase and give them your address, you can expect to increase your level of spam. However, for any product you have that connects to the Internet—including smart devices like TVs, thermostats, light bulbs, webcams, and also your Wi-Fi router—you want to make sure the manufacturer can contact you about potential security issues and remedies. For this reason, you should suck it up and register these devices online if you haven't already. Some of these devices will require manual software updates to fix security bugs; others may require outright replacement. But if you don't know about the bugs, they will just sit there, waiting to be hacked.

When you register online (using your make and model number or perhaps the serial number), you should get a confirmation email of some sort. Make sure that it didn't go to your junk mail or spam folder. If you see it there, you can usually mark it as “not junk,” which should tell your email service to not hide emails from this source in the future. If you want to be doubly sure, you can add the “from” email address to your email contact list.

Tip 7-16. Periodically Reboot Modem, Router

Your modem and your router are both computers running software. Any computer that runs for a while will build up some digital cruft—software resources that aren’t properly cleaned up. This can cause them to slow down, degrading your connection speeds.

Also, if a bad guy somehow managed to compromise your router and install malware, the malicious software will only exist in RAM because these devices don’t have hard drives. That means that the malware isn’t persistent—a simple restart will wipe it out.

For these reasons, I would periodically restart your modem and router—like maybe every couple months. Reread the instructions at the beginning of this checklist for help with this.

Tip 7-17. Disable Network Sharing Features

If your ISP’s modem comes with Wi-Fi built in, call your ISP and ask them to disable it. Assuming you have your own Wi-Fi router (explained earlier), you have no need for the ISP’s Wi-Fi, and so there’s no reason to leave it on—it’s just another way someone can try to hack into your home network.

If Comcast/Xfinity is your ISP, call Comcast and tell them you want to opt out of the Xfinity Wi-Fi service (1-800-XFINITY). You can supposedly disable this yourself, if you want to try:

<https://www.xfinity.com/support/articles/disable-xfinity-wifi-home-hotspot>

Some Amazon Ring and Echo devices have a similar shared network service called Amazon Sidewalk. You can disable it using the instructions here:

<https://www.amazon.com/gp/help/customer/display.html?nodeId=GZ4VSNFMBDHLRJUK>

Tip 7-18. Change Virtual Assistant Privacy Settings

If you don’t like the idea of a human listening to your Siri or Alexa commands, even anonymously, you can disable this “quality assurance” feature. Unfortunately, these settings are tedious to change and are hidden in euphemistic terminology like “improve dictation” or “improve transcription.” Look in the privacy settings on the associated smartphone app or online account. Here are some places to start:

- Amazon Alexa: <https://www.amazon.com/Alexa-Privacy-Hub/b?node=19149164011>
- Apple Siri: <https://www.apple.com/legal/privacy/data/en/ask-siri-dictation/>
- Microsoft Cortana: <https://support.microsoft.com/en-us/help/4468233/cortana-and-privacy-microsoft-privacy>
- Google Assistant: <https://support.google.com/assistant/answer/7126196?hl=en>

Tip 7-19. Use a VPN

Virtual private networks (VPNs) are often touted as a silver bullet for privacy. In reality, they have a few very specific uses that can increase your security and privacy (see the longer discussion in the chapter for details). The main reason for using a VPN is to hide your network traffic (e.g., the websites you visit) from your Internet service provider (ISP). Note that your ISP is whoever is giving you access to the Internet—when outside your home, this could be your cellular provider, a coffee shop or restaurant, or an airport or hotel.

When you use a VPN, you encrypt your Internet communications from your ISP, which is good. But you're now making this information available to your VPN provider. In effect, your VPN provider is now your ISP—so you're really just shifting your trust from one service provider to another.

VPNs can be handy for international travelers who want to access services that are restricted to their home region (like Netflix)—though most of the big-name services have gotten wise to this and just block all connections coming from known VPN service provider IP addresses.

VPN services are notoriously hard to objectively evaluate in terms of user privacy. While they all have stated privacy policies, those policies are usually hard to understand and impossible for you to verify. Furthermore, VPN review sites are often horribly biased due to referral kickbacks. However, some services are more adamant about their

commitment to your privacy and have in some cases paid for independent third-party audits to verify their privacy claims. I'm comfortable recommending any of the following services (and I've used most of them myself):

- Proton VPN: <https://protonvpn.com>
- Mullvad: <https://mullvad.net/>
- NordVPN: <https://nordvpn.com>

Tip 7-20. Avoid Public Wi-Fi and Use Cellular Data

Another alternative to using a VPN when connecting to the Internet while away from home is just using the Wi-Fi hotspot feature built into your smartphone. Most data plans today are effectively unlimited and include the “tethering” option that lets you connect your tablet or laptop to the Internet. This makes your cellular provider your ISP, meaning they can now see all your unencrypted web traffic and your connection metadata. But you're already giving them this information from the apps on your smartphone, so at least you're not bringing yet another party into the circle of (mis)trust. Of course, you can also use a VPN on your smartphone, but they're far from perfect. (We'll discuss this in Chapter 12.)

Tip 7-21. Disable Auto-Connect to Wi-Fi

Some laptops, tablets, and smartphones will automatically connect to public, open Wi-Fi when available (i.e., Wi-Fi service that doesn't require a password to connect). Some will also automatically reconnect to Wi-Fi networks that you've connected to before. Both of these are bad. You should tell your devices to always ask you before connecting to any Wi-Fi network, except for truly trusted networks. If you've given your home Wi-Fi a truly unique name, then it's okay to automatically connect to this network. But in general, you should always be notified first. Bad guys will often create fake networks with common names like “Linksys” or “Starbucks” or “Free Wi-Fi” in an effort to attack or spy on devices that auto-connect. If you use a VPN service that automatically turns itself on for untrusted networks, this can protect you in situations like this, too.

Tip 7-22. Dumb Down Your Smart TV

Smart TVs are notorious for tracking their users' watching habits. Most of them have a technology called Automatic Content Recognition (ACR). Of course, each manufacturer has a different propriety name for this feature and a particular, probably hard-to-find way to disable it. You can ask your TV not to track you and hope that it respects your wishes. This article covers most TV makers:

<https://www.consumerreports.org/privacy/how-to-turn-off-smart-tv-snooping-features-a4840102036/>

However, I would simply disconnect your TV from the Internet entirely by disconnecting the Ethernet cable or removing the Wi-Fi connection settings. If you want to using streaming apps like Netflix, Hulu, Amazon Prime Video, and so on, get a set-top streaming box instead. Now, of course, that box may tattle on your viewing habits, too—so I would invest in the one streaming box maker that has the least to gain from your private information: Apple. Yes, the Apple TV box is more expensive—but that's at least partially due to the fact that you're not subsidizing the manufacturer with your private data.

CHAPTER 8

Spies in Your Midst

Much of what we do today on our computers is surfing the Web¹. Unfortunately, browsing the Internet today means dealing with a vast array of tracking and other privacy dangers. So, in this chapter, we're going to learn about how to surf safely.

It's hard to believe that the World Wide Web is over 30 years old. While technically launched in 1991 by Tim Berners-Lee, most people didn't really know about it until the mid-1990s. The Web as we know it today really took off in the late 1990s with the "dot-com" boom and subsequent bust. We've come a long way since the early days of Mosaic and Netscape Navigator (the first popular web browsers). Web pages have gone from simple blocks of text and hyperlinks to amazingly powerful and complex websites that can do just about anything. Many of the tasks that were relegated to heavyweight software applications like Photoshop and Microsoft Office are now moving into "the cloud." With high-speed Internet connections and powerful new web technologies, there's so much you can now do within the confines of your web browser. In fact, Google has a whole operating system called Chrome OS that is essentially a web browser that acts as a full-fledged desktop operating system. (This OS is the basis for the popular and inexpensive Chromebook laptops.)

The way we access the Internet directly is usually with a web browser. Therefore, we need to find a good one—and by "good" I mean safe, not just full of whiz-bang features. Microsoft and Apple each has their own browsers that come with their operating systems: Edge on Windows and Safari on macOS. And because most people take the path of least resistance, these default web browsers tend to be popular on their respective platforms.² However, there are better choices out there, and in this chapter, I will help you choose the one that's best for you.

¹I must admit I never understood that phrase...wouldn't you be crawling a Web? Or even getting stuck in a Web? I guess it makes as much sense as "channel surfing," which is probably where we got the term.

²The term *platform* here refers to the type of computer and operating system you're using. So, if you hear the term *platform-independent*, it just means that it will work on all the major computer and operating system varieties.

Because web browsers have become the portal to the Internet, the bad guys have focused a lot of time and attention on finding ways to track, scam, and even infect you via this magical gateway. The functionality of a web browser can be extended in many ways, including plug-ins, extensions, and add-ons. I will help you figure out which of these are good, which are bad, and which are just plain ugly.

Certified Secure

Before we get into those specifics, let's dig a little deeper into how security works on the Web. This is going to sound rather technical, but it's important to understand the basics at a high level. Don't worry too much about the acronyms in this chapter—you don't need to memorize them. But I want to get the terms out there in case you've seen them before or run into them in the future. The real key thing to take away here is the general “web of trust” concept that forms the basis for our current Internet security scheme.

Recall that all your computer communications (in both directions) are chopped up into small packets and shipped out over a massive web of interconnected computers. The packets will take many hops before they reach their destination, and each packet could take a slightly different path—it doesn't really matter, as long as they all reach their destination. Previously in this book, we discussed the basic issues that we need to address when trying to communicate securely over the Internet. First, we need to somehow ensure that the person or website we're communicating with is actually who they say they are. Second, we would like our communications to be completely private—that is, we don't want anyone between us and our intended recipient to be able to read what we're saying or what data we're exchanging. Finally, we would also like to know that the messages haven't been tampered with along the way (you don't have to be able to read something in order to alter it).

The way we secure Internet communications and authenticate third parties is using a technology called Transport Layer Security (TLS).³ TLS is used all over the place today to secure all sorts of communication, including digital phone calls, file transfers with cloud storage providers, and, of course, web surfing. When TLS is added to regular web communications via a browser, we move from “HTTP” to “HTTPS”—the added S stands

³It used to be called Secure Sockets Layer (SSL). Some tech people use TLS and SSL interchangeably, but TLS is the proper term for the current technology.

for “secure.” When you are connected to a website via HTTPS, you should see a little lock icon to the left of the web address that indicates that the connection is secure.⁴ Most of this happens automatically behind the scenes. Your web browser and the server at the far end do some quick negotiation, and when both sides are capable of using TLS, they establish a secure connection.

But how do we really know that we’re talking to `amazon.com` or Bank of America? TLS trust is based on the concept of a certificate. There are special agencies called *certificate authorities* (CAs) that are in charge of verifying entities and issuing these special certificates that are digitally “signed” by the CA verifying its authenticity. These certificates are good for a certain amount of time, usually one to two years. When that time is up, the company or person who owns the certificate must reapply. If you click the lock icon in your browser (or perhaps right-click), you can dig down and see the nitty-gritty certificate information.

Figure 8-1 shows key portions of a TLS certificate for the *New York Times*. Again, you don’t need to know this stuff; I’m just showing you what it looks like. Most web browsers will let you see this info, if you know where to look. You can see that it includes the web domain name, the dates for which the certificate is valid, and who issued the certificate. You can also see technical stuff that should look familiar from our discussion in Chapter 3, including the public key and fingerprints (aka hashes).

⁴Note that this will be going away soon because HTTPS thankfully is becoming the default. Instead, you’ll be warned when a website is *not* secure.

Subject Name	
Common Name	nytimes.com
Issuer Name	
Country	US
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Common Name	Thawte RSA CA 2018
Validity	
Not Before	Mon, 14 Mar 2022 00:00:00 GMT
Not After	Fri, 14 Apr 2023 23:59:59 GMT
Public Key Info	
Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	CE:E3:11:BF:B2:B1:35:A3:B6:2F:E0:4E:1B:12:05:10:32:2A:72:60:88:1C:A...
Miscellaneous	
Serial Number	0E:B8:4C:2D:74:A2:76:1B:44:E4:52:7B:99:AB:6C:45
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)
Fingerprints	
SHA-256	62:ED:FB:19:BE:9F:95:CA:E7:60:C2:4F:10:B6:28:69:B6:BF:8D:17:1C:65:...
SHA-1	02:56:44:D7:EB:03:7B:7E:48:EB:F4:98:42:E1:3B:E3:D3:C7:A7:E8

Figure 8-1. Sample TLS certificate

Once the CA issues a cert to the owner of the website, the website provides the cert as proof of identity when establishing a secure connection. This is like showing your driver's license when buying booze to prove that you are who you say you are and that you're old enough to buy alcoholic beverages.

Trust the ID, Question the Issuer

But wait...driver's licenses can be faked. What about certificates? Well, I've got good news, and I've got bad news. The good news is that because certificates use solid cryptographic methods for creation, CA-backed certs can't really be forged. While it's possible to create "self-signed" certificates, no one is going to trust it for anything important. Web browsers have a built-in list of certificate authorities that they trust, and Joe Blow is not going to be on that list. Similarly, liquor shops in the United States would only accept driver's licenses issued by one of the 50 states, and they usually have a folder (or probably an app now) that shows what each state's license should look like. Creating a self-signed certificate is like printing up a homemade ID card on your printer and laminating it. Sure, it looks nice, but it's not going to get you into a bar. Self-signed certificates *can* be used to properly encrypt communications, but few browsers would accept them without warning the user.

So, that's the good news. The bad news is that there are other ways to get a certificate that are arguably worse. Creating a trustworthy certificate is a crucial task, so you'd think we would limit this job to a select few organizations that we can all agree to trust. In practice, there are hundreds of certificate authorities in the world, including the Hong Kong Post Office (I'm not kidding). Any one of these CAs can issue a completely authentic certificate that contains nothing but lies if they choose to. We trust them not to do this, but if they "go rogue" or if they get hacked, it's possible for bad guys to get perfectly legitimate certificates that will allow them to impersonate Google or Yahoo or whoever they want. It would be like getting your "fake ID" directly from the Department of Motor Vehicles... it would be fake only in the sense that it contained wrong information, but it's a perfectly valid driver's license that would pass any examination.

As bad as this sounds, in practice this is not easy to do. You're not worried about average teenager hackers in this situation; you're worried about highly skilled and well-funded attackers, probably backed by a government or a big corporation. The target in this case would mostly be information (espionage). Also, there are other safeguards in place that mitigate the risk of being duped by one of these bad certs. For one thing, even if the bad

guys get their hands on one of these mendacious certs, they still have to somehow get between you and your target server. This is a “man-in-the-middle” attack, which we discussed earlier—they insert themselves in the communication channel and pretend to be the other side to each end. That is, you establish communications with them, and then they turn around and establish communications with amazon.com, let’s say. To you, they appear to be amazon.com; to amazon.com, they appear to be you.

To do this, they need to somehow redirect you to the false website instead of the real one. When you type amazon.com into your web browser, it uses the Domain Name Service (DNS) to figure out where your request really needs to go on the Internet—that is, the IP address of Amazon’s web server. Unless you can somehow also intercept that DNS lookup and provide a hacked reply, then the user will still be connected to the real Amazon website. Also, there are new technologies coming online that will make this even more difficult in the near future (like Google’s Certificate Transparency⁵ project). So, while there are definite problems with the current CA-based system, it still works very well for the vast majority of web surfers, and other safeguards are being put in place to make it much harder to thwart or subvert.

And finally, most popular browsers only trust a subset of all possible CAs. Though that number is still in the dozens of providers, it’s not like your browser will just trust any certificate authority.

So, if we can assume that the certificate system works (which is, as we’ve said, a significant “if”), then we can assume that when we establish an HTTPS connection to another website that (a) we can believe they are who they say they are and (b) no one else can eavesdrop on our communications.

There’s one last—but crucial—point here. When your connection is using “https,” that means your traffic is encrypted and the certificate used by the website is valid. That’s all. It doesn’t mean you can trust the owner of the website. Any website today can get a free entry-level certificate, thanks to an effort by a large consortium of companies called Let’s Encrypt. That’s great—it makes it much easier for mom-and-pop companies to offer secure communications to their website. But the bad guys can also use this free service to obtain a valid certificate for a malicious website. So, “https” in the web address doesn’t mean the website you’re visiting is trustworthy; it only means that no one else can spy on your connection with them.

⁵<https://www.certificate-transparency.org>

Again, don't worry about remembering all the technical details. All you really need to remember here is that HTTPS connections are secure and private. Most websites have moved to HTTPS for all connections, which is a good thing, because everything we do on the Internet should be safe from prying eyes, even simple stuff. In the next section, we'll take a look at just how pervasive web tracking has become.

Tracking Tech

While secure communications are vitally important, we must also address the elephant in the room: web tracking. The amount of information you divulge every time you use a web browser is absolutely staggering: what websites you visit, how long you stay on a given website, how you got to that website (i.e., which site you just came from), whether you bought something on a given website, what ads you saw, what links you clicked, and even how much you spent while there. There has been a lot of debate on the value of this "metadata," but the proof is in the pudding, as they say. These companies wouldn't be bending over backward to get this info (and fighting regulation tooth and nail that would deny them this info) if it wasn't making them lots of money.

And just in case you think it's only retailers who are trying to find the right way to hook you into buying that spiffy new TV or antiaging cream, you should also know that political campaigns are using this data, too. Maybe they want to find sympathetic potential voters and even to identify voters who might be convinced to switch sides. But they would be just as happy to convince or trick people likely to vote for their opponents to stay at home on election day. The scandal involving Facebook and Cambridge Analytica is a shining example. And of course, this treasure trove of personal data is also potentially available to law enforcement and intelligence agencies, as well (foreign and domestic).

This data is often used to specifically tailor a website just for you—and not in a good way. For example, if the retailer happens to know that you're wealthy or that you're a heavy online shopper, they can actually make sure to show you the more expensive products first—in fact, they may even raise the prices⁶—if not based on your information specifically, perhaps based on whether you appear to be from a wealthy area.

⁶<https://lifehacker.com/5973689/how-web-sites-vary-prices-based-on-your-information-and-what-you-can-do-about-it>

The Webs We Weave

Most people just don't realize how wide and vast this tracking network really is. The best way I know to explain the pervasiveness of web tracking to you is to use a nifty little web tool called Lightbeam.⁷ When you go to a website, the content you see is often provided by multiple different companies. Think of a web page as more of a patchwork quilt, with each panel coming from many sources. In addition to the *first-party website* (the website you actually intended to visit), there are often many other *third-party websites* that provide ads and other images and also track what you're doing. To see these third-party relationships, Lightbeam draws a graph that shows you all the third-party sites that are associated with the first-party site you visited. (I know, all this "party" stuff sounds like legalese. It sorta makes your brain want to tune it out. But bear with me here.)

Let's try a real-life example and graph the relationships behind some popular websites and their hidden third parties. We'll start our browsing with Wikipedia.

In Figure 8-2, you'll see the first-party site as a circle—in this case, the one with a *W* in it, which is wikipedia.org. The little white triangle next to that is a third-party website that is associated with the site we visited. However, in this case, the third-party site is just wikimedia.org, which is directly associated with Wikipedia (i.e., it's not a third-party advertising or tracking site). It's not uncommon for the third-party sites to just be extensions of the first-party site. And it's also not uncommon for the third-party sites to be perfectly normal other websites that provide things like web tools, images, and other harmless content. However, many of them are marketing firms and other "Big Data" companies whose sole purpose is to build a portfolio on you.

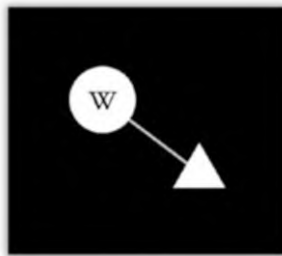


Figure 8-2. Wikipedia graph

⁷Unfortunately, this plug-in is no longer available, but thankfully I still have this data. It's a little old, but if anything things have gotten worse since I collected these images.

Now, let's go to Yahoo.com (Figure 8-3).



Figure 8-3. *Wikipedia + Yahoo graph*

Our little graph has now grown substantially. While Yahoo.com was our primary target (the big white circle at the left with the “Y” in it), we can see that we’ve also triggered a few *dozen* other sites, almost all of them tracking sites. Note that there is no intersection here between the two main websites—no common third parties. Wikipedia—since it doesn’t track you—is actually pretty boring in this regard, so from here on, we’ll just cut them out of our picture.

Now let’s move to amazon.com.

You can see in Figure 8-4 that loading Amazon’s website also caused you to communicate with several other third-party websites. Now we can see the overlapping third-party sites. Those are all tracking sites. And they now know that you went to Yahoo and then to Amazon, and they quite likely know a lot about what you did there. Starting to get the idea?

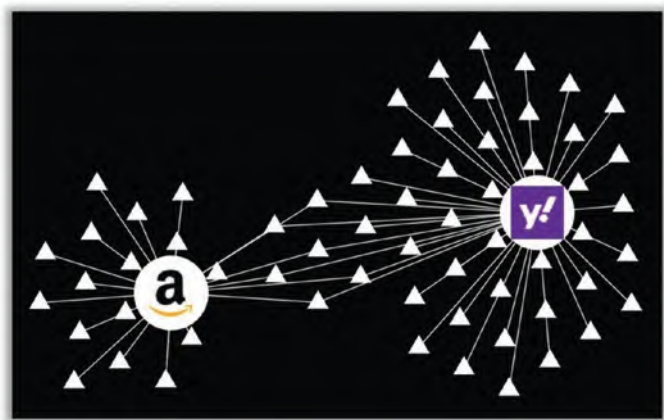


Figure 8-4. *Yahoo + Amazon graph*

Let’s go for the jugular now... let’s go to CNN’s website (Figure 8-5).

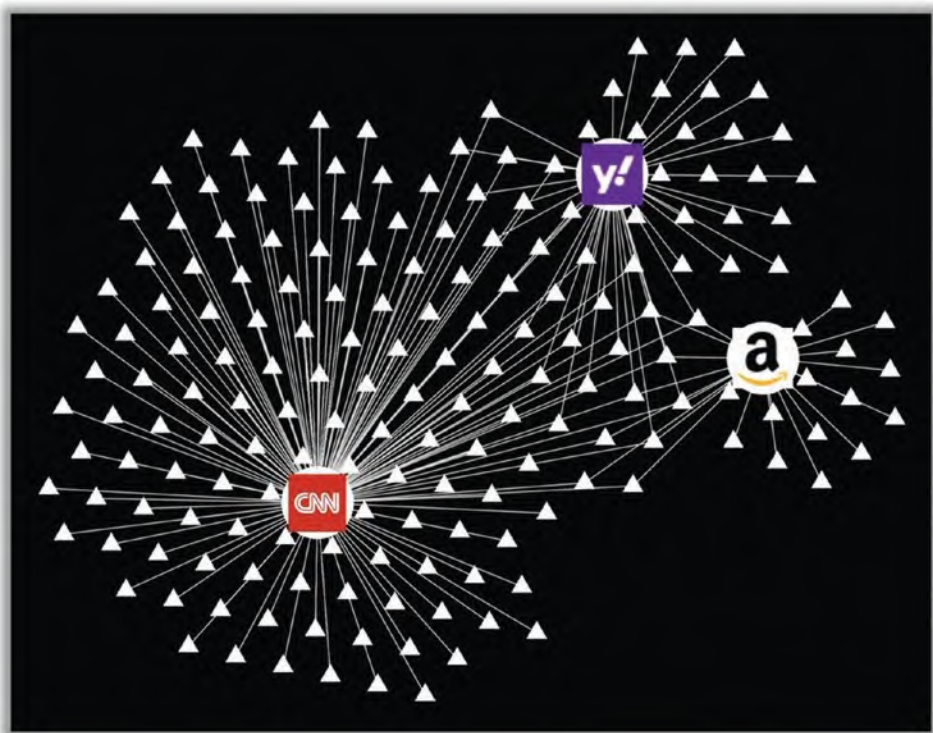


Figure 8-5. *Yahoo + Amazon + CNN graph*

The graph in Figure 8-5 is so crowded now that you can't really even read it. It's hard to tell, but there are 183 third-party websites there. You've visited just three websites so far (ignoring Wikipedia). The triangles that have multiple connections are the tracking sites.

So, just exactly how is it that they track you? The details would make your eyes glaze over. It's very technical and complex. But essentially it boils down to somehow marking you in a way that can later be recognized if they (or someone they know) see you again. These markers come in many forms. One of the most popular tracking devices is called a *cookie*. A cookie is a small bit of data that websites give to your computer, asking your browser to save it off and then repeat it back to them later when they ask for it. This is sort of like a medical chart—the information is kept on you, and when you interact with another party, they look at it to refresh their memories of you. These cookies were originally used by the first-party website to help keep track of your login, your personal preferences, your shopping cart contents, and so on. However, third parties have used them to mark people as they move around to different websites, tracking all sorts of stuff about you. That's the key point here... first-party cookies are between you and the site you *intended* to visit, which tends to be mutually beneficial; third-party cookies are things you generally didn't ask for and may not even be aware of, and it's almost completely for the benefit of the third party.

You're Being Stalked

Let's try an analogy to explain how this works. Let's assume that your local shopping mall wants to gather information on the people who shop there, and all the merchants agree to participate in the program. It's time for you to go Christmas shopping, so you park your car and walk in via the Macy's door. As you walk through the door, a silent little blowgun shoots a sticky dart that attaches to your back. This dart contains a little homing beacon that puts out a unique identifier, specific to you. They don't know who you are (yet), but they want to be able to distinguish you from all the other people wandering the mall. This ID is logged in a special computer system, along with a little note: "Customer 4372 entered mall via Macy's East door on first floor." This entry in the log automatically notes the time and date, as well. You walk through Macy's and into the mall proper. As you do, you walk by another sensor that detects your tag: "Customer 4372 left Macy's without buying anything." Since the time of entry and time of departure were so close, they could probably also conclude that you didn't even look at anything.

Now you walk into a jewelry store. You look around, find the perfect gift—a diamond tennis bracelet—and go to the register to buy it. Your entry to the store was of course logged, but now you’ve also made a purchase. They now know quite a bit more about you. If the store is trying to be nice, they may only log that you are a white male in his mid-50s who lives nearby (based on your credit card billing address) and that you bought an expensive piece of jewelry. From this, other retailers in the mall (who can see all of this information) may well assume that you are married and have an above-average income level.

You leave the jewelry store and head down to Victoria’s Secret, where you make a very different purchase on a rarely used credit card. Marketing data analysis may suggest that you have not just a wife but also a mistress. You now walk into an electronics store. The store personnel can see from your records that you’re in a buying mood today and you have plenty to spend, so they ignore other customers who show less promise and focus on you. They steer you to higher-end equipment, and given that you probably have a wife, they test your interest in kitchen appliances and push hard for you to get a store credit card.

This is all just from a single trip to the mall. Think about all the other places you’ve been and purchases you’ve made—what could they tell about you? How detailed would your profile be? And would you want that profile to be shared with every store you walk into?

The key here is that all the stores have contracted with the same tracking company. They have a common set of sensors that are all networked together, creating a central place to log your activity. While you might think it’s entirely reasonable for a given store to keep information on previous buying and shopping activity, how do you feel knowing that information is being shared with many other retailers (and credit bureaus, potential employers, insurance companies, etc.)? It may be that this tracking company hoards the juiciest bits of information and gives only partial information to each store owner (depending on what level of service they’ve paid for). But it’s important to realize that even with the best of intentions, the fact of the matter is that that information exists somewhere—and therefore it can be stolen, abused, or even compelled by the government.

Hey, I Know You

But we’re just getting started! There are several other tracking mechanisms, as well. People have gotten wise to the third-party cookie tracking method and have learned how to block them, so marketing companies have come up with other ways to track you—ways that can be very difficult to avoid. If they can convince (or trick) you into installing

a browser extension, they can potentially access all of your web surfing data. Even those social media buttons such as Facebook’s Like, Pinterest’s Pin It, and Twitter’s Tweet can be used to track you—*even if you don’t click them!* Sometimes they use tiny little one-pixel images with unique names... when your browser loads that image, they know you’ve been there. Sometimes they use invisible web form fields. The list goes on and on, and the exact techniques change all the time.

Some really clever folks have figured out ways to “fingerprint” your web browser. To help websites present themselves optimally, your web browser gives up all sorts of detailed information about your computer and web browser configuration: what plug-ins you have installed (even if they’re disabled), all the fonts you have installed on your computer, computer screen dimensions, what type and version of operating system you’re running, and what type and version of browser you’re using. The idea behind browser fingerprinting is that few people will have the exact same combination of these items.

Finding this a little hard to believe? Or maybe it just seems too esoteric. Well, the Electronic Frontier Foundation (EFF) has a website you can visit that will tell you just how unique your configuration really is. Take a minute to click this link and see just how recognizable you are:

<https://coveryourtracks.eff.org/>

When I run this test, I get the following result (Figure 8-6):

Our tests indicate that you have strong protection against Web tracking.

IS YOUR BROWSER:

Blocking tracking ads?	<u>Yes</u>
Blocking invisible trackers?	<u>Yes</u>
Protecting you from <u>fingerprinting</u> ?	<u>Your browser has a nearly-unique fingerprint</u>

Figure 8-6. My “Cover Your Tracks” report

I'm a privacy and security guy. I have many anti-tracking tools installed, which this tool affirmed. And yet, my browser has a "nearly unique" fingerprint. The report told me that "within our dataset of several hundred thousand visitors tested in the past 45 days, only 1 in 111819 browsers have the same fingerprint as yours." That means that websites that perform these same fingerprinting techniques would be able to recognize me wherever I go—website A and website B will know that I'm the same person. And if one of those websites happens to also know who I am, they can now associate my identity with that fingerprint. And because they're almost surely using a third party to do this fingerprinting, this information is automatically being shared with many other sites. Looking at the detailed report, I can see what information gave me away (made me more unique). The two factors that were most unique about me were my browser's *user agent* (which includes both my operating system and browser versions) and my gigantic monitor.

Unlike regular cookies and other forms of tracking, there is no way to know that your browser is being fingerprinted, and it's very hard to prevent. It's just not easy to disguise yourself as you traverse the Internet. In this case, your best defense would be to look like everyone else: try to blend into the crowd. Unfortunately, many of the measures you might take to increase your online security and protect your privacy also tend to make you stand out because so few of us take the time to install these tools.

Tracking in Real Life

The shopping mall story we used to explain web tracking is not just an analogy. You're being tracked in the real world very much like you're being tracked in the virtual world.

Video cameras are everywhere now. In the old days, these were big, ugly analog CCTV security cameras with crappy resolution that were hard not to notice. Now the cameras are digital, incredibly tiny and very high resolution. The old cameras recorded to VHS tapes that could store only a few hours of footage would only be viewed by the owner of the store and would eventually be overwritten. Modern cameras send their data to cloud-based servers with nearly infinite storage capacity and are combed through by automated tracking software. The monitoring systems will track where you go in the store, how long you look at that end cap sale, and how often and when you come to the store and may even be able to recognize your face and assess your reactions. And like web tracking, these third-party companies correlate this data across multiple stores and locations. These systems are everywhere in China, and the government there requires

that you register your face with the system. People in China can pay for food at vending machines and ride public transit simply by looking toward a camera.

Several companies are now marketing systems that will use high-resolution video cameras to scan a scene to find all the license plate numbers it can see. The system records each plate number along with the time and place it was seen, and many can then look up these numbers in state databases to match them to their owners. These cameras are being mounted on utility poles, traffic lights, overpasses, and even police squad cars as they patrol. This information is hoovered up and shared with other agencies, creating a massive database of millions of cars. The timestamp and location information can be used to track where you go, identify your travel patterns, and even (potentially) track who you associate with. While this could obviously be useful finding who was near the scene of a crime and where those people live and work, it could just as easily be used to track an ex-wife, patrons of a gun show, patients at a planned parenthood clinic, or people attending a political protest.

I know it sounds hyperbolic, but we are truly living in an era of constant, global surveillance. Unlike the eighteenth-century panopticon envisaged by Jeremy Bentham, we have the computing power to actively monitor a large swath of the populace in real time. And with massive data storage facilities, our watchmen can record massive quantities of our activity, review it later at their leisure, and store it effectively forever.

Cardinal Richelieu once said:

If you give me six lines written by the hand of the most honest of men, I will find something in them which will hang him.

No one is perfect. We make mistakes all the time. We even break the law from time to time. Have you ever gone over the posted speed limit or jaywalked? But for most of human history, if there was no one there to see these transgressions, they were lost in time and forgotten. (If a tree falls in a forest...) But if I had the ability to review everything you've ever done, the chances are nearly 100 percent that I could find something with which to blackmail you or maybe even put you in jail. That's the dangerous power imbalance that all this data collection can create.

Information Leakage

As you can see, it's hard to hide your tracks as you surf the Web. But there are even more ways in which your web surfing is tattling on you.

DNS Queries

As we've discussed in early chapters, when you enter a web address into your browser like "amazon.com," your computer must convert that human-friendly hostname to a computer-friendly IP address. This is done via the Domain Name Service (DNS). Your computer is usually given its DNS provider automatically when it's connected to your home network, at the same time that your computer obtains its local IP address. Your home router is in charge of this, and it all happens behind the scenes without you having to do anything⁸. Your router usually gets its DNS service from your Internet service provider, in much the same manner. So, when your computer asks the router to convert "amazon.com" to an IP address, your router turns around and asks your ISP to do it.

Unfortunately, unlike much of our regular communication now on the Internet, DNS queries are not encrypted by default. And because we have rolled back regulations on what your ISP can track, they are more than happy to keep information about every website you visit and sell it to the highest bidder.

To fix this, you need to choose another DNS provider—preferably one that supports encrypted DNS queries so that your ISP can't see what hostnames you're looking up. The best way to do this is to just alter the DNS provider on your router—change the default to something better. This means every device in your home network will inherit this setting. However, for smartphones and laptops that will leave your home network, you'll want to change this setting on these devices, as well.

Note that this isn't a silver bullet. All web traffic must contain "to" and "from" IP addresses, and if you can look up the IP address from the domain name, then you can also do the reverse. The real solution is using a VPN, but that's hard to do 100 percent of the time. Encrypting your DNS queries still has value.

⁸This is part of the DHCP protocol we discussed in Chapter 7.

Referer Header

There's another obscure way that your computer rats you out, and it's built into the most basic part of the Internet: Hypertext Transfer Protocol (HTTP). Your browser is just trying to be helpful, really, but in doing so it's oversharing. When you enter a web address (<http://something.com>), your web browser hands over lots of potentially helpful information to the website you visit, including the website you just came from. This data is passed to the new website through the Referer header (yes, it's misspelled... a classic Internet-ism). Why? Well, sometimes websites work together, so it's helpful for them to know how you got to the site. It's also a way to pass data on to the next site. But if the website isn't careful, it can share too much information (TMI).

Here's an actual example of a Referer header from the US government website everyone loves to hate, healthcare.gov:

```
Referer: https://www.healthcare.gov/see-plans/85601/results/?  
county=04019&age=40&smoker=1&pregnant=1&zip=85601&state=AZ&  
income=35000
```

Take a close look at the info contained in there. Those are parameters that the user had submitted to the website, probably in a form page. As a quick-and-dirty way to pass that data around to other pages on the healthcare.gov site, it simply included the form values as parameters with the web address. And this full string of characters would show up in the HTTP Referer header. Therefore, as soon as you leave healthcare.gov and go to amazon.com, let's say, Amazon would get all that info, as well—and you wouldn't know it. This bug was fixed on healthcare.gov, but who knows what other websites might be oversharing like this? Luckily, at least one browser maker is automatically cleaning up this for you. We'll discuss that shortly.

Web Form Data Leakage

Speaking of web forms, I need to let you in on another dirty little website data-slurping secret. How many times have you started filling in a web form—maybe to sign up for an account or to answer a survey—and then changed your mind because you felt it was getting too personal or something? So, you closed the page without hitting Enter or Submit. No harm done, right? Maybe not. It's technically feasible for websites to store all the data you enter into a form, *even if you never submit it*. A web technology

called JavaScript that can be used to make sure that you entered good data (e.g., a valid telephone number or email address) can also be used to save that data. That may sound really slimy, but it's really being done on some sites.

Web form data can leak via spell checkers, too. Chrome and Edge browsers both have the ability to enable "enhanced" spell checking. When you turn this feature on, information you enter into web forms may be silently sent to cloud servers for the enhanced checking as you type it. This could include credit card numbers and even passwords, if they aren't hidden. You can hope that Google and Microsoft aren't saving this data and are handling it securely so that no one else can see it... but mistakes happen.

On the Ethics of Ad Blocking

The business model for most of the Internet revolves around advertising, which in and of itself is not a bad thing. It may be an annoying thing, but passive advertising isn't harmful. Passive advertising is placing ads where people can see them. And savvy marketers will place their ads in places where their target audiences tend to spend their time. Pardon the stereotyping, but if you're targeting middle-aged men, you might buy ad space on fantasy football or car racing websites. If you're targeting tween girls, you might buy ad space on any site that might feature something about Ed Sheeran or BTS. And if it stopped there, I don't think many of us would object or at least have solid grounds for objection. After all, this advertising is paying for the content we're consuming. Producing the content costs money, so someone has to pay for it or the content goes away.

Unfortunately, online marketing didn't stop there. On the Web, competition for your limited and fickle attention has gotten fierce. With multiple ads on a single page, marketers need you to somehow focus on their ad over the others. And being on the Internet (and not a printed page), advertisers are able to do a lot more to grab your attention. Instead of simple pictures, ads can pop up, pop under, flash, move around, or float over the articles you're trying to read. Worse yet, ad companies want to be able to prove to their customers that they were reaching the right people and that those people were buying their product. This makes their ad services far more valuable, meaning they can charge more for the ads. The classic marketing adage was this: "Half the money I spend on advertising is wasted; the trouble is, I don't know which half." This is the problem that targeted ads are claiming to fix.

Enter the era of “active advertising.” Today, you’re not just watching ads—those ads are now watching you back. The code that displays these ads is tracking where you go and what you buy, building up profiles on you and selling those profiles to marketers. (This is often referred to as “behavioral” advertising, as opposed to “contextual” advertising.) Furthermore, those ads use up data plans on cell phones and take a lot of extra time to download regardless of what type of device you use. And if that weren’t bad enough, ad software has become so powerful, and ad networks so ubiquitous and commoditized, that bad guys are now using ad networks to distribute malware. We call it *malvertising*.

Over the years, browsers have given users the tools they need to tame some of these abuses, either directly in the browser or via add-ons. It’s been a cat-and-mouse game: when users find a way to avoid one tactic, advertisers switch to a new one. The popular modern tool in this toolbox is the ad blocker. These plug-ins allow the user to completely block most web ads. Unfortunately, there’s really no way for ad blockers to sort out “good” advertising from “bad” advertising. Adblock Plus (one of the most popular ad blockers) has attempted to address this with their “acceptable ads” policy, but it’s still not perfect.

But web content providers need that ad revenue to stay afloat. Many websites are now detecting ad blockers. When you block their ads, they either nicely ask you to “whitelist” their website (allowing their site to show you ads) or in some cases actually block the content unless you turn off ad blocking. In a few cases, you have the option to just pay for a subscription, directly paying for the content.

So...what’s the answer here? As always, it’s not black and white. I fully understand that websites need revenue to pay their bills. However, the business model they have chosen is ad-supported content, and unfortunately the ad industry has gotten overzealous in the competition for eyeballs. In the process of seeking to make more money and differentiate their services, they’re killing the golden goose. Given the abusive and annoying advertising practices, the relentless and surreptitious tracking of our web habits, the buying and selling of our profiles without our consent, and the lax policing that allows malware into ads, I believe that the ad industry only has itself to blame here. We have every reason to mistrust them and every right to protect ourselves. Therefore, I think that people are fully justified in the use of ad blockers—and I wholeheartedly recommend that you use them.

That said, websites also have the right to refuse to let us see their content if we refuse to either view their ads or pay them money. However, I think in the end they will find that people will just stop coming to their websites if they do this. (It’s worth noting that some sites do survive quite nicely with voluntary donations, like Wikipedia.) Therefore,

something has to change here. Ideally, the ad industry will realize that they've gone too far—that they must stop tracking our online pursuits and stop trafficking in highly personal information without our consent—and voluntarily change their ways. But it hasn't happened yet.

Personally, I think we just need to outlaw behavioral advertising and go back to contextual ads (buying ads based on generic demographic data and aggregate analytics). This is the way advertising worked for centuries. But ad companies have convinced content providers that behavioral ads are far superior to contextual ads. Right now, behavioral advertising is completely dominated by Facebook and Google, because they know the most about us. Moving to non-targeted ads would put all marketing companies on equal footing and open the space to competition.

The bottom line is that the ad industry has itself to blame here. They've alienated users and if they're not careful, they're going to kill the business model for most of the Internet. They must earn back our trust, and that won't be easy. Until they do (or until we outlaw behavioral advertising), I think it's perfectly ethical (and frankly safer) to block ads and the creepy tracking tech that comes with them.

Choose Your Weapon

Your primary interface to the wild and woolly Internet is the venerable web browser. For many people, the web browser *is* the Internet. So, it stands to reason that you would want to pick the safest browser to do your web surfing.

There are at least two primary aspects to safety when it comes to web browsing: security and privacy. A secure browser will do whatever it can to prevent you from visiting bad websites, warn you against entering sensitive information on insecure pages, identify sites that aren't encrypted, and strictly enforce policies that prevent malvertising and other malicious web exploits. A private browser will help protect your privacy by severely limiting the ability of websites and marketers to track you.

According to GlobalStats statcounter, the most popular browsers as of May 2022 are Chrome (67 percent), Edge (10 percent), Safari (10 percent), and Firefox (8 percent). Edge is the default browser on Windows PCs, and Safari is the default browser on Apple Macintosh computers. Firefox (which rose from the ashes of Netscape Navigator) is the only browser in the top 4 that is open source (meaning the software code is freely available for inspection by anyone). Firefox is made by the nonprofit Mozilla Foundation,

which is funded primarily by search royalties (accepting money to set a particular search engine as the default). Despite very different aesthetics, at the end of the day, all four of these browsers do basically the same thing: they show you web pages. So, how do you know which is safest?

Most Secure Browser

Let's just get this out of the way now: it's almost impossible to say which browser is the most secure. This is largely because all of these browsers are constantly rolling out new security-related features, fixing security-related bugs, and generally trying to claim the title of "most secure." That's a good thing—they're competing to be the best, so we all win. There are dedicated hacking contests to reveal bugs in web browsers, but it's hard to say whether the number of bugs found in these contests really reflects the security of the browser. How likely were the bad guys to find these bugs? How severe were the bugs? What about the bugs the researchers didn't find? These metrics also don't address factors like how quickly the browser maker fixes their bugs and whether the browser is smart enough to self-update (because if you don't have the latest version, then you don't have the bug fixes). It's really hard to compare the relative security of web browsers.

However, if I had to pick a winner here, I'd probably have to choose Chrome. Google is doing some fantastic work in the realm of computer and web security. That said, I think Firefox and Safari are also very secure browsers. And you could argue that because Firefox is open source, it can be audited by cybersecurity experts—unlike the other three major browsers. Theoretically, this third-party vetting leads to fewer bugs.

Most Private Browser

Unlike security, there are significant and important differences between the four top browsers when it comes to privacy. And this (to me) is the real deciding factor.

While Google has been a true leader in terms of security, it's pretty much the worst in terms of privacy. Its whole business model revolves around advertising (Google makes almost 90 percent of its money from ads⁹). And that leads to an enormous conflict of interest when it comes to protecting your personal data and web surfing habits. Apple has gone out of its way to basically be the anti-Google, making it a point of pride to

⁹<https://www.investopedia.com/articles/investing/020515/business-google.asp>

collect as little data on their users as possible (and causing a collective freak-out by advertisers because of its technology that limits tracking). But Firefox is also doing some great work in this area and adding more privacy features all the time.

So, who's the winner in terms of privacy? Among the top 4, I'd say it's a toss-up between Firefox and Safari, with Chrome being dead last. Edge is somewhere in between, but with Microsoft's recent penchant for collecting user data, I would put it closer to Chrome. Chrome has been trying to tame obnoxious ads with a built-in ad-blocking technology, but it's important to note that it does nothing, really, to prevent tracking. And even if Google were protecting you from other companies tracking you, you should assume that anything you do in the Chrome browser is known to Google. In fact, as of June 2020, Google is being sued for continuing to track its users while in "incognito mode."¹⁰

And the Winner Is...

Based on everything I've found in my research, I believe Firefox is the best web browser for most people. No browser is 100 percent secure, and it's hard for even the most erstwhile browser to completely protect your privacy. But I think Firefox, on balance, is the best of the top 4 browsers. However, there are two other options that I'd like to bring to your attention before we declare a winner.

The Brave browser is a relatively new browser built specifically for privacy. It has built-in ad-blocking and tracking protection, and even its own private search engine. It's built using Chromium, which is Google's open source web browser engine. I'm not sure why Google did this, but it released the software for the core of the Chrome web browser for anyone to use. Chrome, Edge, and Brave are all built off of the Chromium engine, as are lesser-known browsers like Opera and Vivaldi.

So how does Brave compare to Firefox? Quite well, actually. In some ways, I'd even say it's slightly superior—mostly because it's preconfigured for privacy, whereas Firefox requires some "hardening" to maximize your privacy. However, I don't like the fact that Brave is based on Google's web engine, Chromium. While Google has mostly kept their data-gathering tech out of the core engine, it can still make design decisions that will make it more difficult for browsers that use the engine to block ads and limit tracking¹¹.

¹⁰ https://www.vice.com/en_us/article/m7jvvp/google-sued-tracking-users-incognito-mode

¹¹ <https://www.eff.org/deeplinks/2021/12/chrome-users-beware-manifest-v3-deceitful-and-threatening>

But looking at the bigger picture, Firefox is basically the only cross-platform browser left that isn't based on the Chromium engine. We absolutely need competition, and we need non-Google browsers to exist. Therefore, it's crucial that we support Mozilla's struggling Firefox browser. If it goes under, Google will have even less incentive to keep its tracking tech out of Chromium. So, when I take all of these factors into consideration, I choose Firefox as the best web browser.

I will give a very honorable mention to one more browser: the Tor Browser. This browser was crafted specifically to be an *anonymous* browser—to allow you to surf the Web without giving away your identity. It uses the Tor network and a special “onion routing” technique to keep websites you visit from being able to figure out who you are. It's actually based on Firefox and builds in several kick-butt privacy tools that are too technical to sum up here. But if you really need to surf privately, you should give the Tor Browser a serious look. Just note that it's a good bit slower than other browsers, due to the special onion routing privacy technology.

Summary

- Surfing the Web is one of the main ways in which we interact with our computer and the Internet, and as such, it's one of the most important things that we need to secure.
- Our web security system is based on special digital certificates that are used to (a) prove that you're talking to who you think you are and to (b) encrypt the communications between you and the other end. While the certificate authority system has flaws, it's the best we have right now, and it's good enough for most things.
- We've learned why and how your actions are tracked via the Web. Simple things like web cookies and nearly invisible images can be used to track everywhere you go, reporting the information back to central locations run by marketing companies. Worse yet, the configuration information your browser provides to every website can be used to recognize you.
- We are also now being tracked in the real world, not unlike we're tracked on the Web. Facial recognition, ubiquitous cloud-connected HD cameras, automated license plate readers, and cell phone location tracking are just some of the privacy-invasive technologies being used.
- We saw how your browser leaks information about you in several other ways: DNS lookups, Referer headers, and web forms.
- When choosing a web browser, you need to consider both security and privacy. While all browsers attempt to be secure, only a few are really trying to protect your privacy.

In this chapter, we talked about security and privacy when connecting to nameless servers on the Internet. In the next chapter, I'll tell you how to keep your person-to-person communications secure and private.

Going Further

There are a lot of great resources on the Web for surfing safely. Here are a few of my favorites.

- *Who Tracks Me*: This site has some eye-opening stats on web trackers on popular websites: <https://whotracks.me/>
- *Privacy Tests*: This site maintains a staggering amount of privacy information about all the popular web browsers: <https://privacytests.org/>
- *De-Googling My Life*: I wrote a series of blog articles on trying to replace all the Google services in my life. Part 1 dealt with Google Chrome and Google Search, which is relevant here: <https://firewallsdontstopdragons.com/de-google-my-life-part-1/>
- *Techlore Firefox Hardening*: The guys at Techlore do some amazing stuff. I know Henry pretty well and we've each been on the other's podcast. They have a great guide for locking down Firefox: <https://www.youtube.com/watch?v=F7-bW2y6lcI>
- *Protect Yourself from Online Tracking*: This one article has links to several guides on privacy protection, many related to web surfing, but also several others: <https://privacyinternational.org/act/protect-yourself-online-tracking>

Checklist

I have to give one caveat here. Many security and privacy tools can cause some websites to act strangely or even fail to work at all. This is an unfortunate side effect of trying to protect yourself from tracking technologies that are ubiquitous and deeply embedded in the Web. When you come to a website that no longer seems to work properly, you may need to try adding a special exception for that website or disable some plug-ins temporarily. I realize this is painful. As with all security choices, you need to weigh safety against convenience. I would try to be safe by default and make security exceptions only when necessary.

Tip 8-1. ★ Use a Privacy-Protecting Browser

Choosing a secure and private web browser is important. While Google's Chrome browser is very secure, they have a severe conflict of interest with regard to your privacy. Google potentially has access to everything you do in that browser, and that should give you the creeps. Google already knows *way* too much about us.

For me, the best browser to maximize both security and privacy is Firefox. However, if you're purely a Mac user, the Apple Safari browser is also good (though it has some peculiarities when it comes to supporting browser plug-ins like the ones I'm going to recommend here). The Brave browser is quite good, too. If you find that you don't like Firefox for some reason, give Brave a try.

Note You do not need to sign up for a Firefox account to use Firefox. You can just bypass or skip the sign-up screens, if you're presented with any. But if you use Firefox on multiple devices, having an account will allow you to synchronize your bookmarks and settings, which can be very handy. There are also some very helpful Firefox services that will require an account. It's your choice and you don't have to decide right now; you can always sign up later.

- Download and install Mozilla's Firefox browser: <https://www.mozilla.org/en-US/firefox/new>
- Launch the web browser and go through first-time setup. If asked whether you want to make Firefox your default browser, say yes. This may take you to a system preference where you have to change the default setting.
- If asked, you will probably want to go ahead and import bookmarks, favorites, and so on, from your current web browser. However, *do not import passwords*. BitWarden has that covered and we'll handle this in a later tip.

Tip 8-2. ★ Configure Browser for Security and Privacy

Again, I'm going to assume you're using Firefox here. If you're using Brave or Safari, see these links:

- Safari privacy settings: <https://defendingdigital.com/apple-safari-security-privacy-guide/>
- Brave privacy settings: <https://www.privacyguides.org/desktop-browsers/#brave>

To get the best protection, you need to change some default settings.

1. Open the Firefox menu at the upper-right corner of the browser window. It looks like three horizontal lines and is sometimes affectionately called the “burger” menu (because it looks like a hamburger). Click Settings, which is toward the bottom (Figure 8-7).

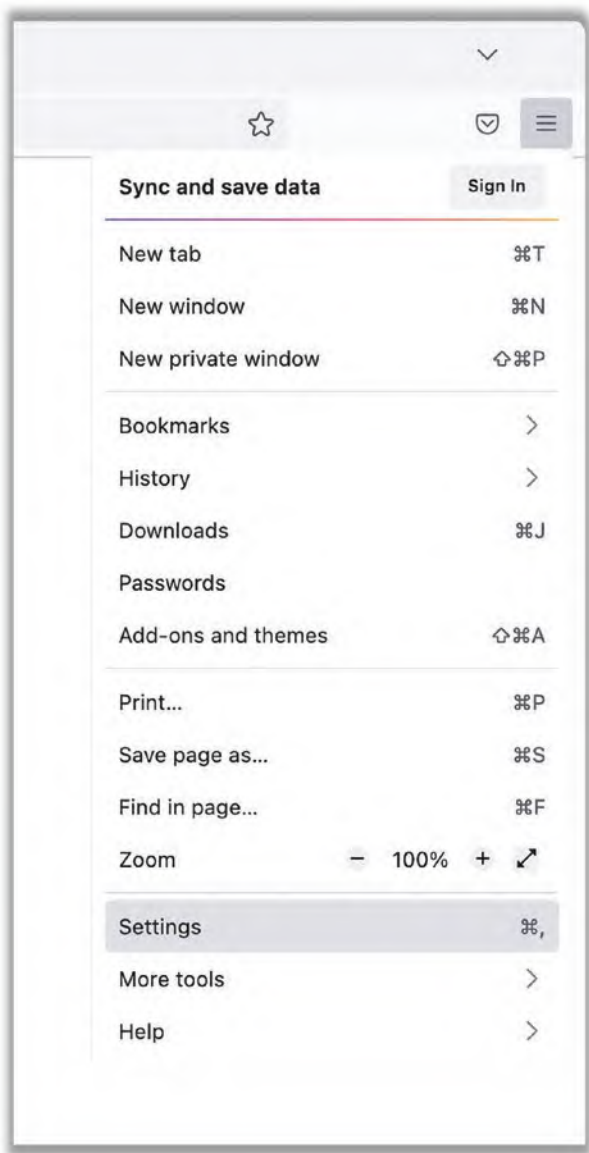


Figure 8-7. *Firefox settings menu*

- 2. Select the Privacy & Security tab at the left. Under “Enhanced Tracking Protection,” you can either select “Strict,” or you can create a custom set of security and privacy settings (Figure 8-8). I personally prefer Strict mode because Firefox adds new privacy features all the time, and selecting this mode generally means that

I get those features automatically when I update the app. Note the warning here—it’s for real. These settings may cause some websites to act weird or fail to load, though I haven’t had much problem with this, personally. If you change this setting, click the “Reload All Tabs” for it to take effect.

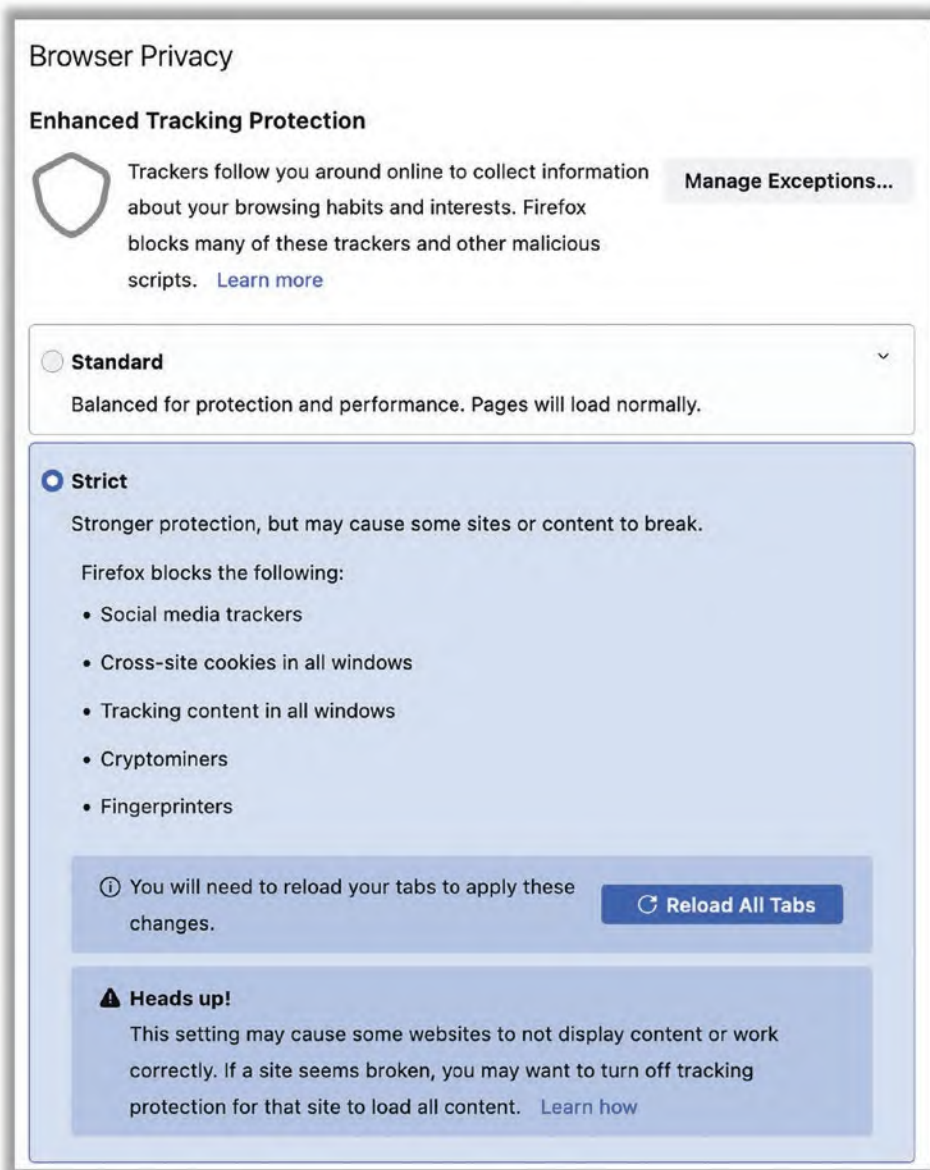


Figure 8-8. Firefox Enhanced Tracking Protection

- 3. If you do have a problem with a website, you can try disabling tracking protections for just that one site (and you can undo this change later). To do this, click the little shield icon next to the address at the top, and disable the Enhanced Tracking Protection (Figure 8-9). (You can also report the site as broken, which will help Firefox tweak these privacy tools.)

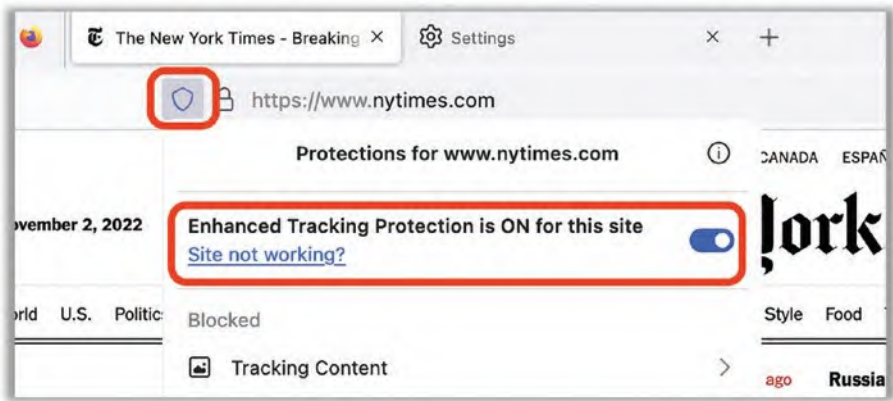


Figure 8-9. Firefox disable Enhanced Tracking Protection for a given site

- 4. I would always send the “Do Not Track” signal just to register your desire to be left alone but realize that this is mostly symbolic—most websites that want to track you will ignore this, sadly (Figure 8-10).

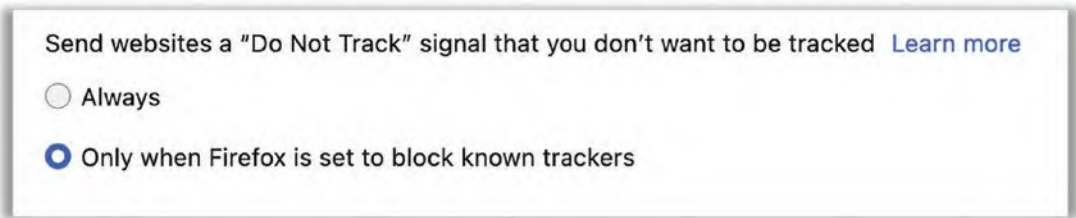


Figure 8-10. Firefox Do Not Track setting

5. There's a more modern version of Do Not Track that actually has some legal teeth called Global Privacy Control (GPC). Firefox supports it, but you have to get into some special hidden settings to enable it for some reason (as of this writing). If you're interested, see this site for instructions:
<https://blog.mozilla.org/netpolicy/2021/10/28/implementing-global-privacy-control/>
6. Note: We'll return to "Logins and Passwords" as well as "Forms and Autofill" when we install the BitWarden plug-in. You can leave this alone for now.
7. Under the "History" section, you can feel free to use whatever settings you're most comfortable with. To see all the choices, you have to select "Use custom settings" from the drop-down menu (Figure 8-11). To the best of my knowledge, Mozilla does nothing with this saved information. As a nice compromise, you can just ask Firefox to clear this history when you quit the app. You probably don't want to always use "private browsing mode," but only as needed.

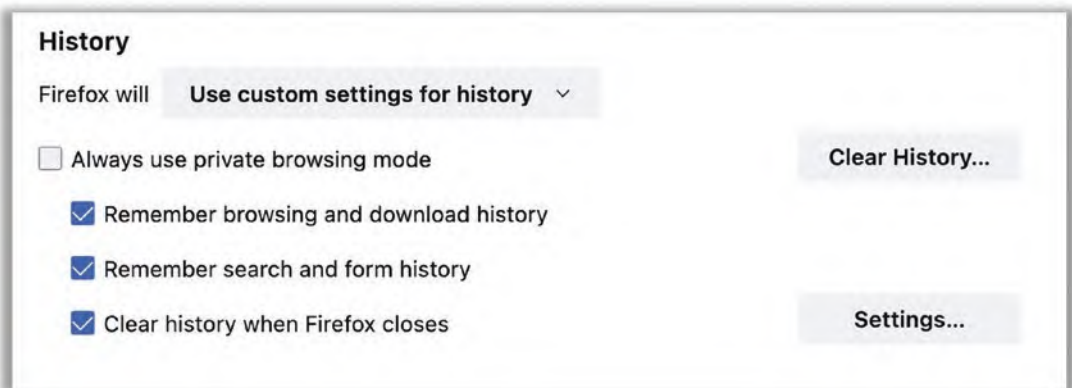


Figure 8-11. Firefox history settings

8. Firefox Suggest is mostly about suggesting stuff you’ve already searched for or tabs you may already have open, but there are a few add-ons that I would disable—all the “suggestions” at the bottom (Figure 8-12).

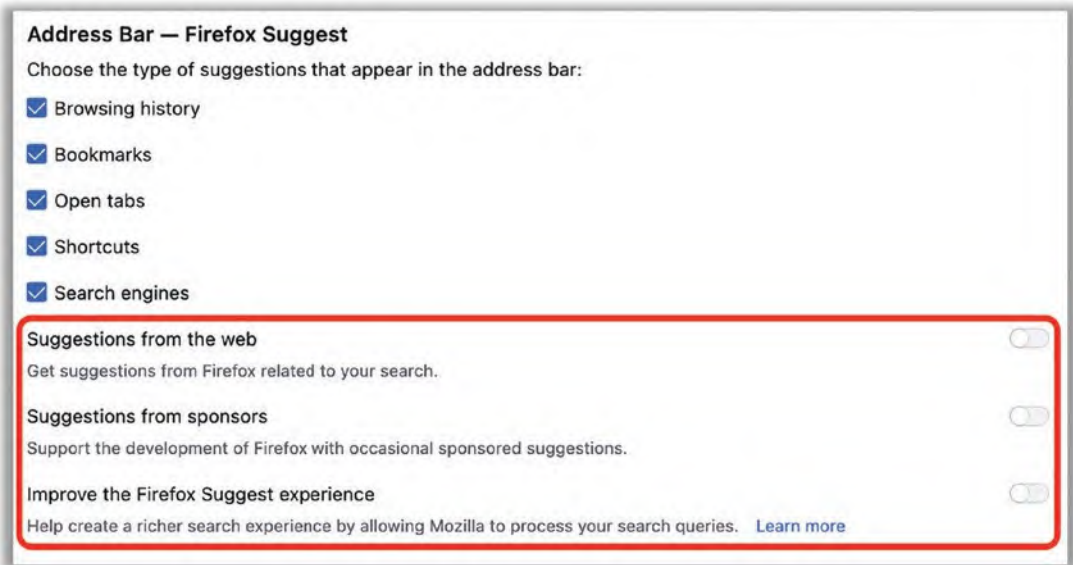


Figure 8-12. *Firefox Suggest*

9. Next, find Permissions (Figure 8-13). There are several settings here, and you should look at each of them individually. By far the safest thing is to block all requests to access your location, camera, and microphone. However, that will break some websites. Firefox will ask you for permission whenever a website requests access to these items, so you can leave these settings at the default. Just know that you can permanently deny or allow any site here. Below the Permissions settings, you should check both boxes. If you changed these settings, Firefox may require a restart.



Figure 8-13. *Firefox Permissions settings*

10. Find “Firefox Data Collection” (Figure 8-14). You can decide what you want here. For maximum privacy, you should share nothing. But for Mozilla to improve its products, it has a legitimate need for *some* user data. But maybe they can just get that from someone else.

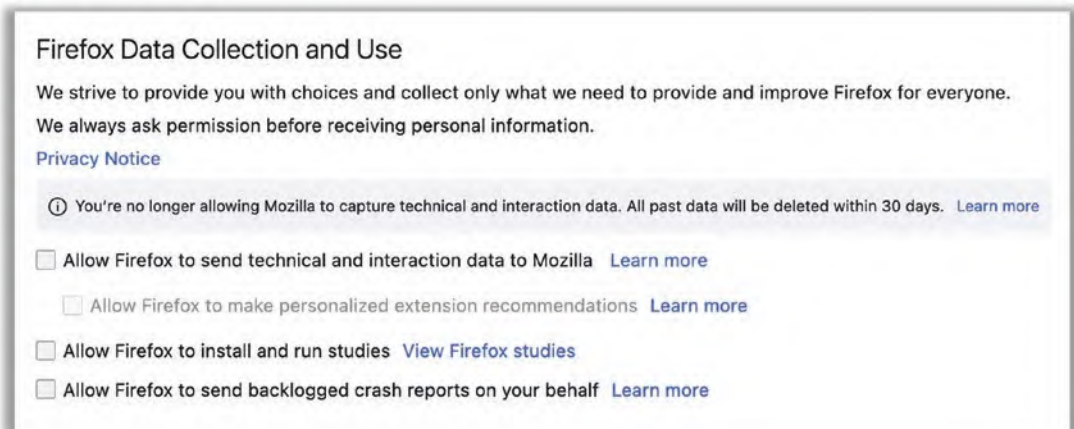


Figure 8-14. *Firefox Data Collection and Use settings*

11. Next, find the section “Deceptive Content and Dangerous Software Protection” under the “Security” section (Figure 8-15). I’m not sure how effective this is, but it’s worth a shot. I would check all the boxes.

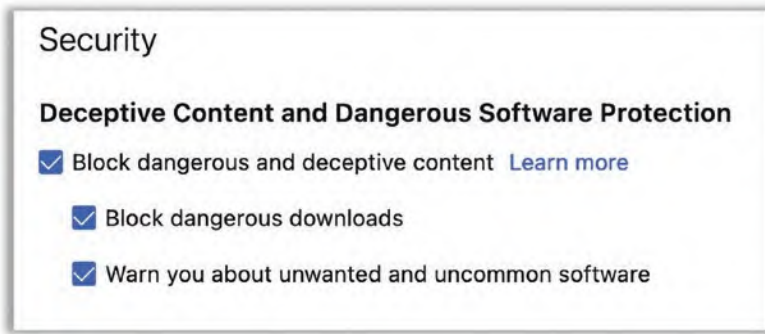


Figure 8-15. Firefox Security settings

12. Under “Certificates,” you should have it ask you every time and query OCSP servers. This is protection against bad certificates, which we discussed in the chapter (Figure 8-16).



Figure 8-16. Firefox Certificates settings

13. At the very bottom, you should enable HTTPS-Only mode (Figure 8-17). While most websites today have HTTPS available, some still allow you to use HTTP (insecure mode) if you ask for it—and some web links are old or wrong and don’t include that all-important “S.” This setting will always try to use HTTPS and warn you if it’s not available.

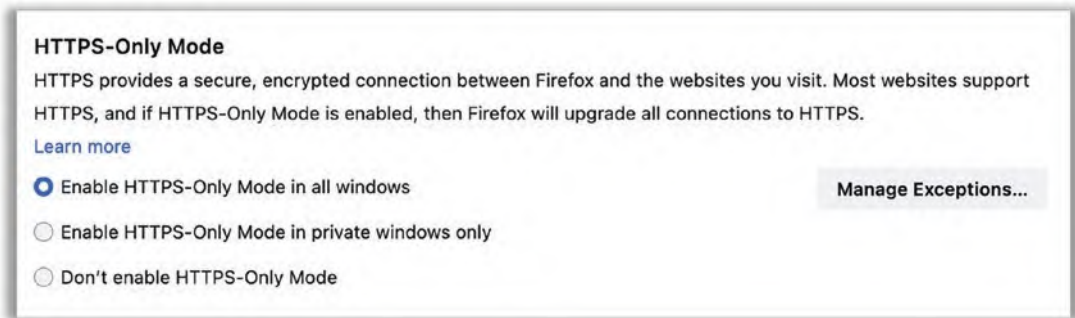


Figure 8-17. Firefox HTTPS-Only mode

14. Finally, go back to the “General” tab at the left of the Settings page. Check the box to have Firefox automatically install updates (Figure 8-18). This is all the way at the bottom. Note that updates will only install when you restart Firefox. You’ll see a little green dot on the “burger” menu if there’s an update available.

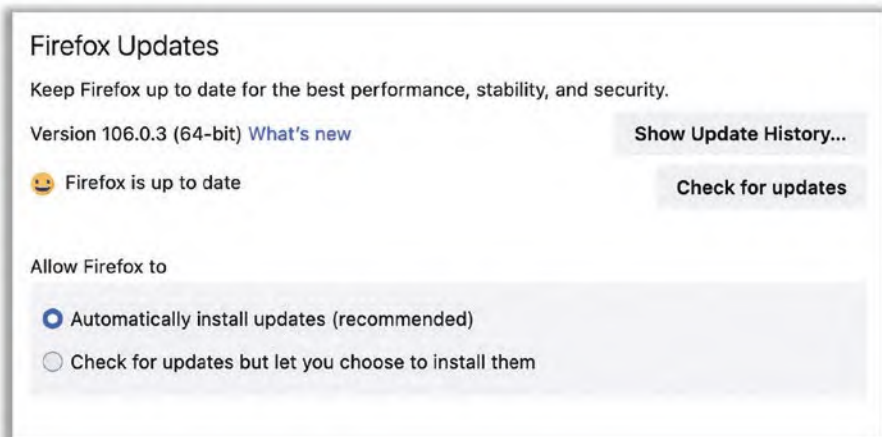


Figure 8-18. Firefox Update settings

Tip 8-3. ★ *Change the Default Search Engine*

Google’s search engine tracks you and everything you search for. Think about some of the things you might search for, and ask yourself if you would like that information saved and made available to someone else—that weird rash on your leg... how to fix a low credit score... where to find that special adult content.... If this idea bothers you, then you should change your default browser search engine to one that respects your privacy.

Unfortunately, to stay in business, Mozilla (maker of Firefox) has made a deal with the devil. Google pays Mozilla quite a bit of money to make Google the default search engine in Firefox. But you can change it easily. There are several good options. I would go with either DuckDuckGo or Brave Search. They’re not quite as good as Google, but they’re close enough and will not track you. Note that with both DuckDuckGo and Brave Search, if you’re not getting the results you want, you can add the text “!g” (exclamation mark and the letter g) to your search query, and it will return Google search results, minus some of the tracking.

To set DuckDuckGo as your default web browser search engine, you can just change the “Default Search Engine” setting. Go to the Firefox settings (as we did in the previous tip) and select “Search” at the left. Find the search options and select DuckDuckGo (Figure 8-19). You can change the search suggestions, if you wish. Basically, this will send the text you enter into the search/address area to the chosen search engine so that it can suggest possible searches (try to auto-complete your query).

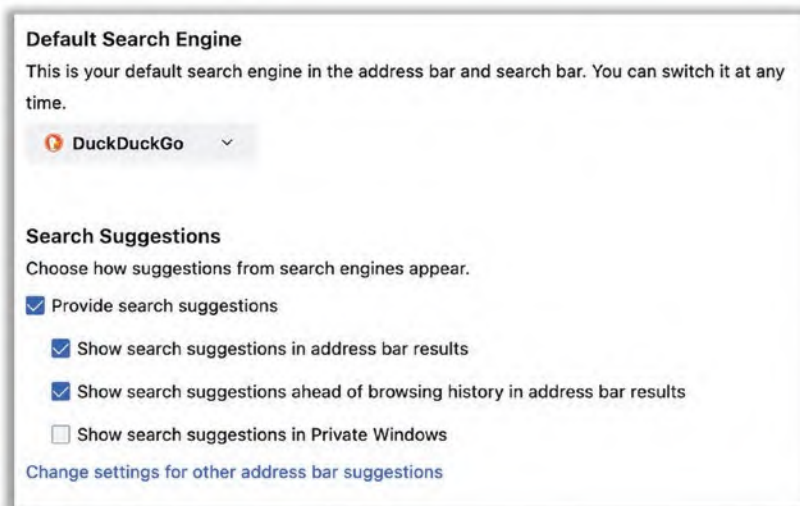


Figure 8-19. *Firefox Default Search Engine*

If you want to try Brave Search, you'll have to do a little more work (until and if Firefox decides to add Brave as a default option in Settings). In your address search bar, go to the following site:

<https://search.brave.com>

Then right click the address bar and select "Add Brave Search" (Figure 8-20). Then repeat the preceding steps to choose this as your default search engine.

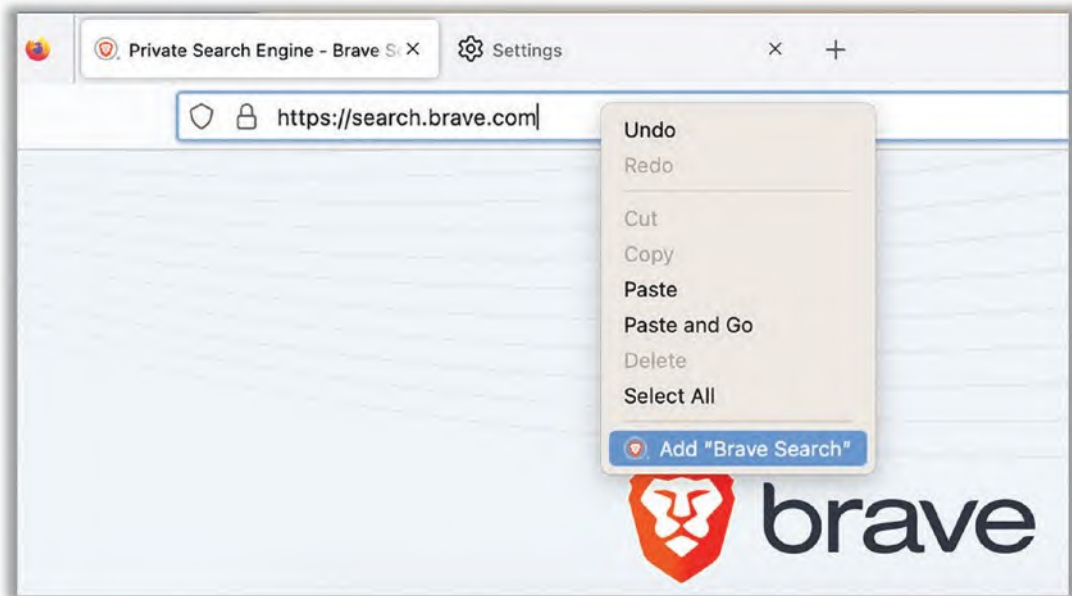


Figure 8-20. Firefox Add Brave Search engine

Tip 8-4. ★ Install Password Manager Add-on

You don't want to install any more add-ons in your web browser than are absolutely necessary. But the single most important add-on is for your password manager. This will allow you to generate, fill in, and save passwords on all web pages.

In this tip, we're going to install the BitWarden browser add-on on the Firefox browser and attempt to import any passwords you've already saved in another browser or in another password manager. We'll also disable the browser's built-in password manager function.

1. You need to open the “Add-ons and Themes” menu. You can get to this from the “burger” menu at the upper right (Figure 8-21). This shows the macOS version of Firefox, but Windows looks very similar.

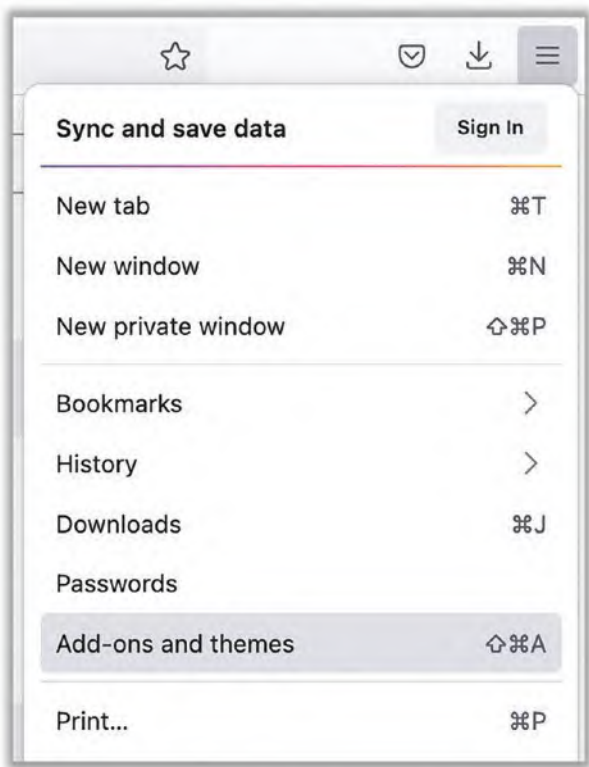


Figure 8-21. Firefox Add-ons and Themes menu

2. At the upper right, search for “bitwarden” (Figure 8-22).

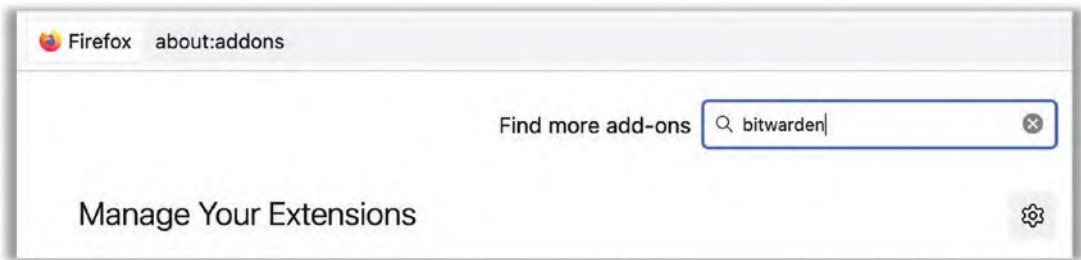


Figure 8-22. Firefox Add-ons search

3. You should see the official BitWarden add-on first in the list.
BE VERY CAREFUL to get the *official* one from BitWarden—it should be listed as “recommended” (Figure 8-23) with hundreds of thousands of users.

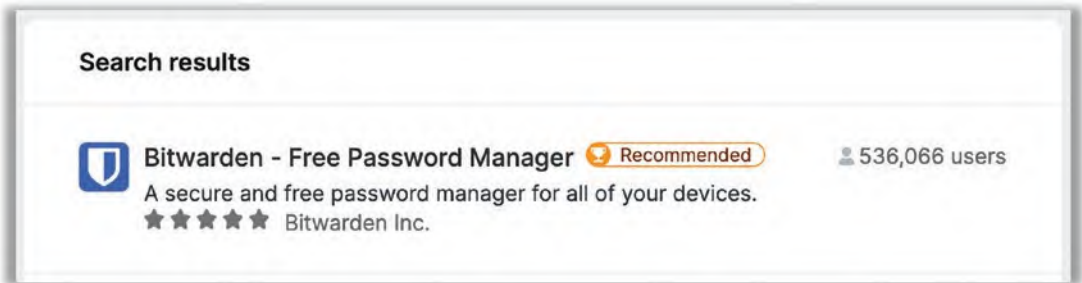


Figure 8-23. Firefox BitWarden password manager add-on

4. Click this search result and then click “Add to Firefox” button (Figure 8-24).

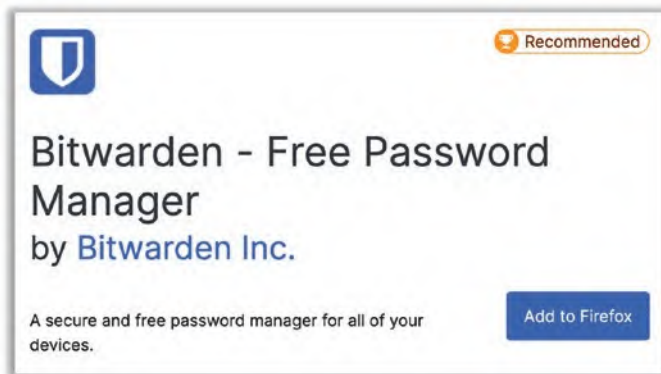


Figure 8-24. Firefox add to BitWarden password manager

5. This may trigger a permissions window (Figures 8-25). You can accept them all. If prompted, I would also check the box for “Allow this extension to run in Private Windows”.

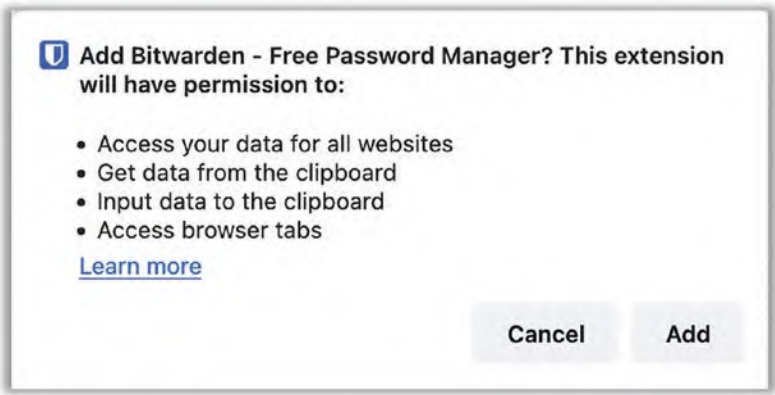


Figure 8-25. *Firefox BitWarden Permissions*

- 6. Once you’ve done all of this, you will need to log in to your BitWarden account. Click on the BitWarden icon (gray shield) at the upper right (Figure 8-26). Enter your email address and click “Continue”.

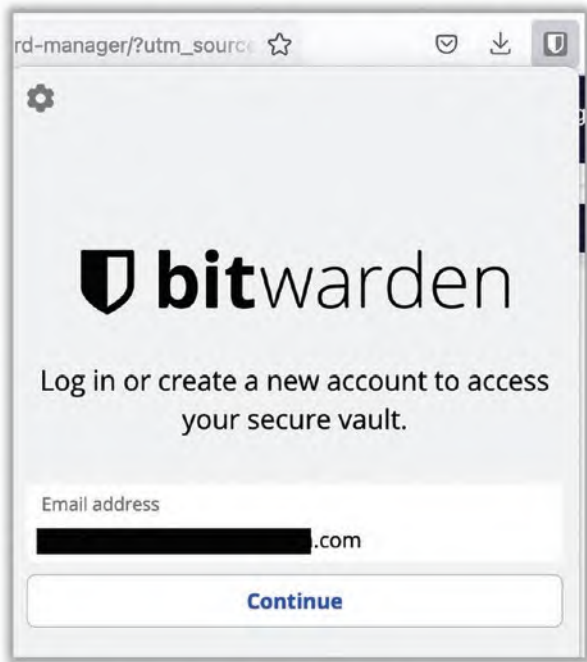


Figure 8-26. *Firefox BitWarden, Enter Email Address*

7. Now enter your master password (Figure 8-27) and click the “Log in” button. If prompted, enter your two-factor authentication code (you did set that up, right?).



Figure 8-27. Firefox BitWarden, Enter Master Password

8. Once you log in, you can import passwords from your old browser or even from a different password manager. For instructions, go to <https://bitwarden.com/help/import-data/> or go to the BitWarden settings, then “Tools” area and select “Import Items” (Figure 8-28) – which should take you to this same web page. There will be instructions there for importing passwords from all popular browsers and password managers.

NOTE If you export your passwords to a file, be sure to give this file an innocuous name (not “passwords” or “secrets”) and then delete it *immediately* after you import this data into BitWarden. This file contains all your passwords and secure notes, but it is *not encrypted*! You don’t want to sync this file to the cloud or back it up or leave it lying around.

If you don’t import your passwords, you can just fill your vault incrementally as you log in to your accounts. BitWarden will pop up a window offering to save them in your vault.

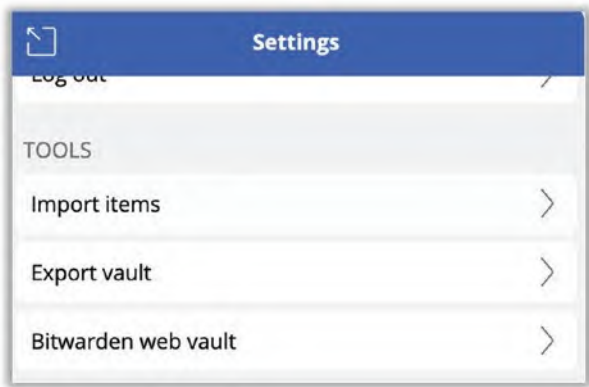


Figure 8-28. Firefox BitWarden Settings, Tools, Import Items

- 9. The last thing you need to do is disable Firefox’s built-in password and form filler functions. You can and should do all of these things using BitWarden instead. Go back to the Firefox Settings, and under Privacy & Security, find Logins and Passwords and Forms and Autofill (Figure 8-29). I would disable all of these, but definitely the logins and passwords.

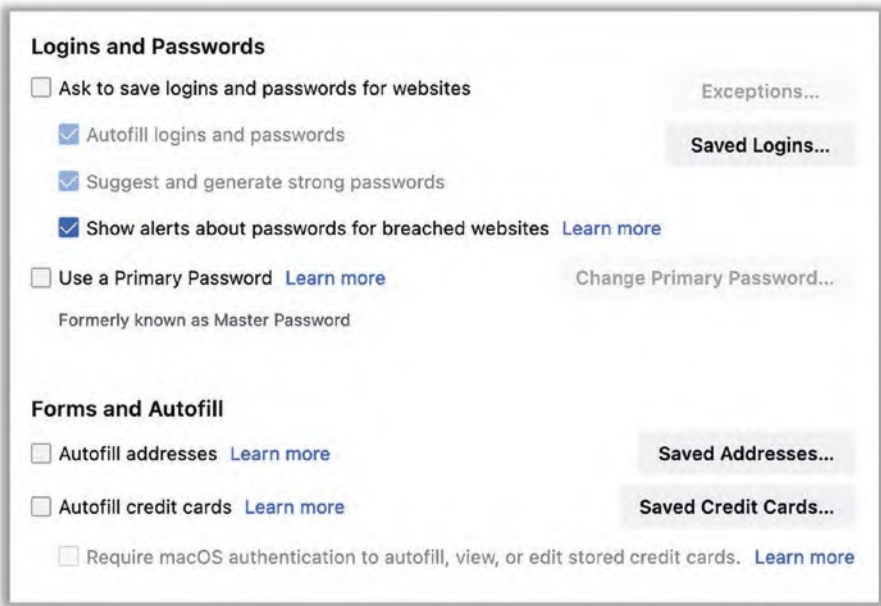


Figure 8-29. Firefox Disable Logins, Passwords, Forms, and Autofill

Tip 8-5. ★ Install uBlock Origin Add-on

There are several privacy add-ons you could add to Firefox, but honestly you only need one: uBlock Origin. This add-on will prevent websites from loading annoying ads and dropping tracking cookies. In fact, it can significantly increase page-loading speed by avoiding lots of stuff you don't need.

I won't show you all the steps for installing this add-on. It works just like the BitWarden add-on we installed previously. Just search for "uBlock Origin" this¹².

Note The nature of this plug-in is to block or restrict unwanted content. This can sometimes break websites that haven't been properly designed for the possibility that people might not want annoying ads, tracking cookies, and so on. If you find a website that is not working properly or somehow acting funny, you might try temporarily disabling uBlock Origin. Or you could also try using a different browser for this particular site, like the built-in browser provided by macOS (Safari) or Windows (Edge).

To disable uBlock Origin for a website, click its icon in Firefox at the upper right and then click the big blue "power" button, and then click the reload button that appears next to it. You can see an example in Figure 8-30. You can see, by the way, that the default Google Search website has several trackers—you can see the number on the uBlock Origin icon at any time. That should be a reminder of what's really going on when you visit some of these sites.

¹² Note: There exists a knockoff called simply "uBlock" —you do NOT want that. You want *uBlock Origin*.

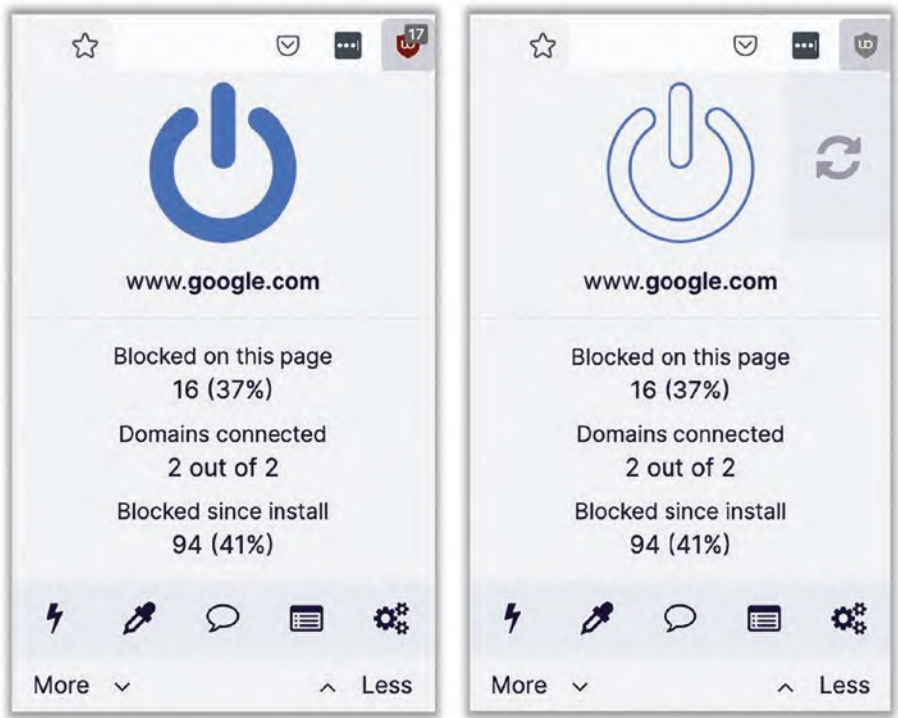


Figure 8-30. Firefox uBlock Origin menu enabled (left) and disabled (right)

This plug-in has all sorts of wonderful features and tools. See this site for more information about uBlock Origin, other plug-ins, and other Firefox privacy settings you can try:

<https://github.com/arkenfox/user.js/wiki/4.1-Extensions>

Tip 8-6. Remove All Unnecessary Add-ons

Web browsers have become very flexible, allowing you to add all sorts of fun and useful features via plug-ins, add-ons, and extensions. Unfortunately, these extras, many of which are free or get installed with other software, can open security holes and seriously invade your privacy. Avoid them unless you *really* need them. If you just installed Firefox, then you probably have no extra stuff installed; otherwise, read on.

If you have any trouble removing an add-on, try searching for “remove <add-on name>” in your web browser. Some of these add-ons are tenacious and hard to remove (and these are the ones you most assuredly need to remove).

Note that disabling an add-on may still allow it to have access to your data. But if you’re uneasy about deleting it, you can start by disabling it to see how Firefox works without it. If you have no problems, you can go back and delete it. (Of course, you can always just reinstall it, too, if you change your mind later.)

1. To disable an unwanted add-on in Firefox, first open the Add-ons menu, as we did before in Tip 8-4. Find the add-on you want to disable, and toggle the slider next to it (Figure 8-31).

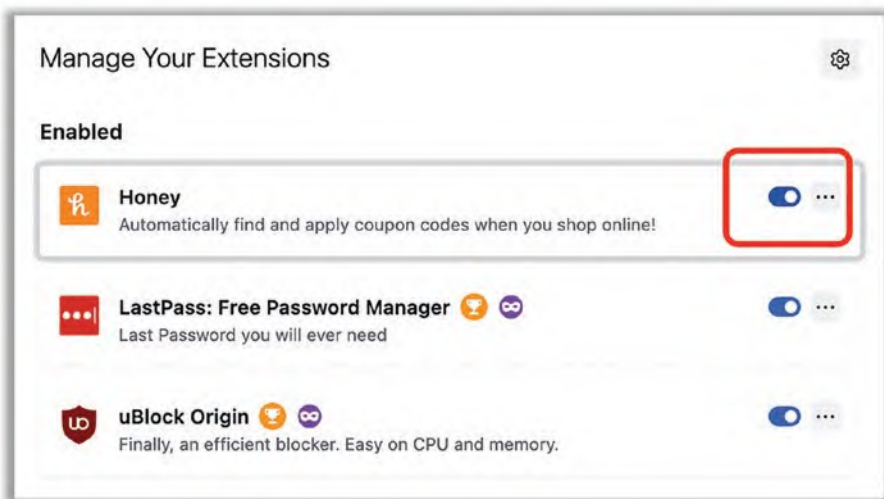


Figure 8-31. Firefox disable add-on

2. To completely remove an add-on, click the little ellipsis menu and select “Remove” (Figure 8-32). You may need to restart your browser to complete this. If you have multiple add-ons to remove, you can remove them all and then just restart the browser once.

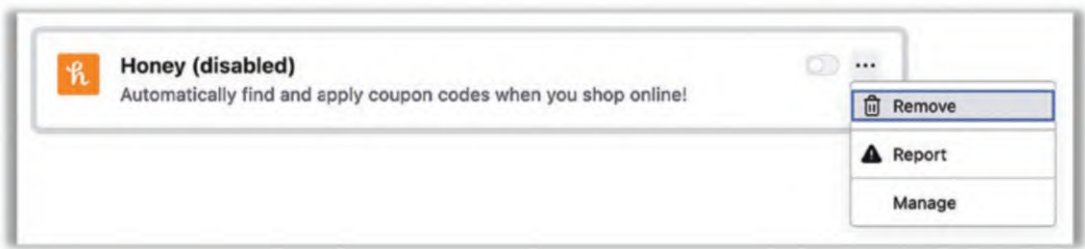


Figure 8-32. Firefox remove add-on

Tip 8-7. Be Careful on “Shady” Sites

Some websites are just way worse than others when it comes to malware, and those sites tend to be associated with what some would call vices... porn, gambling, copyrighted movie and music downloading, and so on. I’m not here to judge. Just know that these sorts of sites tend to be worse than others, and the ones that are “free” are ones I’d worry about the most.

Tip 8-8. Beware of Pop-Ups Offering/Requiring Plug-ins

Some websites will ask/offer to install some malware checker or speed booster or video player or required plug-in. If you get a pop-up window that wants to install something, close the window and walk away. If it’s a plug-in that you really think you need, you should go directly to the relevant website to download and install it. Then return to the original website and see if it works. The rule is: *if you didn’t go looking for something or request it yourself, don’t install it.*

Some of these website pop-ups will actually tell you that you’re already infected with malware or that your computer is having problems. They may sound dire and urgent, but don’t be fooled. They’re just playing on your fears. They’re almost surely scams or malware.

Tip 8-9. Use Private Browsing

Firefox has a special “private browsing” mode that is supposed to remove all local traces of your web surfing once you close the special window. This includes your browsing history, cookies, and anything else the browser might remember about your session.

The key word here is *local*. While it may successfully block your info from being stored permanently, it doesn't make you anonymous or stealthy on the Web. Its sole purpose is to hide what you've been doing from people who have access to your computer (your kids, your spouse, etc.). This may have situational benefits for you, but just be aware that the only privacy here is on your computer.

You can use this feature to log in to a website as someone else (different account) without screwing up a session you already have active or maybe to see what a website looks like without being logged in.

To open a private browsing window, just go to the Firefox “burger” menu and open a new Private Window (Figure 8-33). Everything you do in this window (all the tabs) will be forgotten without a trace once you close the private window. You can tell you're in the private window by looking at the upper-right corner of the browser window—it will say “Private browsing.”

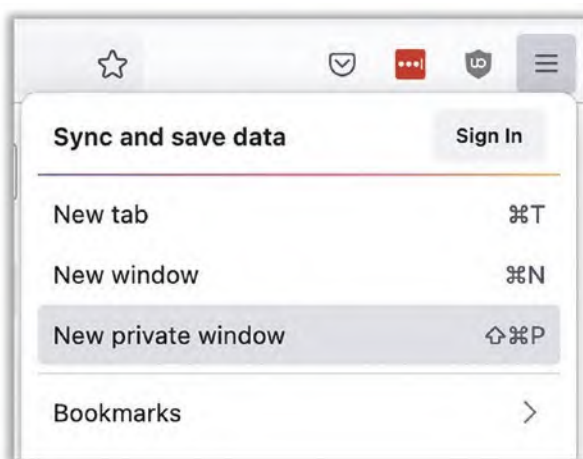


Figure 8-33. Firefox open new private window

Tip 8-10. Delete Personal Info from Google Searches

Thanks to privacy legislation from California and the European Union, Google has been forced or at least prodded into providing tools to help you remove your personal information from their databases. We'll talk more about this in Chapter 10. But this being the web surfing chapter, I figured this was a better place to tell you about Google's “Results about you” tool. If you're being stalked or if some of your personal information

has been showing up in Google Searches, you can ask Google to hide it. Note that this will not remove the information from the sites that the search engine pulled it from. But in a very real sense, if you can't find something with Google Search, it doesn't exist for a lot of people.

Check out this article for more information and instructions on using the tool:

<https://support.google.com/websearch/troubleshooter/3111061>

If this link fails, try searching the Web for “Remove your personal information from Google” or “Google Results About You tool.”

Tip 8-11. Be Careful When Entering Form Data

You might believe that any information you start typing into a web form will only be sent to the website when you click the “Enter” or “Submit” button. However, it's trivial for websites to save this data as soon as you type it—that includes autofilled information. Be aware of this as you're filling in web forms.

Additionally, if you have enhanced spell checking turned on in the Chrome or Edge browsers, anything you type in a form field will be sent to Google or Microsoft's servers for checking, as you type it. This would include sensitive information like credit card numbers, government IDs, and passwords, if revealed.

Tip 8-12. Use a Privacy-Respecting DNS Provider

Remember that DNS is the Internet's “phone book”: it will convert a name (like amazon.com) to a number (an IP address). Today, most DNS lookups are not encrypted, meaning that your DNS provider—and any computers along the way—can see every website you go to as your computer does this name-to-IP-address lookup behind the scenes. By default, your DNS provider is almost certainly set to be your Internet service provider—who is almost certainly recording all your requests and using it to gather information about you. Unfortunately, switching to a privacy-respecting DNS provider, even with encrypted DNS queries, won't really protect you from prying eyes. All web traffic is routed via IP addresses, and your ISP necessarily sees the “to” address on every packet your computers and devices send through it. And just as DNS can be used to convert names to numbers, you can reverse that same lookup to convert numbers back to names.

The only way to really hide this information is to use a VPN, but VPNs are a pain to use 100 percent of the time. So, it's still not a horrible idea to at least try to use a privacy-respecting DNS provider by default. The other advantage to using some of the DNS resolvers I'm going to mention here is that they can also help to protect you from going to malicious websites and block a lot of web tracking.

So, given that, I'm going to recommend three possible options for you to consider. To use one of these DNS resolvers, you'll need to update your "DNS server" settings to use the values in Table 8-1. There are two entries per cell – a primary and backup server.

Table 8-1. *Privacy-Respecting DNS Resolver IP Addresses*

Service	IPv4	IPv6
Cloudflare (no filter)	1.1.1.1	2606:4700:4700::1111
	1.0.0.1	2606:4700:4700::1001
Cloudflare (no malware)	1.1.1.2	2606:4700:4700::1112
	1.0.0.2	2606:4700:4700::1002
Cloudflare (no malware, no adult content)	1.1.1.3	2606:4700:4700::1113
	1.0.0.3	2606:4700:4700::1003
Quad9	9.9.9.9	2620:fe::fe
	149.112.112.112	2620:fe::9
NextDNS	(* see note)	(* see note)

**Note: NextDNS's servers vary depending on your account and location. When you sign up, they will give you your personal server addresses.*

There are two primary places you can change your DNS servers: on the device itself (computer or smartphone) or at your home router. I would personally prefer to make the change at the router because it will then be used by every device in your house automatically (unless a given device has overridden the DNS server setting). But for mobile devices, you'll want to change the DNS settings there, too, so you can use them when outside your home network.

All three of these services have extensive instructions on how to make these changes. In some cases, you can even download a simple profile that can make all of these changes for you. So, instead of trying to explain all of that here for each service, I will just refer you to their documentation:

- Cloudflare: <https://developers.cloudflare.com/1.1.1.1/setup/>
- Quad9: <https://quad9.net/support/set-up-guides>
- NextDNS: <https://nextdns.io/>

Tip 8-13. Use DNS over HTTPS (DoH)

To make your DNS queries (more) private, you should encrypt them. Again, as I said in the previous tip, this doesn't completely hide your traffic—for that, you need a VPN. But you can still encrypt your DNS queries for added privacy. It's easy to do and there's no downside that I'm aware of.

There are a couple ways to do this, but the easiest and most popular one is to just send the DNS queries over HTTPS—the secure protocol we already use for our web surfing. As it happens, Firefox already has this capability built into the browser. You can change these settings by opening the Firefox Settings window and searching on “DNS” (Figure 8-34). Click the “Settings” button.



Figure 8-34. Firefox settings search for DNS

At the bottom of the DNS Settings window, just make sure that “Enable DNS over HTTPS” is selected (Figure 8-35). You can choose Cloudflare or NextDNS, currently. If you go with NextDNS, see your account information for a special configuration parameter you’ll need here.



Figure 8-35. *Firefox DNS over HTTPS setting*

Windows and macOS have built support for DNS over HTTPS, as well. You can look for these settings under the usual network configuration settings. However, if your home Wi-Fi router supports DNS over HTTPS, enabling it there will cover all the devices in your home.

Note that if you change this setting in Firefox, it will override whatever your router and computer settings are for the sites you visit in Firefox. All other network traffic on your computer and other web browsers you might have installed will use the computer or router DNS settings.

CHAPTER 9

Coded Messages and Wax Seals

Web surfing is all fine and good, but it's mostly a solo activity. When we need to communicate with others, we turn to other methods like text messaging, email, and video chat (or perhaps something like Figure 9-1). In this chapter, I'll help you understand how these communication mechanisms work and how best to keep them secure and private, like a king might encode his messages on parchment and enclose them with a wax seal using his signet ring.

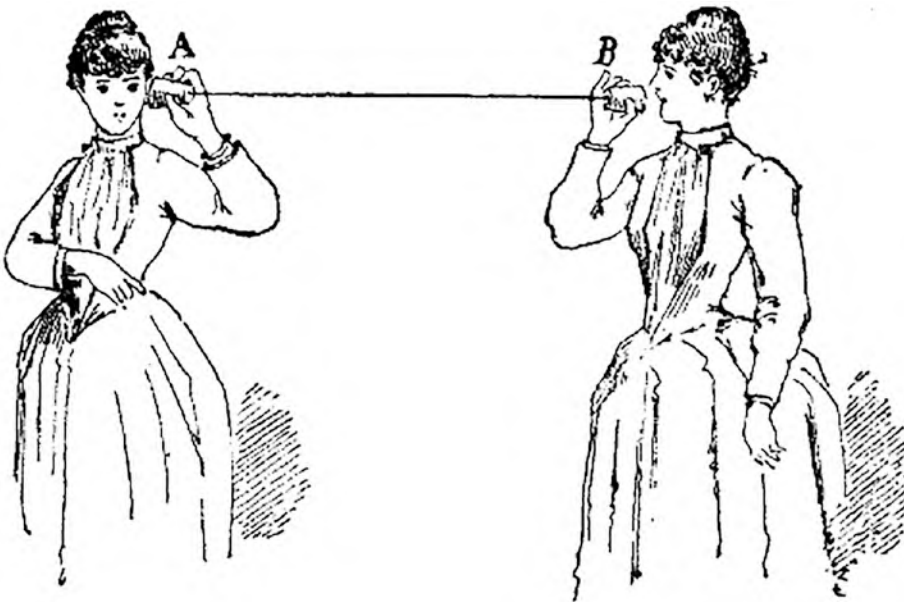


Figure 9-1. *Vintage communications technology*

Email

When you visit a website with your web browser, you are creating a connection between your computer and a distant server such as your bank, an online retailer, someone hosting cat videos, or whatever. If this connection is encrypted (and today, most are), then you can be sure that no one else will be able to see the content you’re consuming—though without a VPN, your ISP will still be able to see all the metadata like what sites you visit, how long you stay there, how much data is transmitting, and so on.

With email, however, the complexity and opportunity for eavesdropping increase quite a bit. To send an email message, you first send the message to your email provider, and then your provider attempts to send the message to the recipient. If Alice wants to email Bob, and they both use Google’s Gmail service, then the email path will look something like Figure 9-2. This mechanism allows the service to *store and forward* the message. If the recipient is not immediately available (i.e., “online”), then the message can be saved in the cloud for future transmission. Even if the recipient is currently available, the nature of the email system is to keep a copy of the message on the server until the user explicitly deletes it.

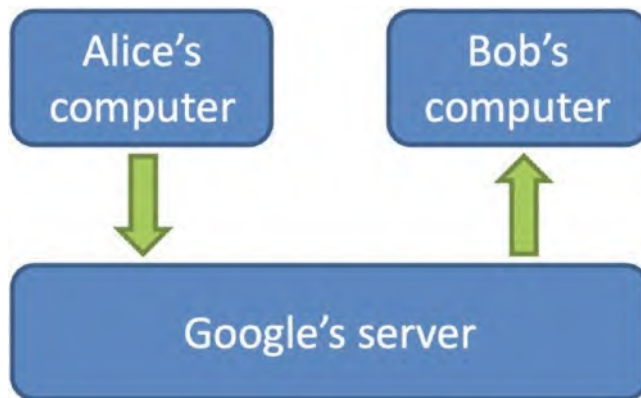


Figure 9-2. *Email communication within a single service*

Note, however, that the recipient may use an entirely different email service than the sender. For example, if `alice@gmail.com` sends an email to `bob@yahoo.com`, then both Google and Yahoo will have copies of that message on their servers—one copy for Alice and another for Bob (see Figure 9-3). If Alice deletes her copy, Bob may still have his copy, or vice versa. (Of course, even if both Alice and Bob delete their copies of this message, Google and Yahoo may well keep copies on the server for some period of time.)

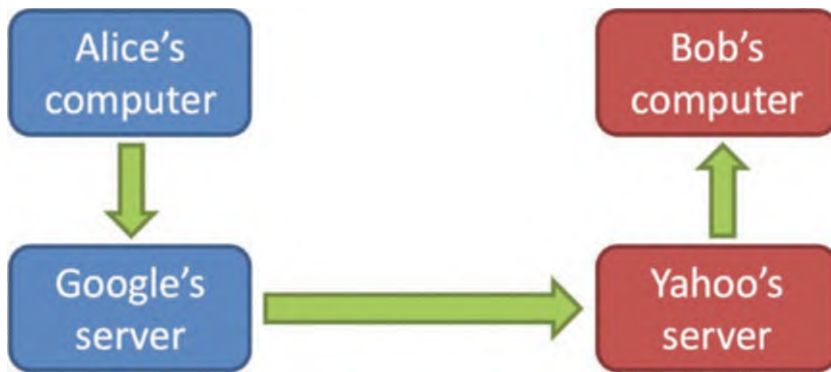


Figure 9-3. *Email communication between two services*

When we talked about encryption used for surfing the Web, all of the communications were point to point and short-lived. With email, the message is often encrypted only in transit (the arrows in the diagram). The message content itself is rarely encrypted, meaning that anyone with access to the computers or servers that transmit or store the message could read the message. Emails are really more like postcards than letters sealed in envelopes. Also, while the connection between Alice and Google's email server may be encrypted, she has no way to know or control whether the link between Google's server and Yahoo's server is encrypted or whether the link between Yahoo's server and Bob's computer is encrypted. In fact, until Snowden's revelations, many of these server-to-server links were unencrypted, allowing spies and law enforcement to intercept them.

So, what can we do about this? The best answer is to encrypt the email message itself, before it ever leaves Alice's computer. Bob would then decrypt it when it arrives, and no one in between would be able to see the contents. Unfortunately, encrypting email messages is not easy for the average person to do, particularly across different email providers.

For many years, the go-to tool for encrypting emails was PGP, which stands for Pretty Good Privacy. PGP is actually *excellent* privacy—the inventor, Phil Zimmermann, was being characteristically humble. PGP was revolutionary at the time it was invented in 1991. The US government was trying to restrict the use of strong encryption, attempting to keep consumer-grade encryption weak enough that their supercomputers could break it. The US government went so far as to label encryption software a “munition” for the purposes of export regulations. Phil created and released PGP because he believed that people had the right to private communications and specifically wanted to help political

activists all around the world. He nearly got thrown in jail for this. The history is truly fascinating. I've had the pleasure of interviewing Phil several times on my podcast (see *Going Further* at the end of this chapter), including for the 30th anniversary of PGP.

But even Phil will tell you that PGP is not the best email encryption solution today, though many people still use it (including me, on occasion). While the technology is still solid, there are better ways to encrypt email now (which I'll explain in the checklist).

Text Messaging

Short message service (SMS, aka texting) came around with the advent of mobile phones. It's still the lowest common denominator today for mobile messaging—all cell phones and cellular service providers around the world support this technology. Texting is similar to sending an email. It supports the store-and-forward function, meaning that your intended recipient doesn't need to be online to get your message. You can send it whenever you want, and whenever they turn on their phone, the message will be delivered. Also, the phone companies have managed to work out the technical stuff to allow someone on Verizon to send text messages to someone using AT&T or T-Mobile or any other carrier. Apple has even integrated SMS with its messaging system (Messages, formerly iMessage). You can use Apple's proprietary system if all parties are using an Apple product (in which case the messages are in a blue bubble) or fall back to regular SMS messaging otherwise (where message bubbles will be green).

Instant messaging (IM) has been around for about as long as email, believe it or not. They both date back to the early 1960s. You might remember services like AOL Instant Messenger, Jabber, and Yahoo Messenger. But no one uses IM anymore—it's been replaced by mobile-oriented messenger apps like WhatsApp, Facebook Messenger, Telegram, WeChat, Discord, and so on. To chat with others, all users must have the same app installed. Unlike older instant messaging, most modern messenger apps will allow messages to be stored and forwarded if the intended recipient isn't currently online.

Like email, text messages themselves are not usually encrypted from end-to-end but instead are only encrypted in transit. They are often readable by the service you use to send the message, for example. In the checklist, I'll tell you about some truly private messaging services.

Google is moving away from SMS and adopting a newer, fancier messaging standard called *Rich Communications Services* (RCS). Communication standards groups have been working on this for a long time, recognizing that SMS is old and clunky. It works across any type of phone or computer, similar to SMS. It supports all the fun new features like read receipts, “typing” indicators, group chats, videos, emojis, and so on. Google announced support for RCS on its Android devices in 2019, and several cellular providers have begun to support it.

Apple, however, has shown no desire to adopt RCS. Therefore, SMS is still the lowest common denominator for mobile text messaging, and it will probably remain so for years to come. Also, RCS lacks one crucial feature that I can’t believe they left out: end-to-end encryption. So, my guess is that RCS will become standard for Android devices, and Messages will remain the standard for Apple devices, with both devices supporting SMS for cross-platform communication.

Spam and Spoofed Messages

Junk emails and messages—often unsolicited advertisements—are referred to generally as *spam*¹. Many of our most used messaging platforms are open by default. That is, if you know someone’s email address or cell number, you can send them a message—no permission required. Some messaging systems have implemented a check mechanism whereby you have to first allow the other person to “follow” or “friend” you before they can send you a message; however, this support isn’t ubiquitous.

If you’re lucky, the spammers will only send you advertisements. However, spam is also a favored mechanism for both malware delivery and phishing attempts. The missive will contain links to fake websites or come with attachments embedded with malicious code.

It’s important to realize that it’s almost trivial for the identity of the sender to be spoofed. That is, just because the “from” on the email or text message is someone or some company you know and trust, you can’t assume that it’s really coming from them. Also, email accounts are often hacked, so even if a message truly is from who it says it’s from, you still have to be very wary of any links or attachments given to you. While antivirus and other safety utilities do an okay job of blocking these things, you can’t assume that they are 100 percent effective.

¹ Believe it or not, this term originates from the Monty Python spam skit featuring Vikings in a greasy spoon diner.

Looks Can Be Deceiving

You also need to realize that you can't trust the text of a link. Just because the link says <http://google.com> doesn't mean that that's really what the link is pointing to. Sometimes if you hover your mouse pointer over the link, your browser or email app will show you the actual link. In fact, if you're reading the eBook copy of this book on your computer and you hover over that link, you'll see that it's actually fake (Figure 9-4).



Figure 9-4. *Misleading web links in text*

Sometimes the bad guys will try to trick you with websites that are slightly misspelled, often in a way that is hard to catch like outlook.com or tvtwitter.com. Did you catch the differences there? It may depend on the particular font you're seeing, which may be different on an eReader than the font in the paper book.

But here's a really tricky way to fool people that is effectively impossible to spot with the naked eye. There's a web technology called Punycode that allows for encoding characters from different alphabets, such as Cyrillic or Greek. But some of these non-Latin characters look just like their Latin counterparts. Bad guys can register web domain names using these other characters, and you won't be able to tell the difference no matter how closely you look. Check the example in Figure 9-5.



Figure 9-5. *Example of Punycode misleading web address*

The top value is what you would normally see, but the unencoded version (the actual website address) is what you see at the bottom. The web browser is just rendering that text using the special characters, so it looks more natural. While this appears to be the Latin alphabet characters a-p-p-l-e, the web address here is actually using characters from the Cyrillic alphabet that happen to look *just like* a-p-p-l-e in the font used by Chrome and Firefox browsers.

Thankfully, web browser password manager plug-ins like BitWarden will not be fooled by either of these tricks. If you go to a website that should be familiar but BitWarden isn't offering to fill in your username and password, then you might not be looking at the website you think you are.

Redirecting Links and Tracking Pixels

Many web links today just immediately redirect you to another website, so you can't be certain that what you see is what you'll get. There are link-shortening services like Bitly (bit.ly) and Owly (ow.ly) that will take long, obnoxious web addresses and shorten them to something much easier to type and/or remember. These services perform a redirect from the shortened link to the real destination. So, for many reasons, you simply cannot judge a link by its text.

Finally, some images that come in emails can be used to track your movements on the Web and will also help spammers to mark you as a viable target. This is why many email clients won't load the images contained in an email until you say it's okay. For example, a spammer may get a list of a million email addresses from someone who hacked into some customer databases. The spammer has no way of knowing whether all of these addresses are still active. They will also not know if a particular email was able to get through all the various spam filters that are between them and the recipient. But if they put an image in that email with a unique identifier and your email client loads that image from the bad guy's server, then they will immediately know that the email address works and that it got through to you... in which case you should expect to receive more junk mail. Legitimate marketers use this technique, too. It's usually in the form of a tiny image called a tracking pixel. This image is often literally one pixel tall by one pixel wide—too small to see, in most cases. The images may also be transparent making them effectively invisible. Their only purpose is to tattle on you.

Dealing with Spam

Many solutions have been proposed for stopping spam, but because the Internet is so driven by marketing and advertising, the key players have strongly resisted their adoption. It comes down to this: who gets to determine what's junk? We've had the same struggle with regular junk mail delivered by the postal service. The postal office makes a lot of money delivering those ad flyers to you. However, the risks of malware I believe will eventually drive the industry to offer some sort of solution.

One option would be to charge a small amount of money to transmit more than, say, 100 emails in a 1-hour period or maybe 500 per day—something that would not affect most people but would cause spammers some grief. Right now, email is essentially free, which leaves it open for abuse. The problem here is that this could hurt small, legitimate businesses and still allow massive, wealthy corporations to continue sending gobs of unwanted emails.

There are several technical solutions² that have been proposed to this problem. They are extensions to the existing email protocols that allow for authenticating email senders. But this doesn't stop spam; it just makes it harder for the sender to spoof their identity. For various reasons, these technical solutions have yet to be adopted widely.

The most draconian option would probably be moving to a whitelist system where you cannot send email to someone unless they first approve you as a sender. This could be automated to a certain degree. When you first email someone, you will get a canned response from the service provider saying something like "I only accept email from people I know. Please contact me by some other mechanism first or answer these few questions to prove you know me." Spammers deal with millions of emails, so they wouldn't have time to bother with this. This would still allow legitimate companies with which you have some relationship to contact you. The process of registering on their website could automatically add them to your whitelist of approved senders, for example. My gut tells me that this is where we'll end up, unless we come up with a completely new scheme for sending electronic messages.

² If you're really interested, you can read about them. Search for DKIM, SPF, or DMARC.

Until then, we have limited methods of dealing with junk messages. We'll cover those in the checklist.

How to Recognize a Fake Email

You should learn to recognize the hallmarks of a fake email. These are used in phishing scams to trick you into giving up sensitive information like social security numbers, account information, or login credentials. Sometimes they will try to get you to open an infected document, like a fake invoice or bank statement. These scams will very often play on your emotions to get you to bite: fear, anxiety, and even charity. Common ploys include the following:

- Problems with your account or your computer
- Fake invoices or shipping notices
- Fraudulent government agency warnings (e.g., IRS, Social Security Administration)
- Winning a contest you never entered
- Extortion emails claiming to know embarrassing things about you

It might be easier if we look at an example. Figure 9-6 shows an actual email that I received, purporting to be from Apple. This one email has at least six things wrong with it, all of which are common facets to a phishing scam. I've numbered them nicely for you, and I'll walk through them one by one. But before I do, take a shot at doing this yourself first. Review each of those numbered items, and see if you can figure out what's wrong before I tell you. Go ahead; give it a shot. Then continue reading.

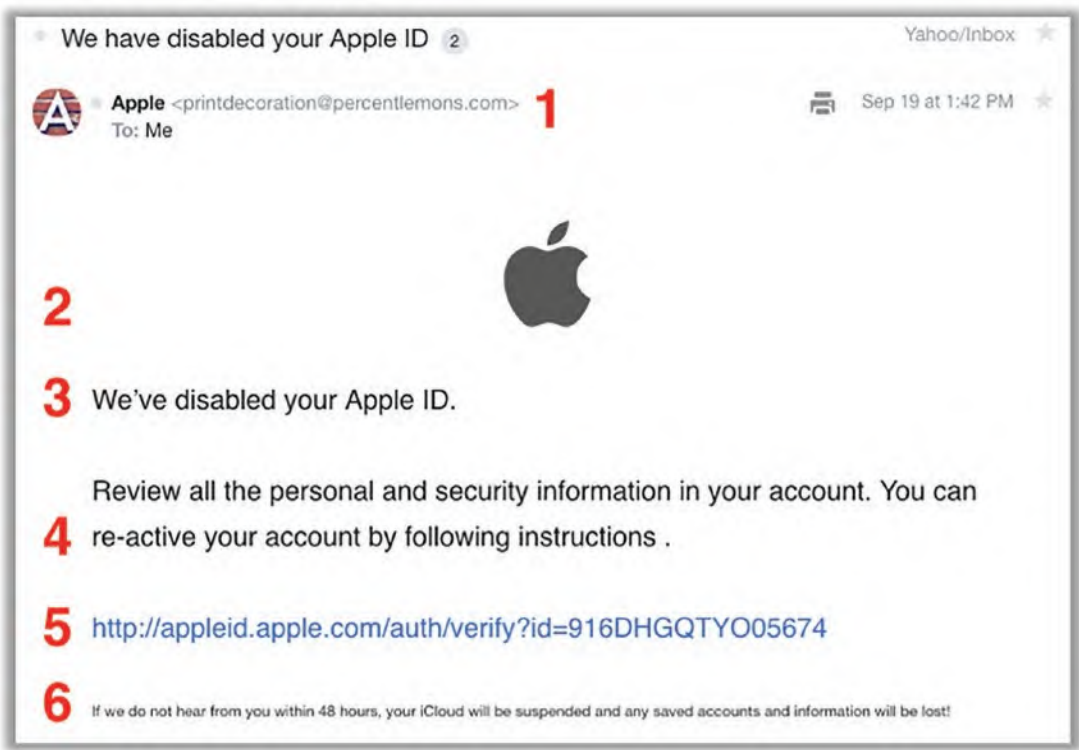


Figure 9-6. Fake email from Apple

Here are all the things that are “phishy” with this email:

1. The name of the sender says “Apple,” but the actual email address for the sender is “printdecoration@percentlemons.com.” They’re not even trying here. It’s not hard to buy a domain name like “appleidproblem.com” or “apple.something.com.” They could even just fake the sender to be “apple.com.” The “reply-to” address doesn’t matter here. The point of this email is to get you to click that link at the bottom.
2. They didn’t address me by name. Apple knows my full name, and any email I get from Apple would use my name in the salutation of the email body.
3. Here’s the scare tactic. Oh no! My Apple account has been disabled! What did I do? How do I fix this? Phishing emails try to scare you and instill a sense of urgency. Don’t think; just act—now!

By the way, in this case, all you need to do is go log in to your Apple iCloud account to verify that this email is completely bogus—if you can still log in, then your account hasn’t been disabled. (Obviously, you would not use the provided link to do this.)

4. The last line of this email has two errors. First, it says “you can re-active your account,” which is bad grammar. Second, there’s a space before the final period. An important email like this from a company like Apple would not have these mistakes.
5. This link appears to take you to `appleid.apple.com`, which is a valid Apple website. But if you were to hover your mouse over that link, you’d see the real web address:

`https://ow.ly/e6Q0501Z2YRxxx`

I altered it a bit, because I don’t want you to accidentally click it. But that’s a shortened URL that would redirect to a website that looks just like an official Apple website, complete with a form to enter your Apple login credentials. This is what they’re really after here.

6. It’s probably hard to read this, but there’s a dire warning at the bottom: “If we do not hear from you within 48 hours, your iCloud will be suspended and any saved accounts and information will be lost!” Apple would never do this.

These are all very common “tells” in phishing emails, though some are much more believable than this one. I’ve received many phishing emails that almost fooled me. In fact, my old company used to send out phishing emails on purpose, as a training exercise. If you clicked the link, you’d be taken to an internal website telling you that you were just fooled and offering tips on how to avoid this in the future³.

Note that no reputable company should ever ask you to send them a password or credit card number or other sensitive personal info via email. Also note that any official government agency would send you a physical letter in the regular mail for anything truly important. Spammers don’t do this because it costs too much money. (Of course, there are plenty of scams that do come in the mailbox—usually insurance or warranty scams.)

³I knew people in the security department, and one of them shared an internal website that tracked all the phishing awareness campaigns. At that point, any time I got an email that looked suspicious, I could just check to see if it was one of the active campaigns.

There's a particular type of extortion email scam that can be really scary. The bad guys send you an email that contains one of your old passwords. They use this "evidence" to claim that they have hacked your computer. They've secretly turned on your webcam and taken compromising pictures or video of you. They've stolen sensitive files from your computer or smartphone. If you don't pay them money, usually in Bitcoin, they threaten to email this stuff to everyone in your contact list, which they also stole.

The hook here is the old password—it probably is (or was) one of your passwords. How could they possibly know that?? Chances are good that some account of yours was involved in a data breach and the bad guys were able to crack your password. These passwords are then sold on the "dark web" in bulk batches of thousands or even millions. So, if this password is still in use by you on any online account, you should change it immediately. But you can stop worrying about the extortion email—it's all a lie.

The safest thing to do with a scam email is to just delete it. If you're worried that it might be real, contact the company/organization directly. Go to their website or log in to your online account by manually typing in the website address. Or just call them.

For things like newsletters and generic marketing emails, they usually come with a tiny, hard-to-find "unsubscribe" link near the bottom. Sometimes it's just labeled something anodyne like "update email preferences." If you know and trust the sender, particularly if you know that you gave them your email address at some point, it's okay to click these links to try to opt out of future emails. However, if you don't know or trust the sender, your best bet is to just delete the email. If your email service has a way to "mark this email as junk," that's even better—not only should it prevent you from receiving more emails from this sender, but it may also prevent others from getting them, too.

Pseudonyms R Us

In the past, online accounts were more like computer accounts—they used to allow you to choose your own username. Today, most online accounts use your email address as your username. This has two primary benefits over letting the user choose their own username. First, you don't have to go through the process of finding a unique name when all the good ones are taken. Who wants to be coolguy349? Email addresses are already guaranteed to be globally unique. Second, having your email address lets them ~~spam you~~ send marketing emails to you.

Most of us probably only have one or maybe two email addresses—like a personal one and a work one. That means that everywhere you sign up for an online account with your email address can be correlated with all the other places. Marketers love that. It also means that if a bad guy somehow manages to get your credentials for one account, they can try those same credentials on other accounts. So, not only is it important to use unique passwords for every account, but it can also be helpful to use unique email addresses, too.

But how can you do that without creating a bunch of email accounts? Even if they're free, that would be painful to maintain. There are a couple interesting options, actually. First, you can purchase your own Internet domain name. It's only about \$15 a year, and you don't have to put up a website—you can just use it for email addresses. If you buy the domain `cooldude.com`, then you effectively own every single email address that ends with “@cooldude.com.” This can be fun, too, because you can make up email addresses on the fly, knowing that they will all go to a single inbox.

For example, when you're at the counter at Macy's and they say that you can save 10 percent right now if you give them your email address, you can say “sure... my email address is `macysucks@cooldude.com`.” And it will work. If they send you too much crap, you can just create an email rule to route all emails to that address to a folder or directly to the trash.

But there's another method that's easier and usually free: email aliases. You need to use a dedicated email alias service, or in some cases your email service provider may already support creating aliases. You ask the service to generate an email alias and then tell it where to forward the emails. For example, DuckDuckGo has a free service that generates email addresses that end with “@duck.com.” Here's how it works. You install a plug-in for your browser and on any web form that asks for an email address; you will now see a little DuckDuckGo icon. If you click it, it will generate a unique email address and fill it in for you. Any emails sent to this new address will first go to DuckDuckGo's server, which will then forward it to your real (hidden) email address. You can even reply to these emails—the responses will go back through DuckDuckGo's server, which will replace your real email address with the alias. The other side will never see your true email address. And at any time, you can tell DuckDuckGo to deactivate the alias, and you'll never get emails from that address again.

There are downsides to this method. Sometimes well-known email alias providers are blocked in web forms—they may say the alias email address is “invalid,” for example. For another, you can't invent them on the fly. For example, in my Macy's checkout counter example, I'd have to pull up the email alias generator tool on my phone to give the clerk a

working address. Finally, you won't be able to rattle off these addresses when asked. Let's say you signed up for Macy's preferred customer account online with an email alias, but now you're at the checkout counter, and the clerk asks you for your preferred customer account email address to get your discount. You'd have to look it up, probably using BitWarden on your phone. It's doable, but not as convenient as just knowing it.

Though email addresses are like gold to marketers, cell phone numbers are like platinum. Almost everyone has a mobile number now. And because these numbers are portable (between cellular providers) and people hate changing them, cell numbers tend to follow people for life. In this way, your mobile phone number is a globally unique identifier that will probably never change. Furthermore, like an email address, marketers can use this identifier to send you stuff. It's so easy to get your cell number these days. Making a reservation? Give me your mobile number. Want to enter a contest? Just send a text message to SPAMME. Want to buy something from a street vendor? Just scan this Venmo code. It's no wonder that spam text and robocalls are so prevalent these days.

Like email addresses, it's technically possible to get a cell phone number alias—that is, a second phone number that will forward to your real one. Or you can get a completely separate account with its own number, sometimes referred to as a “burner” number. Unfortunately, these methods are not as simple as email aliases. For example, some phone number aliases only work for voice calls, while others only work for text messaging. Getting a fully functional second phone number will require some sort of subscription service. I'll give you some options in the checklist for this chapter.

Securing Communications with End-to-End Encryption

So, how can you communicate today without someone eavesdropping? We answered this question in Chapter 3 from a theoretical perspective: we need to use encryption. Your emails are encrypted in transit as they travel between you and the recipient, across various Internet connections and computer systems. This is done for you by HTTPS connections and similar secure data transfer mechanisms. When copies of your email are stored on the email provider servers, they're also encrypted—but the providers hold the keys.

What you need to do is encrypt the contents of the email before you even send it, in such a way that only the recipient can decrypt it. That is, encrypt the message from one end to the other end. That's *end-to-end encryption*, often abbreviated as E2EE.

Think about it this way. You can put your money in a safe—that’s security at rest. If you want to then send that money across town, you could hire an armored car—that’s security in motion. If you want to be really secure, you would have the armored car transport the money in the safe—that’s using both mechanisms at once. If someone hijacks the armored car or follows it to its destination, they’d still have to break into the safe to get the money. Furthermore, you don’t have to put all your trust in the armored car company. This describes would be end-to-end security.

But sometimes you can’t have both encryption in motion and encryption at rest. If you can only do one of these, you should encrypt the content. This would be like driving your money across town in a safe that’s sitting in the back of your pickup truck. Everyone can see the safe—and may well assume that it contains something valuable—but the contents are secure, assuming you bought a decent safe and didn’t write the combination on a sticky note on the dashboard.

So, we have two angles to cover here. First, we need to know how to encrypt messages and files, before we send them, regardless of the sending mechanism. Second, we’ll need to look at finding a secure way to send the communication. We’ll look at email, text messaging, voice calls, and video conferencing. Let’s start with securing the message contents.

Encrypting Message and Files

As we discussed earlier, you have two primary options for encrypting data: symmetric and asymmetric. You could encrypt your message or files using a shared secret (password or passphrase), but then you need some way to get that shared secret to the recipient, securely. You could encrypt your data using the recipient’s public key, allowing them to eventually decrypt it using their private key. This is how PGP works. It’s a very clever solution to the shared-key problem, but in practice it’s tedious to do (as you will soon see). So, let’s start with symmetric encryption.

Symmetric Encryption

Any situation that requires a shared secret means that you will need a secure mechanism to share that secret with your recipient. You obviously can’t send the password along with the encrypted message. You will need to use a completely different communication channel to share this password, one that is also secure.

So, how does one go about encrypting a message or a file? The simplest way is to “zip” the file or files using a special application. These software utilities are usually used to bundle several files together into a single file, usually compressing them in the process so they take up less space. You select the file or files and tell the utility to bundle them up, resulting in a single output file that should be smaller than the original(s). The most common such utility creates a file ending in `.zip`, so the files are “zipped up” into a bundle.

But these zip utilities also often have the option of adding a password to the bundle, meaning that the recipient won’t be able to unzip the file without knowing the password. Adding the password encrypts the entire bundle.

If what you’re sending could be sent as a Portable Document Format (PDF) file, you can also secure the PDF file with a password. So, if you’re sending a single file, you could export that file to PDF and add a password to that file. (This may require opening “advanced” options when exporting the file.)

With symmetric encryption, you’ll have a password or passphrase that you need to share with your recipient. You’ll need a secondary, secure communication channel to exchange that secret, like an encrypted chat message—or just a phone call.

Asymmetric Encryption

I’m not going to get into the details on how to do this because it’s frankly too tedious for most people. Our computers use this technique all the time, but they don’t mind the tedium. Still, I thought it would be kinda fun to walk you through how one would go about using asymmetric encryption to send a file securely. For this example, I’ll use the classic asymmetric encryption tool: Pretty Good Privacy.

First, I need to securely generate a pair of keys: one public, one private. You can do this with a command-line tool like `ssh-keygen` or a graphical tool like GPG Suite⁴. Here is my actual PGP public key:

⁴That’s not a typo. This tool is named for Gnu Privacy Guard, which is abbreviated GPG. Clever, but also confusing.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
```

```
mQINBGHe8eoBEADs/BA7s5fk9W5uR6mZEkRoZ2uKw+Aw/mnKbzDxNCYRpf9by0K
BhjdpqLdZ0EmHtDhnmBwLjAoLtoXTPYm70AQhAXPp4vXL01ULERET4ACj5WNY
EHTzqpyS+BYDXFme98M2A7fNbnEH71bbvy1tQtSjofekLCTVbszYRexJv8Zzem65
6w+MV0+m/52yn4hs3jEViLhCrYBUZYiic1YorZ+TVRj06J3LySfYIE8uqG0YrOQZH
/NHQ7TzduLT59UTCzAwC7Y26T8Ws/+EjDB8dWuVfnvd5FFepdvdv36fe/LQ1d2mtP
8BjkeV2hVNuTGzLKkeP2fPdmreba0zw7fLLV3cynBT9BrBXxu7+D1EDEewARAQA8
FiEEgEx4gRyTr5qkC2ttLUQwQnr2mJfAmH8XQcGwMFCQeGH10FCwkIBwIGFQoJ
V2BdkCRipavYYXHPzktqafFUpw24/wLhVPPXAui+H/HeYVjdXJ/RTjWZRT+mp
tLpUyFNpVjgQPhNsQpTgGqQDNTAypaPZcIPcXeY01n876w1N5FjMB9FrzFT81tL
JhN3Rdbbz1sduXC3S/DgGzR3hnOaDDfnh1vA5v7DhifSg6Epzqc8V0hhaW/zBct3
f8HG3mjI3mQr6aA9/1dKuR/Td2mZFrVw5i1VCLniwdVlhybgwepU9Cx6ye1JpKH7
iGPMg1hKp6ZHRX8tE0+td5+w16ENknIJS/ZqRKA8BfQu7hUXKMghkV/8qNU+Y1
td7nVFEz0XIdK0o+AM20MUNhcmV5IFBhcmT1ciA8Y2FYzX1AZm1yZXdhbGxzZG9u
BBYCAwECHgECFA4W1QSAthBHJ0vmqLa20tRDBCEvaanNUCYfXeqA1TZAQAACRAT
2qcahYuya1LZ7W8efp9K+ybYGFDoJuprwc5DKjzHDH79VB1Rz2t+4A1T1WdUc0e/
1I0cT6ggQ/Y7aMoIiFuH8+PD712xY53se/1RUZU0ee/ZTiX+am/dmuKuakA6CCBD
bcxxXSMp0MQhD2E2qnG0Cr93E64joB0Vv0e/eD6SI8DORX0rE0tD9ywjrbvzg2Vs
ULq0U9zQfwdSx0K1sD5P0oqgyVvRYyIwGUvIyRAR1Nzbw35pnmaY98Z3kPMpjfd
yXjYjcaVbVfuuEHTgdQSF19mJY4h5fG0k17qumF7ARc7KD7jRrCLyYOfzacz2+4/R
3VhQARAAsGcdLiCtqTmWcnNajL5n1Ufb23giRCfmp7Z4/DZv5MxQnPaQ27IbHyR
KnI+BkfxVvvcFAXvKt1smrKBIbtbrg07AKRwR21+oG6xVphYFEK9t83YtBHvH3G
7N1DBCWqXuZvddoAdgs0H1w6+mmT5QeL0B8K7b0zCF013G5vc8mK0LHiB9p7qBR1
nTNvKzWGNzQP16XzqpuI6KevFAgJtXfj1k30qJL5tYdh95HjQz30MqXmWgVm8NL
e+dem1UUsXobhgwK89+3vRJB8M8CQ012fXk7EpI9bvApYtJE0C2DSXDIBnJJzahZk
2HkJKvBwFc/480797n9x8mvA1arIRzmbPxI966bU8na51rp057EAEQEAAyCAPAQY
MEJ69p01bjkP/IDA01HTs4i18JWk9dafhL0wMM/npXBHnNjY/udwTUwbls7nf6fc
V1Xh1J3muApZwQJmU50NMxuc/X8w1AY5eMzs3wFVFN3mXo2MA/car5zQ4awjtCMY
C/Uj1oWLPx/EjHB6teKZvexUeu20b0fTyrnoJ5+MMB+HJX9A+vYTDz/Tum42y1z
dXa1TQeah/Yg8Ka/w111G4e14dDtE1bmBYvd4WCZz1KI9MwK0b01N2IDoTLGc3eR
+dmwDH7GM2jQw54kmbkZ1R7G1K0Rorizd4Y6ebHwWFezGa2ice603d8yviubu1G
OX1qZmPNF5pJwiSDvuboyA5A3LHThw0bGzCSUnF2UJLPslu1TN1s2 =1p/g
-----END PGP PUBLIC KEY BLOCK-----
```

This two-column view is not the canonical format, but I wanted to condense it a bit. That’s a 4096-bit RSA public key. To make it available to anyone who wants it, I’ve uploaded that public key to a key server on the Internet. You can find it here:

<https://keys.openpgp.org/>

Most people don’t share the entire key, for obvious reasons—they instead share the fingerprint or hash of their key, which can be used to look up the full key. My key fingerprint is as follows:

804C 7881 1C93 AF9A A40B 6B6D 2D44 3042 7AF6 9A35

So, let’s say you need to send me a secure message. You first get my public key. Now you need to use a PGP utility of some sort to encrypt the message, which may be contained in a text file, PDF file, Word document, or some binary. First, you import my public key into your encryption utility and then use the tool to encrypt the file using my public key. The encryption app will output a file in a special format, like a .gpg file, that you can now send to me however you’d like—let’s say you attach it to an email. When I get the email, I will download the encrypted attachment and use a similar tool to decrypt this file using my private PGP key, which only I have access to.

You can see why few people go through the trouble of doing this⁵. However, you really don't have to. There are several great tools for exchanging files over the Internet securely that handle all the tedium for you. I'll cover them in the checklist.

Secure Email

As we've said, emails are encrypted in transit and when stored on email providers' servers, but the email providers hold the encryption keys. They are almost surely scanning your messages to improve their marketing profiles on you. Most of this is automated (it's not a human reading your stuff), but nevertheless, you're paying with your privacy to use these "free" services. They may also be selling this information to data mining companies, who will package this up with other information about you and sell to yet other companies. It's an amazing economy that most people never see or hear about.

But there will come a time when something you want to send via email needs to be completely private. Maybe you're sending a steamy love letter, or maybe you're just trying to send financial information to your tax preparer. Remember that copies of whatever you send will likely remain on the email servers of your messaging provider(s), possibly even after both you and the recipient delete the message in question. You want that info to be locked up in a way that will resist breaking, potentially for years.

The simplest method for obtaining E2EE with email today is to use a secure email service. These services will take care of encrypting both the contents of your email and any attachments. The encryption will happen locally on your computer before the email is sent—and decryption will only happen at the far end when your intended recipient reads the email. The downside to these services is that both you and the recipient usually need to have accounts with the same secure email provider. Some services allow you to use PGP so that the recipient can use a different but compatible secure email service. Some will let you send a message to any other email service (even an insecure one) by providing a special link that the recipient must click to read the message. This usually requires a shared password.

Of course, you can also just encrypt your message as a file and just attach this file to your email, using any email service you wish. This is the safe-in-your-truck-bed approach. But

⁵If you want to try this out just for funsies, feel free to send me an email with an encrypted attachment. It may take me a while, but I'll send you back an encrypted reply. Be sure to tell me where to get your public key!

you now have a secret (password or passphrase) that you must securely share with the recipient somehow. You obviously can't put it in the email. You need to send the password for the encrypted file via a secure text messaging app or perhaps over the phone.

Secure Text Messaging

Let me say at the outset that regular SMS messages ("texting" or green-bubble messages) are not encrypted. This means your cellular provider(s) can view the contents, as can anyone else who may be able to tap the communication lines. Unfortunately, Android's preferred replacement for SMS, Rich Communications Service (RCS), is no more secure.

Apple's Messages app will encrypt your messages end-to-end, but it's important to know that Apple can decrypt those messages if you save them to iCloud.

There are several end-to-end encrypted text messenger apps out there that will allow you to communicate privately with someone via your smartphone or your computer. But here's where the "end-to-end" part gets tricky. These messages must be in plain text (unencrypted) while you create the message and must be decrypted for the recipient to read it—that is, the message text is necessarily unprotected at each end. That means that your messenger app also has access to the unencrypted text. You therefore need to fully trust that application and its maker.

Unfortunately, many apps that do have end-to-end encryption technology are not really trustworthy. For example, Facebook Messenger and WhatsApp (both owned by Meta) have E2EE, but I would not trust them with my messages. Maybe the app will just scan the text for ways to target me with advertising without making that text available to a human somewhere (e.g., by a rogue employee or in response to a warrant), but that's still a violation of my privacy that I can't abide.

Knowing who to trust is difficult, but I'll have some solid options for you in the checklist.

Secure Video and Voice

Old-style landline phone calls are not encrypted, but we don't use those much anymore. Most cell phone calls and Internet video chat services today are encrypted, including cell phone calls and Zoom meetings. However, as I keep saying, the service provider in most cases controls the encryption keys. Nevertheless, this is sufficient for most cases because these calls and video conferences don't tend to be recorded and stored—they take up too much disk space. So, once the call is over, the audio and video are gone (unless one of the participants made a recording). Nevertheless, there are times when you're going to want fully end-to-end encrypted voice and video calls. Again, I've got you covered—I'll have specific suggestions in the checklist.

Summary

- Email and text messaging add a new dimension to the problem of secure communications. Instead of just having to secure a single channel between you and a web server (as with web surfing), you also need to secure the channel from the server to the intended recipient—and perhaps between your service provider’s server and their service provider’s server. That is, communication between two or more people is almost never direct—there could be other “legs” along the way that are not secure.
- Furthermore, even if all of these separate channels are encrypted, the messages themselves are almost surely not, meaning that the servers between you and the intended recipient will have copies of your messages that they can read or scan whenever they like. Those copies can remain long after you and the recipient delete them.
- Email addresses and phone numbers are globally unique identifiers, tied to accounts that contain lots of personally identifying information. Marketers love to gobble up these addresses and numbers because they know most people will never change them. It’s easy and helpful to create aliases, however, that can hide your true identity and prevent cross-account correlation.
- We have to be careful when clicking links and opening attachments we receive, even if they appear to be from someone we know and trust. Email in particular can be used to send dangerous, malware-laden files or links to fake websites that will attempt to infect your computer or trick you into giving up sensitive information.
- If we want truly secure and private communications, we need to encrypt the message itself as well as the channel by which it’s sent.

In the next chapter, we’ll talk about securing our online accounts, shopping and banking online, and reining in the amount of data we share on social media.

Going Further

I've had the honor and pleasure of interviewing Phil Zimmermann multiple times on my podcast. I particularly enjoyed our discussion on the 30th anniversary of PGP.

- <https://podcast.firewallsdontstopdragons.com/2021/10/25/through-the-past-privately-pgp-turns-30/>
- <https://podcast.firewallsdontstopdragons.com/2021/04/05/social-media-is-ruining-society/>
- <https://podcast.firewallsdontstopdragons.com/2018/05/07/we-now-live-in-the-golden-age-of-surveillance/>

Checklist

There are a plethora of options today for secure communications. And there are several important techniques for avoiding malware and phishing scams.

Tip 9-1. Scan Files Before Sending

As a matter of Internet hygiene, you should consider scanning files before you send them on to someone else (particularly if you aren't the original creator of the file). If you don't have an antivirus program installed (or if you just want to be super sure), there's a great website that will examine an uploaded file for viruses using literally dozens of third-party antivirus scanners. Of course, be aware of privacy issues here. While this site is trustworthy, you are still sharing information with a bunch of third parties here. Also, your company might not like it if you were to share proprietary information.

<https://www.virustotal.com/>

Tip 9-2. Encrypt Your Message and Files

You should never send sensitive or highly personal information via email or text message without encrypting it first. Again, most of these messages should be thought of as postcards, not sealed envelopes. And copies of these messages may remain on email servers long after you and the recipient delete the message. Sensitive info would include social security numbers, credit card numbers, passwords, medical or financial data, and anything else that you wouldn't want someone else to see.

The easiest method for encrypting a message and/or file(s) is to create a password-protected zip file⁶. While you will need some special tools to create this encrypted zip file, your recipient should be able to open this file without needing a special application. And even if they do, the applications are free and easy to use.

Your first step is to pick your password. Since this is something you'll need to be able to communicate to someone else (your recipient will need this to open the file), consider how you will send it. You can't use the same mechanism for sending the zip file and sending the password. Will you have to call them on the phone? Can you send them a secure text

⁶In macOS, there's another option: you can easily create a password-protected PDF file using the Preview app: <https://support.apple.com/en-ca/guide/preview/prvw587dd90f/mac>

message? Will they be able to copy and paste it, or will they have to type it by hand? You want something they can handle without too much trouble, but it can't be easy to guess. Once you have your password, proceed with the following steps to create your file.

Once you've created your password-protected zip file, you can send it via email, messenger app, or file sharing service. For maximum security and privacy, you should also use a secure messaging or file transfer service. This gives you both encryption at rest and in motion.

Tip 9-2a. Windows

The default zip function build into Windows, particularly older Windows versions, is not very secure. I would instead suggest using a free, secure zip utility for Windows called 7-Zip.

1. Download and install the 7-Zip application: <https://www.7-zip.org>
2. Put all of the files you want to encrypt into a single folder, say "my secret stuff." Then right-click this folder. On Windows 11, you'll first need to select "More Options" at the bottom (Figure 9-7). On Windows 10, you'll see the 7-zip menu directly in the first right-click menu (see in the following).

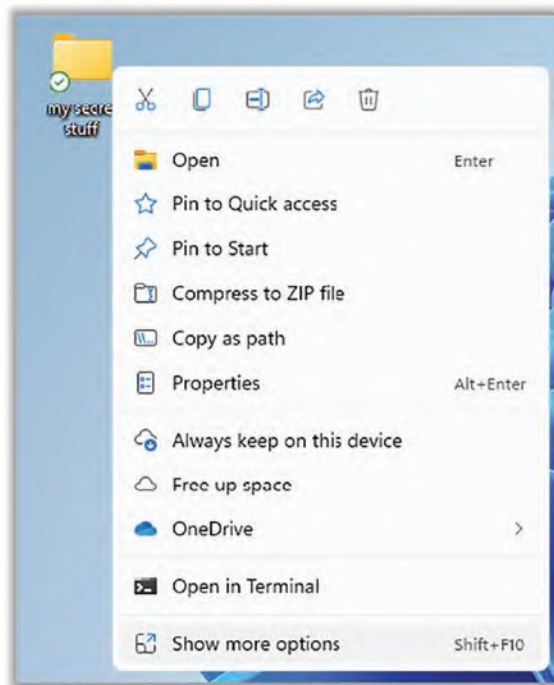


Figure 9-7. Windows 11 Show more options

Select the 7-Zip menu, and then “Add to archive” (Figure 9-8).

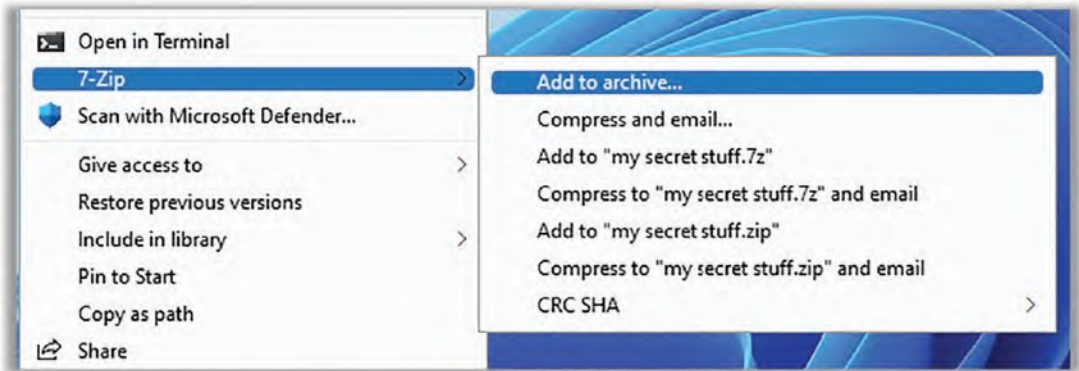


Figure 9-8. 7-Zip Add to archive

3. Don't let all the options scare you. In the window that pops up (Figure 9-9), you only have to check three things:
 - a. Set “Archive format” to 7z (upper left).
 - b. Set “Encryption method” to AES-256 (lower right).
 - c. Enter your chosen password (just above the AES-256 setting).

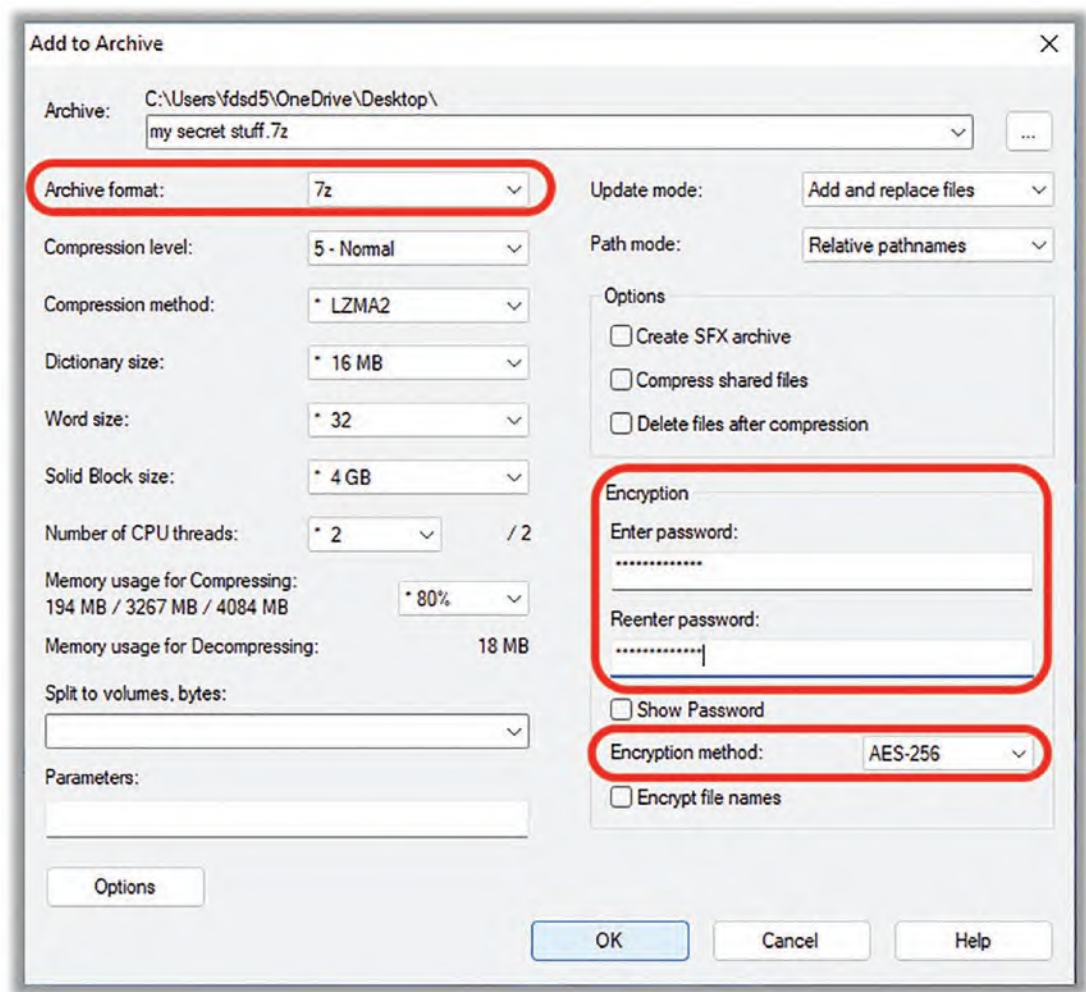


Figure 9-9. 7-Zip password-protected archive settings

- 4. Click OK to create your password-protected file (it will end in .7z).

Send this file to your recipient. If they have trouble opening it, have them download 7-Zip (Windows) or Keka (Mac, which I’ll discuss in the next section).

Tip 9-2b. macOS

1. Download and install Keka. Ideally, you would do this via the Mac App Store (\$4.99). But you can also find it on the developer website (I think for free):

<https://www.keka.io/en/>

2. Keka is handy but a little odd to work with. Launch Keka, and from the Keka menu, open Settings/Preferences (Figure 9-10). Select the Compression tab. Don't let all the option scare you. Just select the "Use AES-256 when encrypting" option.

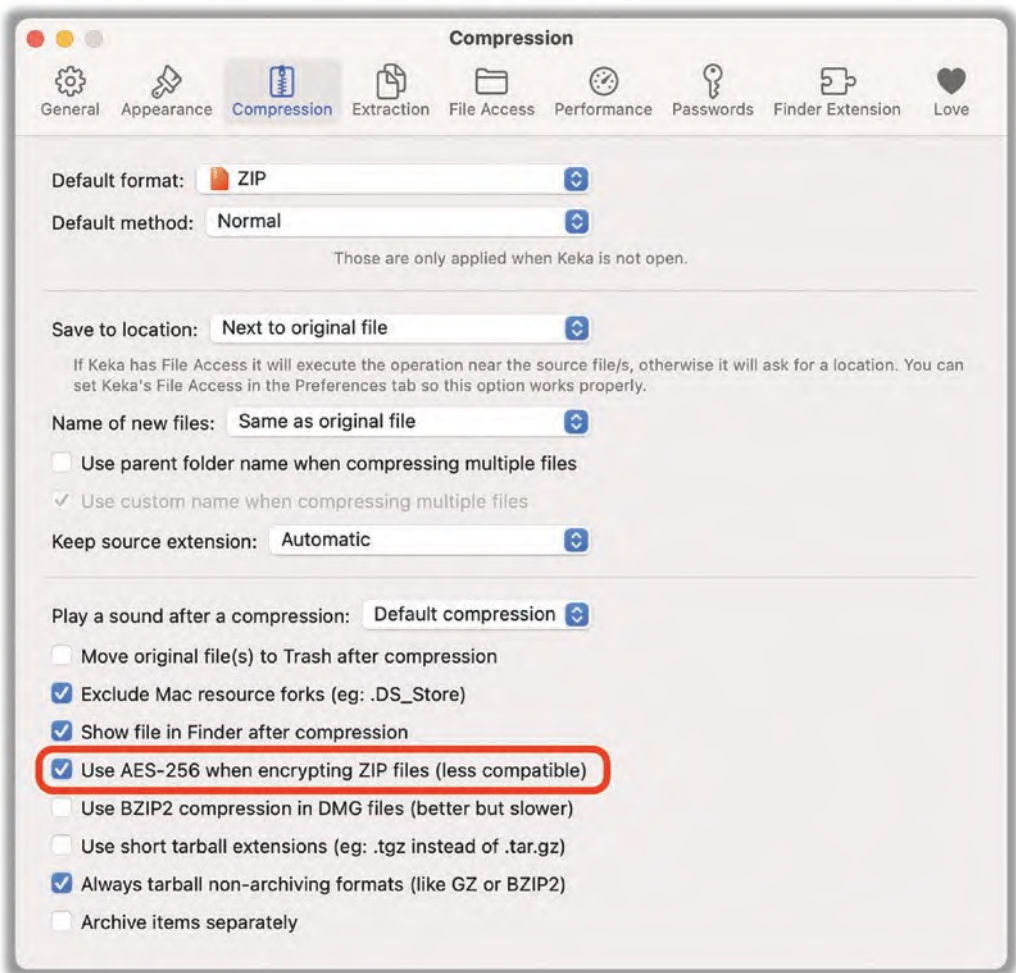


Figure 9-10. Mac Keka compression preferences

- Now, in the main Keka window, select “7Z” option at the upper right, if not already selected (Figure 9-11). Fill in your chosen password. I usually also select “Exclude Mac resource forks” (harmless and invisible to Mac users but confusing for Windows users).

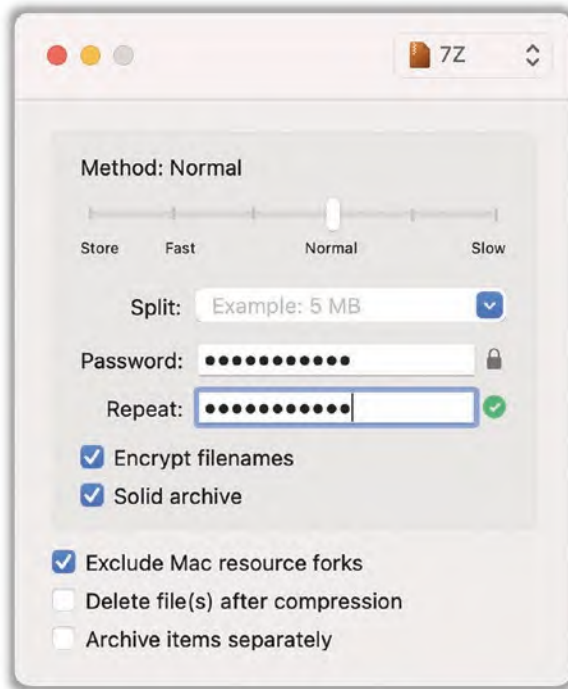


Figure 9-11. *Keka password-protected archive settings*

- Put all of your files into a single folder, say “my secret stuff.” Here’s the weird part. Drag that folder on top of the Keka window and it will change completely (Figure 9-12).

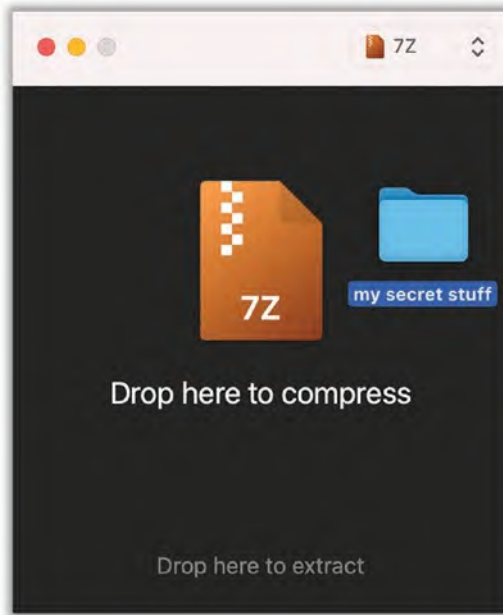


Figure 9-12. Keka creating an encrypted archive

5. When you drop the folder on Keka, you will be presented with a save dialog. Choose where you want your 7-Zip file to be saved. You can change the name of the file, if you wish (Figure 9-13).

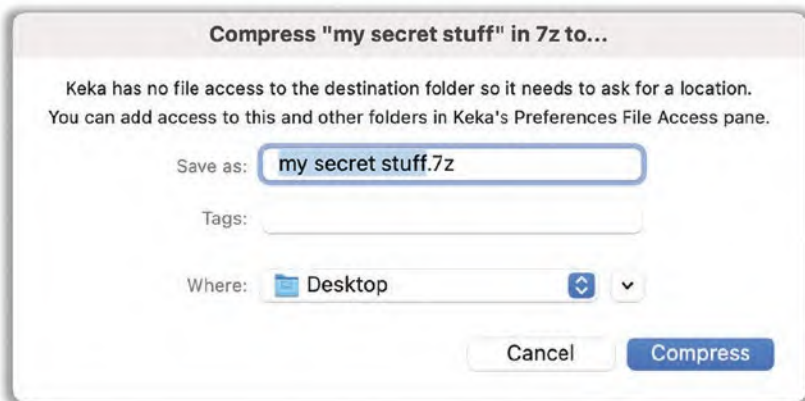


Figure 9-13. Keka file save dialog

6. Send this file to your recipient. If they have trouble opening it, have them download 7-Zip (Windows) or Keka (Mac).

Tip 9-3. Send Files Securely Using the Web

Over the past several years, several secure file sharing services have popped up. They all work in much the same way:

1. You go to the service's website.
2. You drag your file onto the web page, which securely uploads it to their server.
3. When the file is uploaded, you're given a custom link.
4. You simply give this link to your friend, and they securely download the file.

These services can handle pretty big files—from 2GB and up. Some services impose a size limitation unless you sign up for a free account.

Of course, anyone who gets a copy of this download link can get your file. But these services offer optional protections. You can password-protect the file. You can set a maximum number of downloads or set a time limit on the download or both. Of course, you can also pre-encrypt the file yourself using the previous tip.

Here are several options you can choose from. I've used most of them and tend to like SwissTransfer, but to the best of my knowledge, they're all good.

- SwissTransfer: <https://www.swisstransfer.com/>
- Wormhole: <https://wormhole.app/>
- Send: <https://send.vis.ee/>
- FileMail (use “send as link” tab): <https://www.filemail.com/>
- KPN: <https://filetransfer.kpn.com/>

If you don't like the idea of your file being on someone else's server, there's another option you can try that doesn't store anything. The downside is that both you and the recipient need to be online at the same time—because the file is directly transferred from your computer to theirs. Drop your file on the website and it will give you link. Send this link to your recipient. When they click it, the file will transfer. I actually like this option, if you can manage to coordinate being online at the same time.

- FilePizza: <https://file.pizza/>

Tip 9-4. ★ Use a Secure Email Service

The desire for truly private email communications is definitely increasing as we learn more and more about mass surveillance and hackers liberating embarrassing conversations from poorly secured servers. The marketplace has responded with new offerings that provide true end-to-end encryption.

I've tried several of these secure email services and I keep coming back to one: Proton. This company started as ProtonMail but has since expanded their services to include a VPN, secure calendar, and secure cloud storage. I'm sure they'll be adding more services. I've actually interviewed the CEO of Proton several times on my podcast. I trust these guys, I use this service myself and can recommend without hesitation. They have a perfectly functional free tier that you can start with, though I recommend paying for a higher tier—to get more functionality and storage space, but also to support good companies doing important work.

ProtonMail supports PGP and also allows you to send encrypted emails to any other email service. The recipient will receive an email with a special link—when they click it, they'll be taken to a website where they can enter pre-shared password and read your encrypted email online. But to get the most out of ProtonMail, it's best if your recipient also has a Proton account. Again, it's free to get a basic account, so there's very little friction involved. I've coerced several of my friends to create Proton accounts.

<https://proton.me/>

Some other options to consider are Tutanota, Mailbox.org, and StartMail.

Tip 9-5. ★ Use Secure Messaging Apps

Most text messaging today is not very secure. Short message service (SMS)—aka plain old text messaging—isn't secure at all. Other messaging apps have some encryption. Some, like WhatsApp, Facebook Messenger, Telegram, and Apple's Messages, even technically have end-to-end encryption (E2EE). But you still have to trust the endpoint and the service provider. Of these, I would trust Messages the most, but there are still situations where Apple can access your message content.

There are only a handful of secure messaging services that go out of their way to have zero access to your communications. There are very few of those around. But one that is almost universally trusted is called Signal. The designers of this app are zealous privacy advocates and incredibly talented at creating secure encryption systems. Signal can be run on Mac and Windows, Android, and iOS. You can even make audio and video calls with Signal. The software is completely open source, allowing third parties to review it for vulnerabilities and bugs. It's not quite as flashy as other, more popular apps, but it's plenty good enough. It's completely free, funded by donations and the Signal Foundation.

<https://signal.org>

You'll have to sign up for a Signal account and create a PIN code for added security. Be sure to save this code in BitWarden or somewhere safe!

Signal accounts are tied to your cell phone number. Signal is promising to provide a more anonymous method for creating an account, but I don't believe this is available yet. One benefit to using your cell phone number is that anyone else who knows your cell number can easily find you on Signal.

Note that whoever you're communicating with will also need to install Signal. This can be a barrier because people are sick of installing yet another messaging application. But you can convince them that this should be the last one! Seriously, though, if no one uses these secure applications, then existing, less secure services will never get the message (no pun intended) that people care enough about privacy to expend some effort.

If you'd like to see some other options, you might try these:

- Element (Matrix): <https://element.io/>
- Session: <https://getsession.org/>
- Threema: <https://threema.ch/>

Tip 9-6. Use Secure Voice and Video Apps

In the age of the coronavirus, we've all been introduced to the concept of multiparty video chats. The company Zoom became a household word overnight, though there are many such services out there: Webex, Skype, FaceTime, and more. Many messenger apps today also support voice and video calling.

While many of those are secure and private enough, you might at least consider stepping it up a notch. The simplest secure option is probably one you’ve never heard of: Jitsi. It’s free, the software is open source, and it’s end-to-end encrypted. It honestly works a lot like Zoom—all participants need is a meeting link and a web browser. Check it out:

<https://jitsi.org>

Of course, you can also use Signal, though it would require all parties to have an account. But honestly, for what most people need, most of these services are secure and private enough. (Zoom, in particular, has really stepped up its game after some initial missteps.)

Some general tips for doing a group video chat:

- Use a password for the meeting and don’t send the password along with the meeting link (it defeats the purpose). Send the password via another communication channel.
- Don’t use a static meeting link—use a new, random meeting ID each time. And don’t share the meeting link on social media or any other public forum.
- If the service has a “lobby” or “waiting room” option, this will allow you to explicitly admit each party (and weed out any unwanted crashers).
- If you’re doing a large meeting with some people you don’t know, restrict access to things like screen sharing, chat functions, and even the ability to rename yourself. These can all be used to harass or embarrass your group.

Tip 9-7. Open Attachments Safely

It’s easy to say “never open email attachments,” but sometimes you really need to read attachments. I usually qualify that rule: never open email attachments you weren’t expecting. If you ask someone to send you a file, and they then send you that file as an email attachment, it’s kind of pointless if you’ve decided to never open an email attachment ever.

There are a couple techniques you can use if you're worried about the security of a particular email attachment.

First, you can read the email using the web-based email client instead of an email app like Apple's Mail or Window's Outlook. While Outlook and Mail have some fancy features, they run on your computer or smartphone—and some malicious attachments can exploit these apps to gain access to your computer. Using the web client can give you some added protection—opening the attachments there will open them in your web browser, which adds another layer of protection between them and your computer. Most popular web email clients have built-in virus and link scanners. These clients also have much more limited access to your local files and operating system—they're "sandboxed" to help contain bad things within your browser. Here are some popular web clients for email:

- Apple's iCloud mail: <https://www.icloud.com/mail>
- Microsoft Outlook: <https://outlook.live.com/owa/>
- Yahoo Mail: <https://mail.yahoo.com/>
- Google Mail (Gmail): <https://mail.google.com>

If you want to check a given file for malware, you can upload it to Virus Total (Tip 9-1).

You might also try opening attachments using a nonstandard application. For example, for Microsoft Office documents, you can try opening them using LibreOffice (link in the following), Google Docs (online), or one of Apple's apps (Numbers for Excel, Pages for Word, or Keynote for PowerPoint).

<https://www.libreoffice.org/>

Tip 9-8. Use Email Aliases

Most people have a one, maybe two email addresses. Furthermore, most online accounts now require email addresses for your username. Marketers love this. They use these unique identifiers to track you around the Web and correlate your personal information across all your accounts.

But there's a very simple and free solution for this: use email aliases. An email alias is a sort of pseudonym for your real email address. Emails sent to the alias will be routed to your real email address, showing up in your inbox as usual. But the sender will never see your real email address and therefore cannot tie it to your real identity or correlate it across other accounts. The email aliasing service acts as a go-between, keeping your real address a secret.

The one gotcha with email aliases is that some websites will reject these addresses as invalid if they recognize it as a “dummy” address. They want your real address. But I haven't had too much trouble with this (yet).

Here are some email aliasing services you can try. They each work a little differently, so look at them carefully to decide which one makes the most sense for you.

- DuckDuckGo: <http://duckduckgo.com/email>
- Apple Hide My Email: <https://support.apple.com/en-us/HT210425>
- Firefox Email Relay: <https://relay.firefox.com/>
- SimpleLogin⁷: <https://simplelogin.io/>
- FastMail Masked Email: <https://www.fastmail.help/hc/en-us/articles/4406536368911-Masked-Email>

I would only use forwarding email aliases for unimportant accounts. They're particularly useful for one-off accounts that you never plan to use again. But for important accounts, I would use “real” email addresses. Note that this would include email addresses from a domain name that you own. To do this, you need to choose and purchase a custom domain name from a *domain registrar*. I personally like Hover (hover.com), but there are many to choose from. For most domains, you should expect to pay about \$15 per year (the first year might be cheaper). Be sure to set up automatic renewal.

⁷Note that Proton bought SimpleLogin and Proton may be renaming this service.

Then you need to find an email service where you can bring your own custom domain. This will also cost money. Even free email services will usually force you to move to a for-pay account in order to use a custom domain. Then you'll want to set up a "catchall" email address (see the respective help documents for the email provider you choose). Here are a few good options:

- Fastmail: <https://www.fastmail.help/hc/en-us/articles/360058753394-Custom-Domains-with-Fastmail>
- ProtonMail: <https://proton.me/support/custom-domain>
- Tutanota: <https://tutanota.com/blog/posts/own-domain-email/>

Tip 9-9. Review Unused Email Accounts

Over the years, you may have accumulated several email accounts. Sometimes your ISP will create an automatic email address for you, for example. Or perhaps you had to set up an email account for some special occasion and now have no need of it. If you never check it, you may never realize that it has been taken over by spammers or other ne'er-do-wells. I recommend checking in on your old accounts from time to time. Look in the Sent folder and make sure it hasn't been hijacked. (If so, see Chapter 13 for dealing with a hacked email account.)

If you don't plan to use the account anymore, you have two options. If this account was rarely used, I would delete all email in all folders, clear out any saved contacts, and then contact the email provider on how to delete your account.

If you want to delete an account that you've used a lot and is well known to your friends and family, I would instead consider just leaving it alone. Email providers will sometimes recycle old email addresses, meaning that someone else could end up with your address (like someone else getting your old phone number). This can lead to confusion and could even be abused. So, you might delete all the emails and contacts and then just check it from time to time to keep it active (from the perspective of your email provider). Make sure this account has a strong, unique password, too.

Most email accounts have a backup account—an email address where alerts should be sent. Make sure you have a good address set for any accounts you maintain.

If you've forgotten the password, you can usually find a "forgot my password" link that will send a reset email to whatever your backup email account was for that account. (I know...it's a vicious cycle, right? Do you have access to *that* account?)

Tip 9-10. Monitor Your Account Activity

Many email providers will alert you if they detect suspicious activity on your account. This often means accessing your account from unusual locations. (Remember, each computer has a unique IP address, and this address can be used to find your general location on the planet.) Every so often, you might take a peek at your recent activity to look for this yourself, especially if you have some reason to believe your email account may have been hacked. Here are links to three of the most common email account services. However, you can probably find similar "activity" information under your profile/account settings for most services.

- Google: <https://myaccount.google.com/notifications>
- Yahoo: <https://login.yahoo.com/myaccount/activity/>
- Outlook: <https://account.live.com/Activity>

Tip 9-11. Deal Properly with Spam

If you get an email that you're pretty sure is junk, don't even open it, and certainly don't reply to it. You don't want the sender to know your email address is active and valid. Don't try to "unsubscribe," unless you're sure the sender is reputable. If your email application has the option to mark the message as junk or spam, do that—it will help them to filter these messages out in the future (not just for you, but for others, as well). If there is no such option, just delete the message. If the sender is a company you have an account with, then log in to your account and find your email preferences. You should be able to turn off (or at least reduce) their emails there.

CHAPTER 10

Protect the Market and Town Square

We've talked about how to surf the Web safely and covered the basics of digital communications. Now we need to cover a few other related topics that have to do with your online behavior in general. We'll cover online banking and shopping, social media, cloud storage services, and just commonsense tips for living in the digital age.

Banking and Shopping Online

Online commerce was already popular before the pandemic, but once we were all staying home for months at a time, online banking and shopping transactions became the norm.

Credit vs. Debit Cards

As we discussed in previous chapters of this book, the security standards used by almost all banking and shopping websites are sufficient for protecting your credit card information, at least during the transaction. As long as you have an HTTPS connection, your communications with the far end are encrypted and secure.¹ The real concern is saving your credit card information for future use. While most large online retailers do a good job guarding this data, there have definitely been situations where hackers have managed to steal users' credit card information from these sites. But, as I said earlier in this book, fraudulent credit card charges are not a huge issue for the credit card owner—the credit card companies will not hold you liable for these charges, and you will never actually be out any money (assuming you report the charges in a timely manner, of course).

¹ Web browsers have mostly stopped showing the lock icon because today well over 90 percent of connections are secured. Now they just warn you when the connection is *not* secure.

This is *not* the case with debit cards, however. Debit cards provide immediate access to the funds in your bank account. If those funds are taken, they're gone until you can convince your bank to reimburse you. This is why it's always best to do your online shopping with a credit card instead of a debit card.

So, is it safe to save your card information with online retailers to make future purchases easier? Yes, I would say it's fine to do this with any major, reputable retailer, if you plan to do a lot of shopping there. But you can also store your payment card info in your password manager and fill in all the relevant info on any online shopping site with a couple clicks of the mouse. So, instead of trusting the retailer with this info, you can just trust it to your password manager. However, since the risks are fairly low with credit cards, it's really a matter of personal preference. But I would never save debit card information with any retailer—I'd keep that in my password manager and fill it in from there.

There are some other interesting options for online payments in terms of security and privacy, such as virtual credit cards and card "aliasing" services. I'll cover those in the checklist.

Online Banking

Online banking is another practice that makes some people very nervous. Because banks are doing everything possible to reduce the need to hire human beings, it's actually becoming hard to avoid online banking—and even expensive. Banks have taken to charging their customers for excessive in-branch transactions that require interacting with a live person². Like it or not, online banking is here to stay, and it's the only way to avoid the growing list of banking fees. Like online shopping, interacting with your bank online is perfectly secure and safe. You should feel at ease checking balances, making transfers, and paying bills using your computer or smartphone. I know it seems scary, but financial institutions have been sending trillions of dollars in financial transactions over computer networks for decades, and they have a vested interest in doing it securely. Nothing is 100 percent secure, but this is pretty close.

²One of my banks actually uses remote tellers. It's a funky machine that can accept cash, cards, and your ID, plus an interface where you can talk to a live human through a video screen and a payphone-like audio handset... like a cross between an ATM and prison visitor center.

However, what you may want to do is to set some reasonable limits on what someone can do with your accounts. I say “someone” because we’re talking about the case where someone other than yourself has gained access to one or more of your accounts. This is true whether you use online banking or not, actually. For example, overdraft protection can be helpful for you if you accidentally write a check that your primary account can’t cover, but if you allow *unlimited* overdraft protection, this could also allow someone who manages to steal your checkbook or debit card to drain multiple accounts. So, you should put commonsense limits on your bank accounts and limit how your various accounts are linked together. This is similar to creating a regular, non-admin computer account. You’re guarding against the case where someone gets access to your account and limiting the amount of damage they can do.

It pays to be vigilant, as well. You should check in on all your online financial accounts from time to time, looking for suspicious activity and verifying the account balances. Many online banking sites offer automatic notifications for all sorts of specific activities on your account like transfers, withdrawals, and purchases over a certain amount. You can also be notified of things like password and account changes, overdrafts, large deposits, and so on. This is a great way to keep tabs on your account activity.

Mobile Payment Systems

Credit cards arguably replaced physical currency decades ago. People just don’t carry cold hard cash around much anymore. But there’s one place they still can’t be used: between you and friend. Or really between you and anyone else who isn’t a vendor and has way to swipe your card. And that’s where popular personal payment apps like Venmo come in. While these apps have all done a pretty good job with security (at least in terms of the transfer itself), where they often fail is with privacy.

But let’s discuss security first. There are a few main aspects to security when it comes to payments. First and foremost, the app shouldn’t allow anyone to get at your money without your knowledge or consent. Second, you expect that when you do send money, that exact amount of money you specified (no more, no less) will be transferred and that it will transfer safely. Finally, you expect that the money will go to the proper recipient.

Most of the popular payment apps—Venmo, PayPal Mobile Cash, Zelle, Cash App, Apple Pay, Google Pay—do all of these things just fine. Some apps are better than others when it comes to preventing simple human mistakes, like a typo in the recipient’s info or the

amount. They provide a link you can share or a QR code you can scan, for example. However, it's worth noting that in all cases, the transaction is final. If you make a mistake, you're at the mercy of the recipient to give it back. (Apple Pay and Google Pay payments can be rescinded if the recipient hasn't accepted the payment yet.)

As you might have surmised, privacy is where these apps differ most—but not as much as you might hope. You should assume in most cases that whoever runs/owns the service has full knowledge of your transaction details. That doesn't necessarily mean that they're doing something nefarious with it—for instance, they're surely using this data to detect and prevent fraud. But in many cases, that info is likely shared with one or more third parties for “marketing purposes.” But the more companies that have the info, the more likely the info will be used in a way you'd rather it wasn't. These companies (as well as Visa and MasterCard) are surely monetizing your spending habits—with the possible exception of Apple Pay and Apple Cash. Apple has added a lot of interesting privacy features to their payment services.

Venmo has a special problem, though. Venmo is primarily a “social” app. That's shorthand for “share as much info as possible, with as many people as possible.” For a long time, all of your Venmo transactions were globally public³. BuzzFeed once used this “feature” to find Joe Biden's Venmo account, along with members of his staff, members of Congress, and even their families...and of course, all of their contacts, too. This was also an unwelcome surprise to the third of millennial Venmo users who used the app to pay for drugs⁴.

The bottom line is that most of these apps are secure but are poor when it comes to privacy. Also, you should treat these mobile transactions as final and irreversible. They have all the finality of a cash transaction with much less privacy and zero anonymity. I'll give you some other alternatives in the checklist for this chapter.

Financial Account Aggregators

One last odd case to cover: financial account aggregators. Probably the most famous one is Mint.com, but there are several other “fintech” (financial technology) companies out there that now do the same thing. Most financial advisors, for example, have some sort of

³<https://techcrunch.com/2021/07/20/venmo-removes-its-global-public-feed-in-a-significant-app-redesign/>

⁴<https://lendedu.com/blog/nearly-third-millennials-used-venmo-pay-drugs/>

“unified view” that shows you where all your money is going. To do this, these sites need access to your bank, credit card, and investment account transactions—all of them.

In order to access these transactions, the aggregators will ask you for all the account login credentials. When your aggregator asks you to give them your credentials and insist that it’s safe, they’re doing some magic behind the scenes to gain limited access to your accounts, probably using a service from a company called Plaid (plaid.com). This should absolutely make you nervous. However, in most cases, I believe this is safe⁵.

Credit Bureaus and Identity Theft

Identify theft is one of the nastiest problems you can deal with because it can negatively affect you for years, even if you do everything right. If someone manages to open a line of credit in your name and runs up a huge bill and these bills go to collection agencies, they could hound you for a long time.

Much of this hinges on some shadowy but powerful organizations called *credit bureaus*. The “Big Three” credit bureaus—Equifax, Experian, and TransUnion—know all about you. And yet you are not their customers; you’re their product. You can’t take your business elsewhere if you don’t like their service. You indirectly agreed to give these companies your information by agreeing to terms of service with your banks, credit card companies, utility companies, and loan agencies. The bureaus track all of your spending and debt and then generate a single score that supposedly determines your creditworthiness. The precise algorithm for calculating your credit score is a closely guarded secret, and even your access to your own credit history is strictly limited (one copy of your report for free, per year, per bureau).

In 2017, Equifax suffered a massive security breach, and the records of almost 150 million customers (nearly half the US population) were stolen. Equifax’s response was slow and insufficient, and yet to date there have been no real consequences for the company,⁶ or even the industry as a whole.

⁵ <https://identitytheft.org/faqs/is-plaid-safe/>

⁶ They were fined “up to” \$700 million. But they also made \$3.5 billion that year. One executive did go to jail: Jun Ying, the Chief Information Officer. But it wasn’t for lax data security; it was for dumping stock before the breach went public. He got four months in prison.

While many financially savvy people are aware of the “Big Three” credit bureaus, many are less aware of the Work Number and the National Consumer Telecommunications and Utilities Exchange (NCTUE). The Work Number is a service provided by Equifax that collects wage information from employers on about one-third of the working US population. This information is being used to do things like verify your employment history for prospective employers and validate your income for loans and social services.

The NCTUE is a sort of specialized credit bureau that is focused on cellular services but is also being used by utility companies. While this company appears to be a consortium of agencies, most of them appear to ultimately be owned by (wait for it) Equifax.

To be fair, these agencies do provide a valuable service that many consumers and lenders rely on. The problems are that they are not responsive to consumers and their security mechanisms have proven to be abysmal.

You can’t currently opt out of these credit services, meaning that they will still collect your data—and it will therefore remain at risk of being stolen or abused. However, you can at least protect yourself from someone opening new credit in your name (i.e., identity theft) by implementing a *credit freeze*. The process can be tedious (and we’ll go over this in the checklist), but at least now it’s free everywhere, thanks to some legislation passed in 2018. Freezing your credit means that your credit score and credit history will not be available to anyone for any reason. This means you can’t get a new credit card or a new loan without first “thawing” your account. But realize that your credit history is also often checked for other reasons: signing up for utility services, getting a new cell phone, applying for a job, and so on. When this happens and you need to grant access to your credit report, you’ll have to find out which credit bureau they use and temporarily thaw your account.

Planting Your Flag

There’s another benefit to freezing your credit: claiming your online accounts with the credit bureaus before the bad guys do it for you. This is often referred to as “planting your flag”. There are certain accounts that almost all will adults have, whether they want them or not. Many of these accounts are for governmental programs like social security/insurance or taxes or even the postal service. You already have an entry in their databases and there is an online account for that entry which you can establish. If a cybercriminal manages to set up and claim that account before you do, they can claim your benefits, file fraudulent tax returns in your name, or use these accounts as part of a broader identity theft scheme.

But there are other accounts that most adults will have that you should probably also explicitly claim. For example, you probably have a bank account. Even if you never want to do banking online, you should still create and secure your account through the bank's online portal. If you have any online investment accounts, including retirement accounts, you should be sure to establish your ownership of those, as well.

Finally, you should set up accounts associated with your home, as well: utilities, mortgage company, and your internet service provider.

Again, even if you never intend to use these online accounts, you technically already have them – so you're going to want to claim them for yourself before someone else does. Give them very strong passwords and set up multi-factor authentication.

Cloud Storage Services

Everything is moving to the cloud. That is, more and more of our services and data are going online. As we discussed in Chapter 6, Apple and Microsoft have made it nearly mandatory to sign up for their cloud accounts in order to use their products. However, in this chapter I'm focusing on cloud storage services. These services give you a virtual hard drive somewhere out on the Internet where you can store just about any type of computer file.

There are dozens of cloud storage providers these days, all claiming to protect your data with “military-grade” or “unbreakable” encryption. As we discussed with online backup, you need to understand who holds the keys to your encrypted data. In most cases the answer is “them,” unless you explicitly take steps to change that behavior.⁷

The simplest analogy for this is renting space in a physical storage facility, like U-Store-It or PODS. You buy a certain size container (the larger it is, the more it costs to rent), and then you put your excess stuff in the box. When you're ready to leave, you lock it. But who keeps the key? Would you be comfortable leaving the only key with the owner of the rental facility? That would mean anyone who could convince the owner to open that container would have full access to whatever is stored there. Most places allow you to keep the key (or perhaps there are two locks on the door and you each keep one

⁷ While this book was going to publishing, Apple announced that they would finally support client-side encryption for iCloud backups. This is a huge deal. The feature, dubbed Advanced Data Protection for iCloud, is supposed to roll out in 2023. When this rolls out, I will try to add more info on my book's web page.

key). This isn't only for your protection; it also neatly absolves the rental facility from responsibility for protecting access to the key and deciding who should be allowed to check out that key. The owner knows that, if necessary, they could break your lock and gain access, too—for instance, if you die or lose the key or if a law enforcement officer comes knocking with a warrant.

However, the default key arrangement for cloud storage is usually the exact opposite—the storage provider keeps the key, not you. Again, this means anyone who can convince (or coerce) the owner into coughing up the key can gain full access to all your digital stuff. It also means the cloud storage company (or any of its employees) has complete access, as well. However, some of these cloud storage providers will give you the option to provide and manage your own encryption key. You have a password manager, so you can use it to safely store these keys. There are also applications you can use that will manage this encryption for you, in the case where the storage provider doesn't offer the option for you to keep the keys. They will encrypt all your data before it's stored and decrypt it when you need it. You can think of it as a second lock or a container within a container—like storing a safe inside your storage container.

Sometimes, though, this is just too much hassle. Encrypting your data in the cloud means that it's harder to share with other people, and it may break some nice features (like searching by file name or content). The thing to keep in mind if you're not going to hold the encryption keys yourself is that whatever you put in the cloud could potentially be seen by someone else. As long as you don't care about that, then you can forget about pre-encrypting the data. It's important to realize, however, that just because you've deleted a file from this cloud service, they may still keep a copy. For example, when you delete a file from Dropbox, you can actually log in to your Dropbox account on a web browser and *undelete* it! That means it was never really deleted in the first place. These services may keep multiple copies, as well—so that if you change a file, they may retain a copy of what it looked like beforehand. They do this not to be sneaky (probably) but to help you recover something if you accidentally alter or delete it.

Social Media

Now we finally come to the web services that we lovingly refer to as *social media*. This includes things like Facebook, Twitter, Instagram, LinkedIn, TikTok, and Pinterest.⁸ The stated purpose of these services is to allow people to find, connect, and share things with other people. However, I'm here to tell you that the actual purpose of these sites is to compile massive dossiers on as many people as possible and sell that data (or access to that data) for money. Facebook even keeps tabs on people who don't have Facebook accounts⁹.

The profit model for all of these “free” services is to provide companies with highly targeted advertising on the principle that catering to an individual's tastes, income, education, religion, and so on will make them much more likely to buy. Social media services are the most colossally effective Trojan horses ever created by humans. People willingly provide hordes and gobs of extremely personally information on these sites. Even if you try to restrict access to your closest friends and family, you've already given the service provider permission to share this information with third parties and “partners” (this is buried somewhere in your terms of service, in language that is not very clear).

Probably the best example of this is the Cambridge Analytica scandal.¹⁰ It's a long story, but basically a political research and marketing company wanted to learn about as many US voters as possible. Working with a psychology researcher named Aleksandr Kogan, Cambridge Analytica (CA) created a fun little Facebook survey called “This Is Your Digital Life” that attracted 270,000 people to respond. When you take these surveys, you're granting the third-party survey maker access your Facebook data. However, Facebook also allows third parties to gain access to all of your Facebook friends' information, too. This allowed Cambridge Analytica to amass a database of highly personal information on nearly *90 million* Facebook users. Using this data for marketing purposes was against Facebook's policy, but CA lied and said it was using it for academic research.

⁸ Note that Microsoft owns LinkedIn and Facebook owns Instagram.

⁹ <https://www.cnet.com/news/privacy/shadow-profiles-facebook-has-information-you-didnt-hand-over/>

¹⁰ If you haven't seen the Netflix documentary *The Great Hack* (2019), it's well worth a watch.

But the real problem isn't policy, enforcement, or even security. The problem is that this data is being collected in the first place. The mere *existence* of so much highly personal information begs for it to be stolen and/or abused. On a personal level, people will invariably use this data to stalk love interests, check up on spouses or ex-lovers, dig into the lives of celebrities and politicians, and so on. It's just human nature. At the corporate and government level, the potential for abuse is almost limitless. While we have the Fourth Amendment in the United States that is supposed to protect citizens from unreasonable searches (usually requiring a judge to sign off on a warrant for very specific things), there's nothing preventing law enforcement from just buying your personal information from a data broker. *The only way to prevent your data from being abused is to not collect the data in the first place.* Since we can't prevent these companies from collecting the data, the next best option is to just never use these services.

Yeah, yeah, I know. That ship sailed a long time ago for most of you. These social media services are wildly popular because people truly enjoy using them to share all sorts of information with friends and family. So, let's just acknowledge that and move forward. However, you might want to reread Chapter 2 on this topic—limiting your oversharing of data now will still have a positive impact on your overall privacy. The information you've given away in the past will eventually get “stale” and be discarded.

Much of the juiciest personal information on social media is provided willingly by the account owner (i.e., you). Most posts on social media are public by default. This has all sorts of implications. First of all, how many websites still use “security questions” to recover your account when you forget your password? Common questions are “what street did you grow up on” or “what is the make of your first car” or “who was your first employer.” Much of this information is there for the taking on social media.

Second, these platforms have been used to get information from gullible people. Here are a couple examples:

- If you turned your social security number into a dollar amount, how rich would you be?
- Your porn name is the name of your first pet plus your mother's maiden name. What's yours?

Those may seem painfully obvious to you, but these quizzes, polls, and games glean lots of other personal information.

But there's another way that you give juicy information to these services (and potentially to bad guys) that you may not be aware of: metadata—specifically, photo metadata. Let me give you just one example. John McAfee (of antivirus company fame) was sought as a “person of interest” in a murder in Belize. McAfee is rather paranoid and said he believed the local police would kill him—so he fled the country. He did a covert interview with *Wired* magazine to tell his side of the story. When published, that interview came with a photo of McAfee at his secret hideout location. But the magazine failed to remove the photo metadata before posting it online. This photo metadata (called EXIF data, or Exchangeable Image File format) contained the exact longitude and latitude of the photo, along with the date and time. Turns out, he was in a posh resort in Guatemala. This nearly got him extradited back to Belize, but McAfee claimed that he faked a heart attack to give his lawyer time to come save him. He was eventually deported to the United States. Belize didn't pursue him, but McAfee said they did seize and auction off all his stuff. (He's not the most trustworthy news source.)

Note that some social media sites will automatically remove some metadata from your uploaded photos so that you're not unwittingly giving this information away to whoever downloads these images. But I would bet that the social media companies still keep that information for themselves.

In the checklist for this chapter, I will give you some specific advice on how to lock down access to your social media accounts and how to avoid giving out the wrong types of information. But if you're ready to make the break, I'll also tell you how to delete some or all of your social media accounts.

Giving Away Your DNA

There's one more topic I'd like to cover here: DNA. This might seem like an odd place to cover it, but I think about it in terms of online accounts like 23andMe and Ancestry. These services allow you to use your own DNA to track your family heritage and perhaps find long-lost relatives. Some services even claim to help you identify possible future genetic health risks.

While there is obvious value to these services, there are many scary ways this data can be abused. Law enforcement and intelligence agencies are using these DNA databases to find people—or, importantly, their relatives. Because you share a significant percentage of your DNA with your parents, your siblings, and your children, you are also submitting *their* DNA when you submit your own.

Of course, there are other ways we give up our DNA, some of which you can't really control. Whenever you take a swab test or give a blood sample, you're giving away some of your DNA. Most hospitals take blood samples from newborns and send them to state agencies to test for congenital diseases. Some states hold on to these samples for years, even decades. And now law enforcement agencies are tapping these DNA databases, without even notifying (let alone requesting access from) the DNA donor, for use in criminal investigations¹¹.

While we can hope that your DNA will be stored securely and access will only ever be granted to law enforcement when presented with a valid, court-reviewed warrant, I wouldn't count on that either. Databases can be hacked. Companies can be coerced. People do things they're not supposed to.

Worse yet, companies are constantly looking for new ways to bump up their stock price, and monetizing data they already have is an easy way to do that. They may change their privacy policy and slip in something like “by continuing to use this service” or “by installing this update” you agree to the change. What if your health or life insurance company could get your DNA? Or what if your DNA is sold off to a medical research company and they didn't anonymize it properly? What if drug companies could pay to send mailers to people likely to have various genetic illnesses?

So, bottom line: think carefully before you give up your DNA or someone else's. I would at least avoid any of the DNA family heritage services until we have strong DNA privacy laws in place.

¹¹ <https://www.wired.com/story/police-used-a-babys-dna-to-investigate-its-father-for-a-crime/>

Summary

- Online banking and shopping are very safe, in most cases. As long as you deal with a reputable retailer, make sure your connection is secured, and use a credit card from a major bank; you should be fine.
- Avoid using debit cards for online transactions. You have much more protection if you use a credit card, instead.
- Mobile payment systems like Venmo, Zelle, Google Pay, Apple Pay, PayPal, and others are all fairly secure and convenient. However, you're giving away a lot of potentially sensitive personal information (what you buy, where you shop, who your friends are, etc.). Also, these transactions are typically irreversible and should be treated like giving someone cash (without the privacy benefits).
- Identity theft is one of the most difficult attacks to recover from. To prevent someone from opening new credit in your name and sticking you with the bill, your best option is to freeze your credit.
- Similarly, you already have accounts with many governmental, financial and other organizations whether you want them or not. You should take the time to claim those accounts online before the bad guys do it for you – that is, you should plant your flag.
- Your DNA literally *is* you. Giving it away for any reason can have unintended consequences—not just for you, but for all your blood relatives. Until we have strong DNA privacy laws, I would avoid giving anyone's DNA away to services like 23andMe or Ancestry.
- Cloud services provide extremely convenient ways to access and share your files, pictures, and other data, but you need to understand who holds the keys to that online storage and know that your storage provider may save copies of your files long after you “delete” them.
- Social media services like Facebook and Twitter collect unprecedented amounts of information on their customers, and they make money by selling that information to advertisers. You need to be mindful of what information you give them and what you share with others.

Everything we've discussed so far in this book applies to just about everyone, regardless of age. However, there are specific issues that only apply to children. In the next chapter, we'll look at security and privacy problems for our kids.

Going Further

- Debit cards can be dangerous. Someone managed to drain one of my bank accounts by guessing my debit card number: <https://firewallsdontstopdragons.com/my-debit-card-was-hacked/>
- You might find it interesting to know what some of your personal data is worth to online criminals: <https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it>
- To learn more about DNA rights and potential abuse
 - <https://www.eff.org/issues/genetic-information-privacy>
 - <https://www.consumerreports.org/dna-test-kits/privacy-and-direct-to-consumer-genetic-testing-dna-test-kits-a1187212155/>

Checklist

The checklist for this chapter sort of covers the “rest of the Internet”—things like online banking and shopping, social media, and online behavior in general. The items here are a bit of a hodge-podge of online safety guidelines, tips, and tricks.

Tip 10-1. ★ Lock Down Your Apple/Microsoft Accounts

It’s almost impossible to avoid setting up Apple iCloud and Microsoft user accounts. These cloud services are deeply embedded into most recent versions of macOS, iOS (iPhone and iPad), and Windows. But you can still tweak the settings on these accounts to better protect your privacy. In this section, we’ll lock down the settings on your computer and online. (In Chapter 12, I’ll show you how to lock down your iOS and Android cloud settings.)

There’s no way to sugarcoat this... there are a gazillion settings here and they’re confusing. This is absolutely on purpose. I’m not going to go through every single one of them, just some key ones. I suggest you poke around and at least familiarize yourself with as many of these settings as you can find. You want to look for things like privacy, customization, personalization, advertising, marketing, history, and permissions.

The other hard truth is that these settings change often. And when new settings show up, they’re often “on” by default (i.e., set to the least private option). This is the world we live in now. Keep in mind that all of the talk about “personalized experiences” is really about building up a profile on you that may be shared with others. The way they customize your experience is by collecting data about you. Just say no wherever you can. Until we have strict privacy laws or change the Internet business model, you have to assume that all of this data collection is more for their benefit, not yours.

Tip 10-1a. Windows 11

There are two main places to change your Microsoft account privacy settings: your computer settings and your online account settings. We’ll cover both of those here. Many of these services are handy—and if you know you want to use them, then just be aware that you may be sharing data. For anything you are not using or are not sure if you’re using, turn data sharing off. You can always come back and change the setting later.

Computer Settings

- 1. On your computer, search for just generic “settings” and open the Settings app. Click the “Privacy & Security” tab at the left (Figure 10-1).

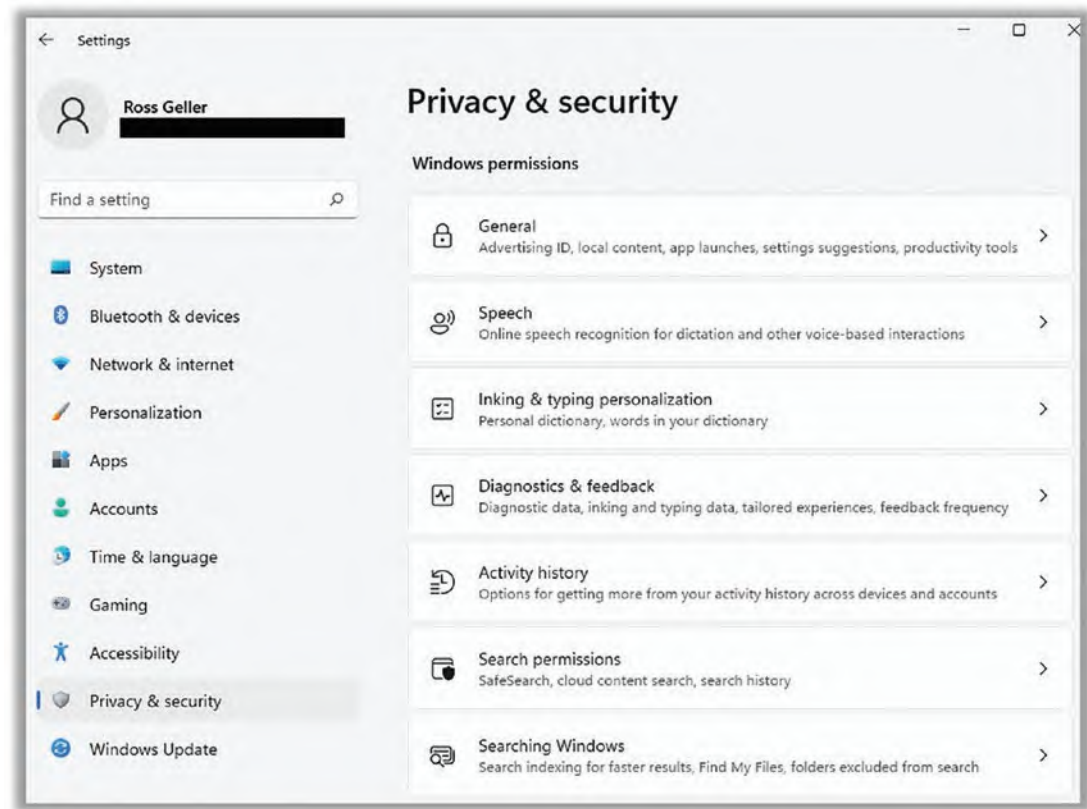


Figure 10-1. Windows 11 Privacy & Security settings

2. Under the General section, I would turn off everything except maybe “Let websites provide locally relevant content.” This would limit search results to English sites, for example (Figure 10-2). This probably only affects their Edge browser, anyway (and you’re using Firefox, right?).

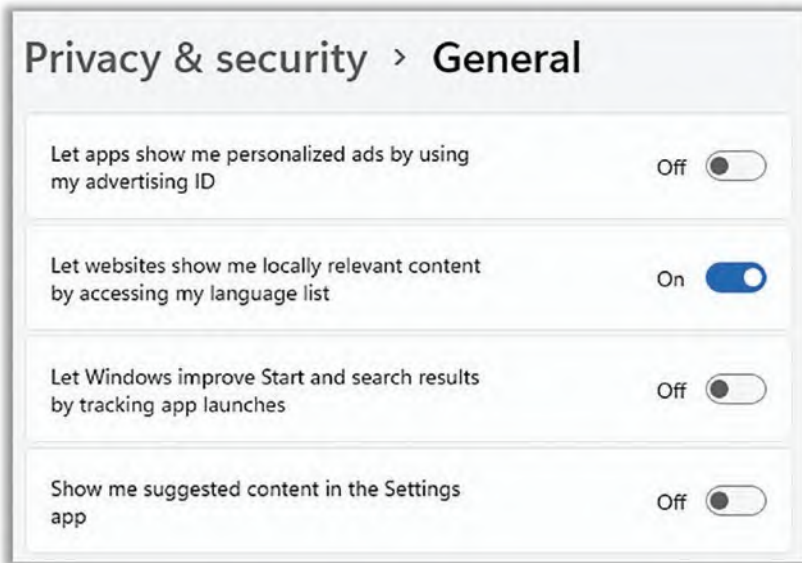


Figure 10-2. Windows 11 General privacy settings

- 3. Now (for some dumb reason) you have to go to a Under the “Diagnostics & Feedback” tab; I would turn everything off—especially the “tailored experiences” (Figure 10-3).

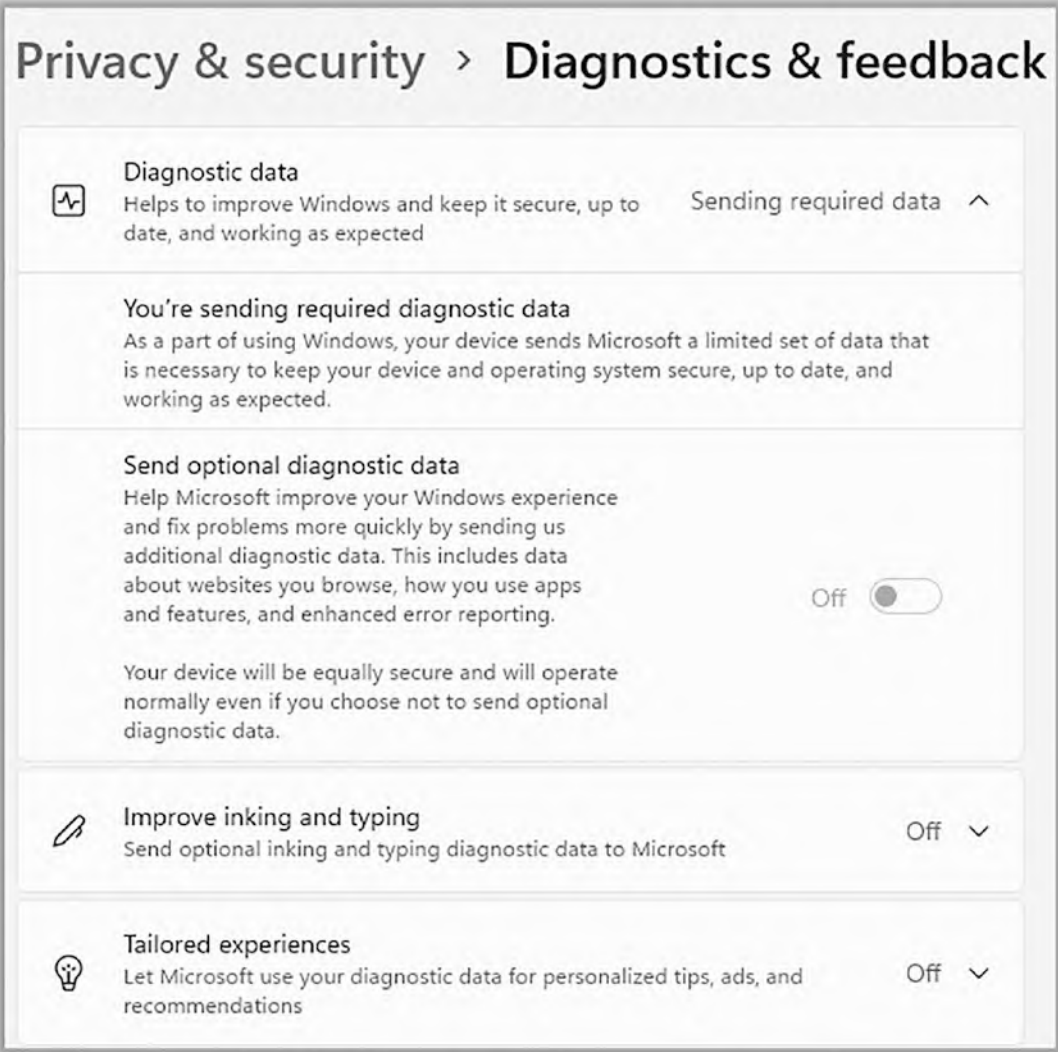


Figure 10-3. Windows 11 Diagnostics & feedback

4. And now for the fun one: app permissions. There are a gazillion settings and in Windows 11 they're hard to get to. Click the "Apps" tab at the left and then select "Apps & Features" at the right (Figure 10-4).

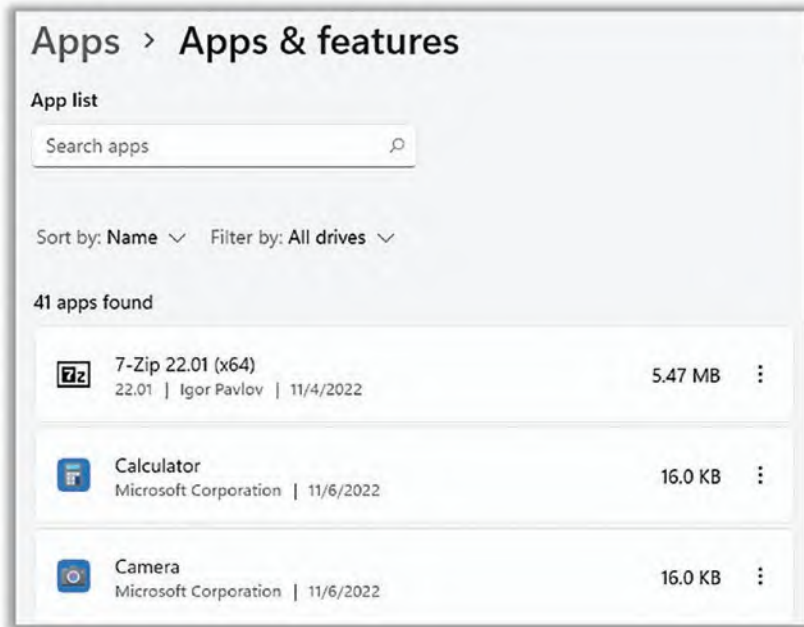


Figure 10-4. *Windows 11 Apps & features*

5. Basically, you need to look at each application in the list; click the little vertical three-dot menu at the right and look for "Advanced Options." If available, there will be a permissions section where you can enable or disable access to things like location, microphone, camera, calendar, contacts, and more. You can see an example in Figure 10-5, the Camera app. Repeat for each app in the (probably long) list.

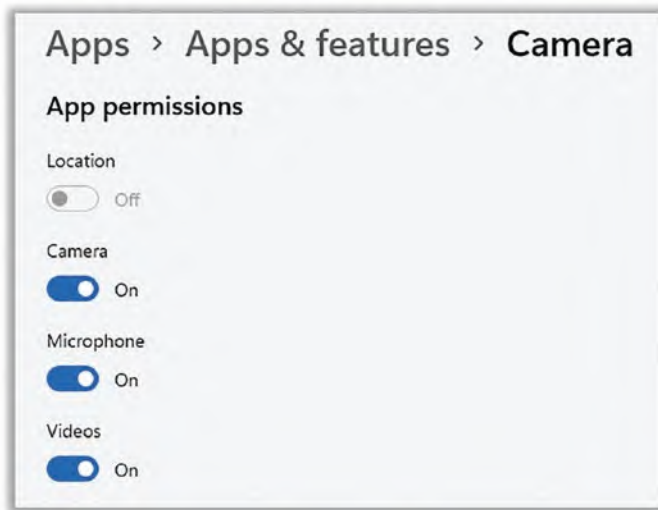


Figure 10-5. *Windows 11 Camera app permissions*

Privacy Dashboard

Next, you need to go to your Microsoft online account, if you have one, and review the privacy settings there. Go to this site:

<https://account.microsoft.com/privacy>

Again, there are many, many settings here. Here are the settings I'd be sure to look at.

- **Activity Data:** In this section, you can view (and delete) the activity data that Microsoft has saved about you. You may find this very revealing.
- **Personalized Ad settings:** This is toward the bottom of the page—click the icon to open the settings. Just turn this off.
- **Apps and services:** Review any apps contained here and revoke access wherever you can. Some of these you may wish to keep, but think about each one.
- **Promotional communications:** I assume you'd want to disable all of these.

There are several links here that will help you find more Microsoft privacy settings, including their search engine (Bing), Microsoft Office, Microsoft Teams, Xbox, Skype, LinkedIn, Outlook.com, and OneDrive.

Tip 10-1b. Windows 10

There are two main places to change your Microsoft account privacy settings: your computer settings and your online account settings. The computer settings will be covered here. For the online account settings, see the Windows 11 section on “Privacy Dashboard” directly above. Many of these services are handy—and if you know you want to use them, then just be aware that you may be sharing data. For anything you are not using or are not sure if you’re using, turn data sharing off. You can always come back and change the setting later.

Computer Settings

1. On your computer, search for just generic “settings” and open the Settings app. Click the “Privacy” at the bottom right (Figure 10-6).

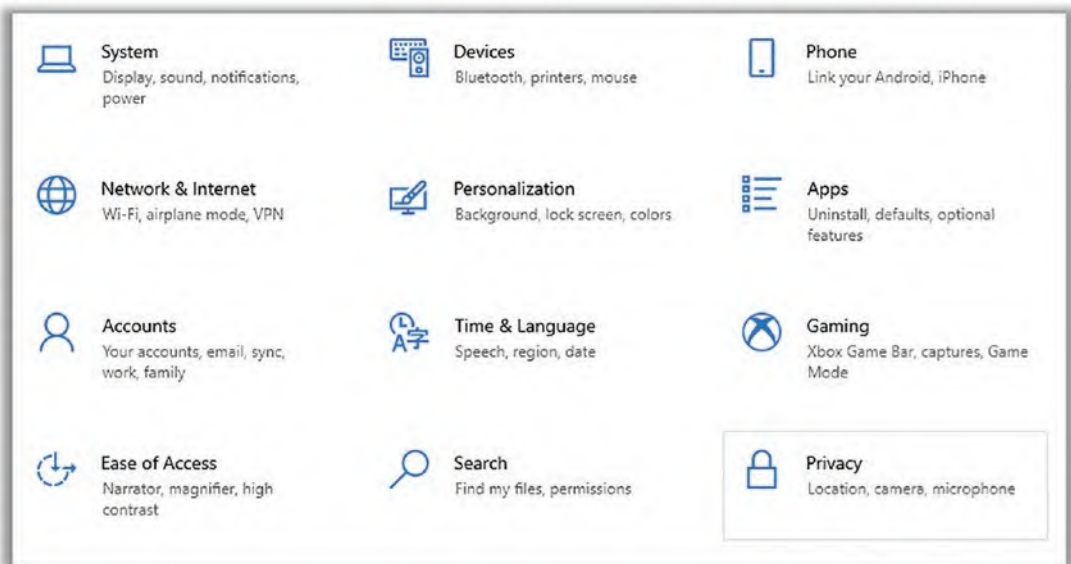


Figure 10-6. Windows 10 Privacy & Security settings

2. Under the General section, I would turn off everything except maybe “Let websites provide locally relevant content.” This would limit search results to English sites, for example (Figure 10-7). This probably only affects their Edge browser, anyway (and you’re using Firefox, right?).

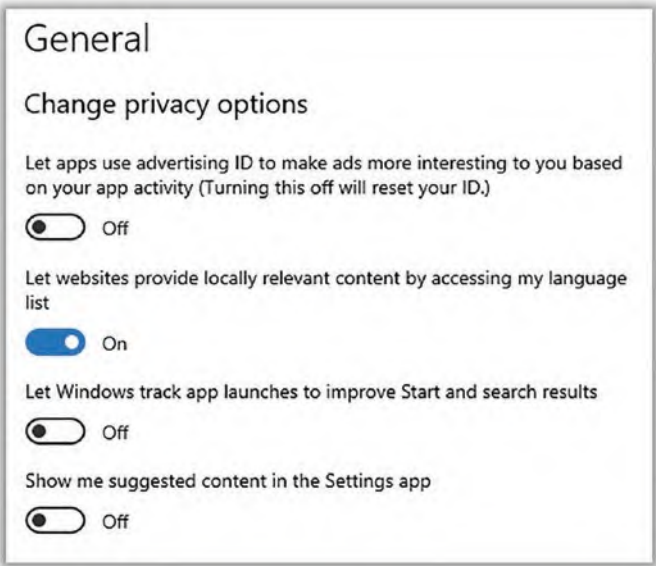


Figure 10-7. Windows 10 General privacy settings

- 3. Now (for some dumb reason) you have to go to a Under the “Diagnostics & Feedback” tab, only send the “required” diagnostics (Figure 10-8).

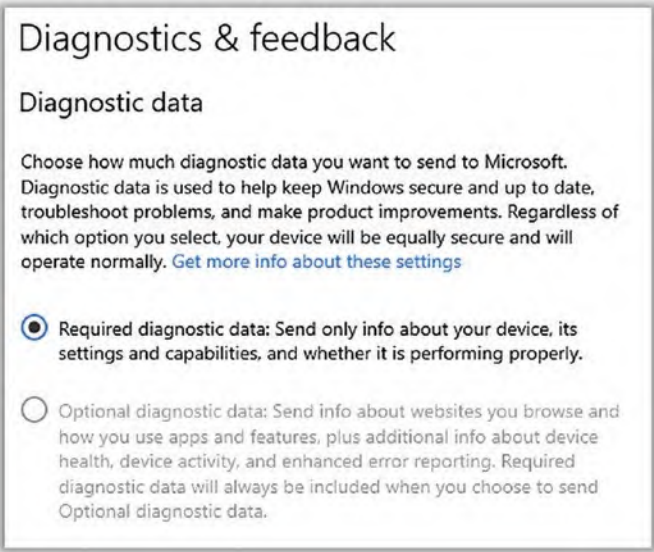


Figure 10-8. Windows 10 Diagnostics & feedback

4. Scroll down a bit and disable “Tailored experiences” (Figure 10-9).

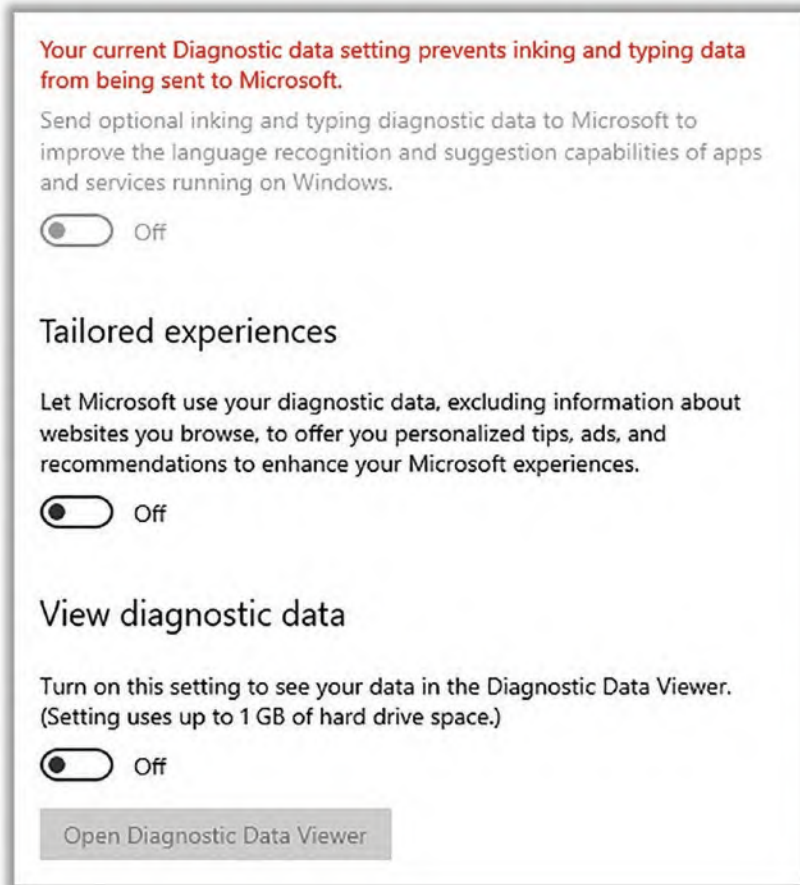


Figure 10-9. *Windows 10 Tailored experiences*

5. And now for the fun one: app permissions. There are a gazillion settings here, but at least they’re organized better than on Windows 10. Scroll on the left to the “App permissions” section. Click each category to see what apps have which permissions and revoke any that aren’t absolutely necessary. One example is shown in Figure 10-10. Note that (as the red warning states) you’ll need to log in to your Windows admin account to change some of these settings—and when you do, it will apply to all accounts on this machine.

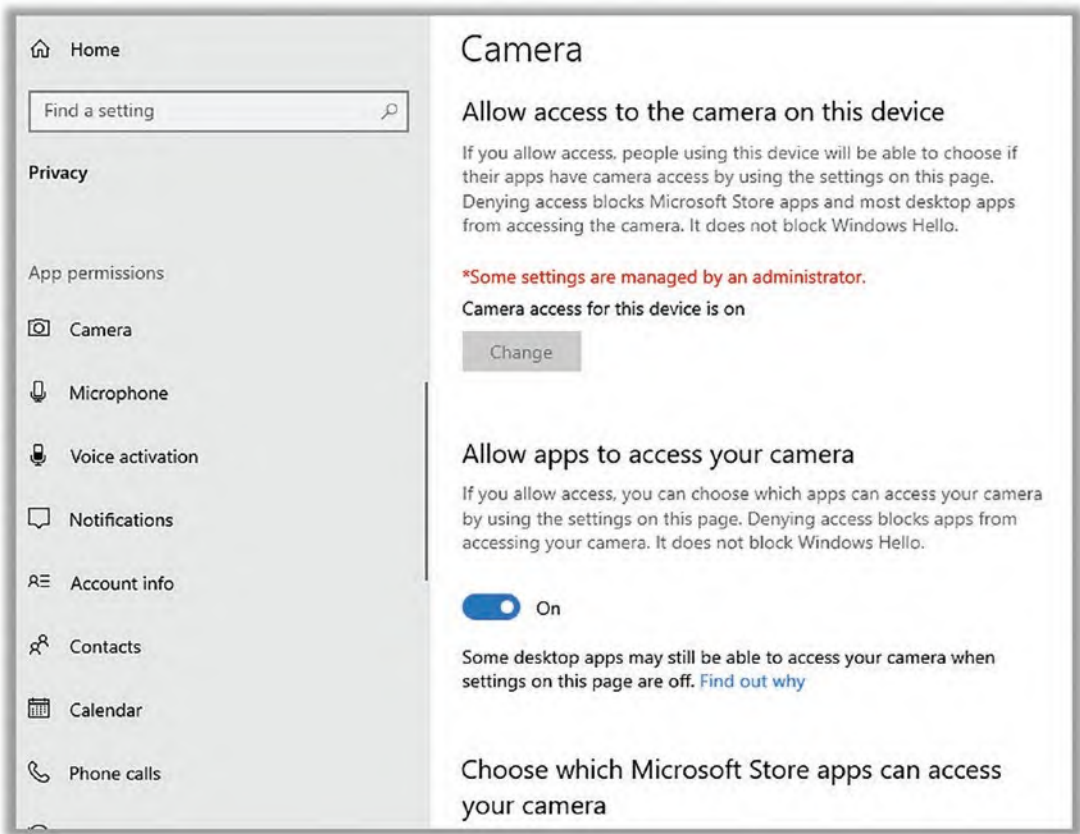


Figure 10-10. *Windows 11 Apps & features*

6. Now you need to review your Microsoft online account privacy settings. See the “Privacy Dashboard” part of the Windows 11 section prior to this one.

Tip 10-1c. macOS Ventura

There are two areas you’ll want to check: your iCloud settings and your Security & Privacy settings. To control what information is stored in iCloud, you need to go to the iCloud settings. The more you sync or put in iCloud, the more Apple knows about you: it’s that simple. That said, these are handy services, particularly if you have multiple Apple devices. Despite being a privacy nut, I sync my contacts, notes, and reminders through iCloud because I have many devices, and I like having them stay in sync automatically (and because I trust Apple a lot more than I trust Google or Microsoft).

1. Go to System Settings and click the “Apple ID” button at the very top of the left list, the one with your avatar image. Then select iCloud at the right (Figure 10-11). You will then see several options for services to sync or back up in iCloud. You’ll want to make your own choices for each of these, but here are some specific things to consider.

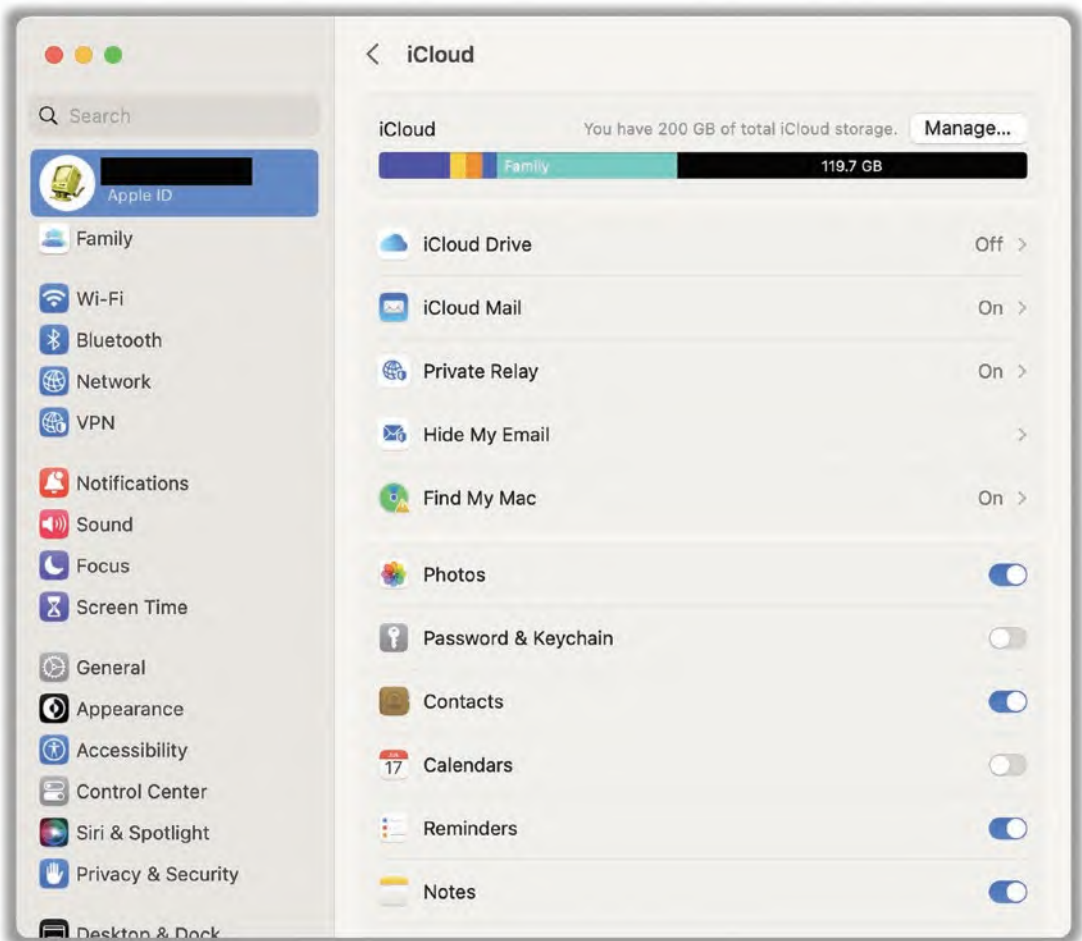


Figure 10-11. *macOS Ventura iCloud settings*

2. You will then see several options for services to sync or back up in iCloud. You'll want to make your own choices for each of these, but here are some specific things to consider:
 - *iCloud Drive* is Apple's built-in cloud storage service, like Dropbox but with more Apple-centric features. Apple pushes you to use this *constantly*, which is annoying. And the amount of free space they give you (5GB) won't cover much. But for \$0.99 per month, you can get a lot more (50GB). Just realize that currently anything you back up this way is accessible to Apple—you can't encrypt this with your own password (yet).
 - *Private Relay* is a great privacy tool, but so far it only works for Apple's Safari browser. You can learn more here: <https://support.apple.com/en-us/HT212614>
 - *Hide My Email* is an email aliasing service from Apple. It works well, but I personally prefer solutions like the ones I mentioned in Tip 9-8.
 - I would disable Keychain backup to iCloud. You have a password manager for managing your passwords. While this can be convenient because it's built into all of Apple's products, it's currently not as secure as BitWarden. (This may change with time. Apple is becoming very serious about its security and privacy.)
 - If you have a laptop (MacBook), I strongly encourage you to enable Find My Mac. It's less useful for desktop computers that never leave the confines of your home, but if you're at all worried about your computer being stolen, you should enable this feature that can help you find it.
 - You need to decide how much information you want to put into iCloud. Look at the other settings here and disable anything you don't need to synchronize with other Apple devices.

3. Next open Security & Privacy settings under System Preferences (Figure 10-12).

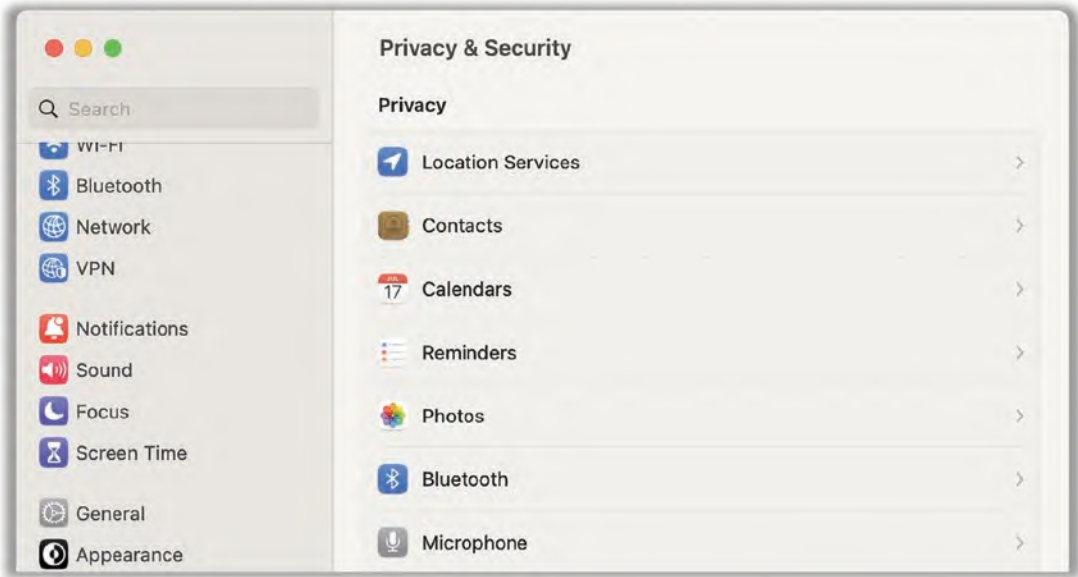


Figure 10-12. *macOS Ventura Security & Privacy settings*

4. If necessary, unlock the settings by clicking the padlock at the lower left. There are several settings here. The basic idea is that you want to limit access to potentially private things to only those applications that truly need it. When in doubt, turn it off—you can always turn it back on. The important ones to restrict for privacy are location, photos, microphone, camera, contacts, and calendar.

To learn more about Apple's privacy settings, you can go to <https://privacy.apple.com>.

Tip 10-1d. macOS Monterey

There are two areas you'll want to check: your iCloud settings and your Security & Privacy settings. To control what information is stored in iCloud, you need to go to the iCloud settings. The more you sync or put in iCloud, the more Apple knows about you: it's that simple. That said, these are handy services, particularly if you have multiple Apple devices. Despite being a privacy nut, I sync my contacts, notes, and reminders through iCloud because I have many devices, and I like having them stay in sync automatically (and because I trust Apple a lot more than I trust Google or Microsoft).

1. Go to System Preferences and find your iCloud settings. Click the "Apple ID" button at the very top right (Figure 10-13).

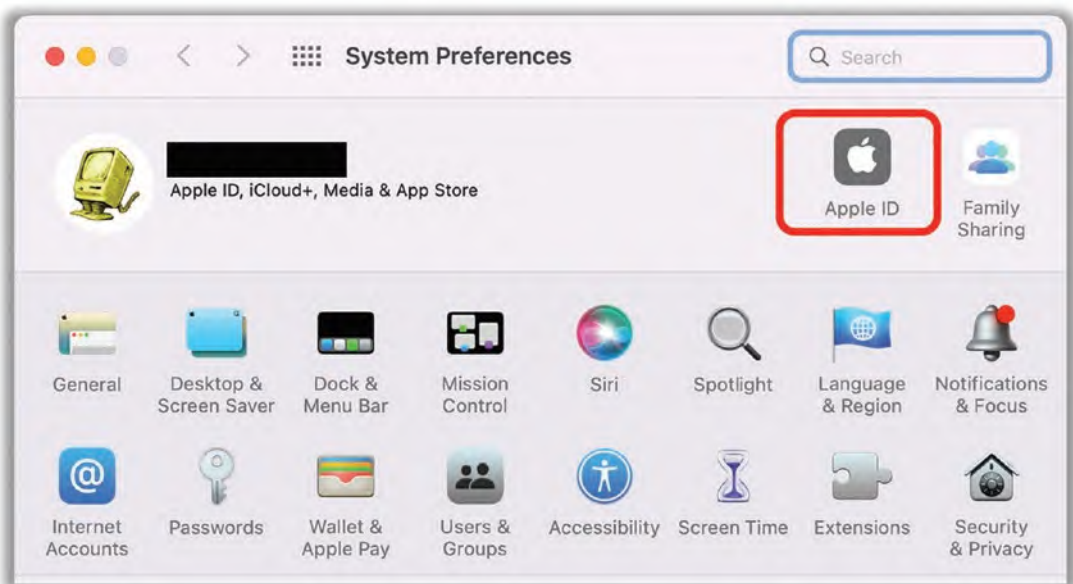


Figure 10-13. macOS Monterey System Preferences, Apple ID

2. From the Apple ID settings, click iCloud at the left. You will then see several options for services to sync or back up in iCloud (Figure 10-14).

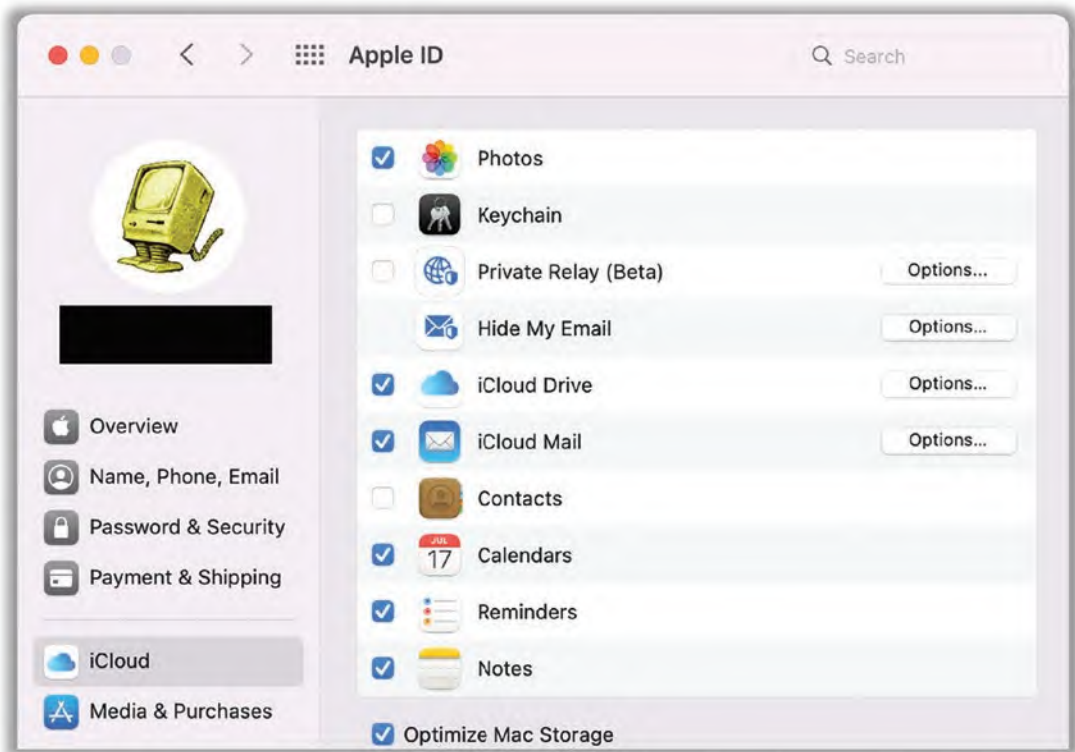


Figure 10-14. macOS Monterey iCloud settings

3. You'll want to make your own choices for each of these, but here are some specific things to consider:
 - *iCloud Drive* is Apple's built-in cloud storage service, like Dropbox but with more Apple-centric features. Apple pushes you to use this *constantly*, which is annoying. And the amount of free space they give you (5GB) won't cover much. But for \$0.99 per month, you can get a lot more (50GB). Just realize that currently anything you back up this way is accessible to Apple—you can't encrypt this with your own password (yet).

- *Private Relay* is a great privacy tool, but so far it only works for Apple's Safari browser. You can learn more here: <https://support.apple.com/en-us/HT212614>.
- *Hide My Email* is an email aliasing service from Apple. It works well, but I personally prefer solutions like the ones I mentioned in Tip 9-8.
- I would disable Keychain backup to iCloud. You have a password manager for managing your passwords. While this can be convenient because it's built into all of Apple's products, it's currently not as secure as BitWarden. (This may change with time. Apple is becoming very serious about its security and privacy.)
- If you have a laptop (MacBook), I strongly encourage you to enable Find My Mac. It's less useful for desktop computers that never leave the confines of your home, but if you're at all worried about your computer being stolen, you should enable this feature that can help you find it.
- You need to decide how much information you want to put into iCloud. Look at the other settings here and disable anything you don't need to synchronize with other Apple devices.

4. Next open Security & Privacy settings under System Preferences (Figure 10-15).

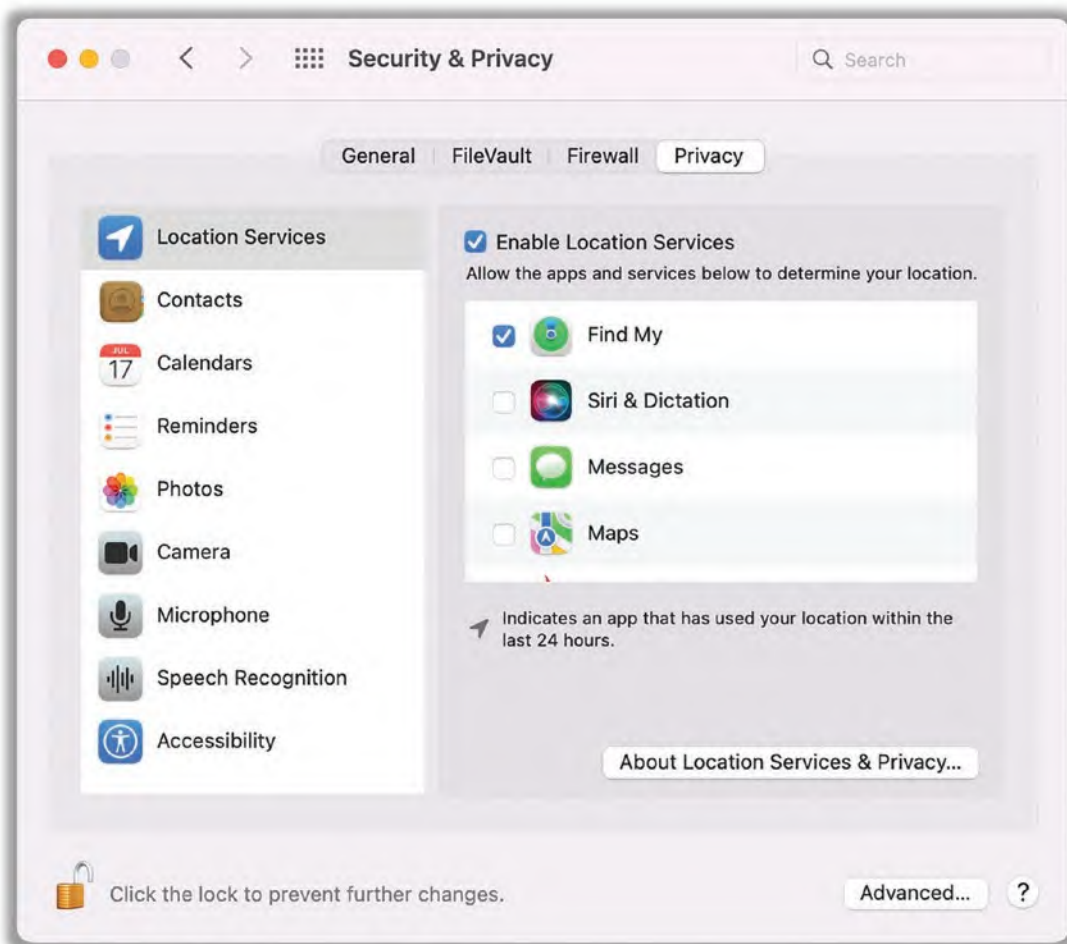


Figure 10-15. macOS Monterey Security & Privacy settings

5. If necessary, unlock the settings by clicking the padlock at the lower left. There are several settings here. The basic idea is that you want to limit access to potentially private things to only those applications that truly need it. When in doubt, turn it off—you can always turn it back on. The important ones to restrict for privacy are location, photos, microphone, camera, contacts, and calendar.

To learn more about Apple's privacy settings, you can go to <https://privacy.apple.com>.

Tip 10-2. ★ Enable Two-Factor Auth Wherever You Can

You might not think that locking down your social media accounts is that important, but it's almost as important as locking down your email and financial accounts. Hackers with access to your account can pretend to be you—and in a virtual sense, anyone who can log in to your accounts is you. They can send notes to your friends asking for emergency money. They can send them links to infected websites. They can even lock you out by changing your password. Enabling two-factor authentication is a great way to significantly reduce that risk. Use your favorite search engine to search for “two-factor authentication <service>,” where <service> is whatever service you're using. Many offer it now. This handy website can help you find the sites that do:

<https://2fa.directory>

Note that if you have the option of using an authenticator app (like Google Authenticator and Authy) or using a text message (SMS), you should definitely use the authenticator app. Text messaging isn't as secure as it should be. It's better than nothing, however; so if that's your only option, take it—and when they inevitably offer the time-based authenticator app option, switch to this method.

We already set up Authy for BitWarden in Chapter 5 (Tip 5-5). Setting up 2FA for other accounts is very similar. Log in to the account for which you want to set up 2FA using a web browser on a desktop computer. Look in your profile or settings for “security,” and if they offer two-factor authentication, you should find it there.

Tip 10-3. ★ Use Credit Cards Online (Not Debit Cards)

Quite simply, if someone charges something to your credit card without your permission, you're not actually out any money—the credit card company is. As long as you report the fraudulent charge in a timely manner, you won't be responsible for the charge. With debit cards, that money is actually gone from your bank account, and you then have to fight to get it back. So, whenever you shop online (or over the phone), use a credit card.

Tip 10-4. Use Virtual Credit Card Numbers

Some credit cards offer a one-time-use “virtual” credit card number—it's an alias for your actual credit card. This is a great option for buying something online from a store that you will probably never do business with again. This is usually done online, through

your credit card account website, but it can be hard to find—call the number on the back of your card and ask about this service. This service will generate a throwaway 16-digit credit card number that will work only one time. It comes with its own expiration date, security code, and everything. The charge will show up on your regular bill. Just be sure to save that temporary card info until you’ve received the merchandise, in case you need to return it or something (and need to be able to give them information about the card you bought it with).

The Capital One service, Eno, allows you to create cards that act as aliases for your real credit card. Unlike single-use virtual numbers, you assign these cards to a particular merchant. This has at least two benefits. First, if that company is hacked, the card info will be useless to the hacker—it works only for that vendor. Second, if your real card is ever lost or stolen, these alias cards will not be affected. They will still be tied to your account and will be associated with your new credit card number.

The Apple credit card (Apple Card) offers a lot more privacy than your average credit card. You need to realize that Visa, Mastercard, and others are keeping track of everything you buy and using it for their own purposes as well as selling it in some supposedly anonymous form to third parties. Apple doesn’t share or sell any of this, except with Goldman Sachs (the bank backing the card)—and supposedly they don’t allow Goldman Sachs to sell or share it, either (outside of Goldman Sachs). If you couple it with Apple Pay, it adds even more layers of privacy with randomly generated card numbers and limiting access to cardholder information.

And finally, there’s a company called (tantalizingly enough) Privacy.com that runs another anonymizing, virtual credit card service. The number of features is truly amazing, but the basic service is about creating virtual credit cards that are tied to your bank account through a debit card.

Tip 10-5. Be Careful Using Mobile Payment Services

There are several mobile payment services today, including Venmo, Google Pay, Apple Pay, PayPal, Zelle, and Cash App. They all do basically the same thing: let you give money to someone else. This could be a person you know, a street vendor, a contractor working on your house, or really just about anyone. Like text messenger apps, both you and the recipient need to use the same service for this to work.

While most of these apps are secure, they're not very private—with the possible exception of Apple Pay (and Apple Cash). Venmo in particular is horrible about privacy. If you insist on using Venmo, then check this article for ways to make it more private:

<https://www.eff.org/deeplinks/2021/06/victory-you-can-now-make-your-venmo-friends-list-private-heres-how>

Treat mobile payments just like cash—once you've sent money to someone, it's gone. To get it back, they'll have to agree to it. That means that you need to be very careful not to make mistakes when entering the recipient information. Don't blindly trust QR codes for sending money, either—clever bad guys have covered real QR codes with their own stickers. If you're going to send a large amount of money, try sending a much smaller amount first—like even just a dollar. Make sure you have the connection working before sending the full amount.

Tip 10-6. Give Your Credit Card Company a Heads-Up

Because credit card companies are ultimately the ones on the hook for illicit purchases, they have implemented all sorts of automatic antifraud protections. Their computers are well aware of where you live and what sorts of things you typically buy. If you suddenly buy something in a foreign country or make a large purchase from an online store, they may turn off the card until they can talk to you and verify that the charges were legit.

To avoid this, you can give them a call ahead of time to let them know you'll be traveling abroad or will be buying something expensive from a place you don't normally shop. Some sites have a "travel notice" form on their websites, too, which you can find under your account online. If your bank has your cell number or email address, and you give them permission, they will text or email you when you have suspicious charges, giving you a chance to validate the purpose before they disable your card.

Tip 10-7. Set Up Restrictions on Your Financial Accounts

Services such as overdraft protection, fund transfers, and linked accounts can be convenient. However, you need to think about what someone else could do if they were to somehow gain access to your checkbook, ATM card, or debit card. Anything you can do with it, they can also do. Don't link two accounts unless you really need to (like with overdraft protection).

Also, if possible, put limits on daily withdrawal and transfer amounts. If you need to, you should always be able to go into your bank branch if you need to exceed these limits—but at least in that case you will deal with a human that can verify your identity.

Tip 10-8. Turn On Account Alerts

Many online banks, credit card companies, and financial firms have ways to create alerts on various types of account activity including being able to set trigger levels. For example, you can be alerted whenever someone withdraws more than \$200 from an ATM or charges more than \$300 on your credit card in one day. These are really fantastic ways to keep tabs on your accounts. I highly recommend that you use them.

Tip 10-9. ★ Freeze Your Credit

The most potent way to prevent an identity thief from opening a new line of credit in your name and sticking you with the bill is to freeze your credit at the big credit bureaus. When you freeze your credit, you prevent banks, lenders, credit card companies, employers, and really anyone from obtaining your credit record or opening new credit. This effectively prevents anyone from getting a credit card or loan or bank account in your name (including yourself). If you need to do anything that requires a credit check, you will need to find out which credit bureau will be used and temporarily “thaw” your account. Thanks to recent legislation, this process is now completely free (as it should be). You will have to individually contact each agency.

If you know you will be needing to access your credit report frequently (making the freeze/thaw process too painful), you might instead set a fraud alert on your account. This will require that they contact you before opening any new credit lines in your name. This is also free but will expire after a year. You only need to contact one of the agencies for this—that agency will contact the others for you. (And because the credit bureaus make money on each credit request, they will often try to convince you to use a fraud alert instead of a full freeze. Don’t let them talk you out of it—if you can handle a full freeze, do it.)

You can freeze your credit online using the following links. Innovis is a newer credit bureau but getting more popular.

- Equifax: <https://www.equifax.com/personal/credit-report-services/credit-freeze/>
- Experian: <https://www.experian.com/freeze/center.html>
- TransUnion: <https://www.transunion.com/credit-freeze>
- Innovis: <https://www.innovis.com/securityFreeze/index>

Equifax operates a totally different database of employment and salary information called the Work Number. They work with many employers to actually record your paycheck information and employment history. Originally, this information could be accessed online by providing a social security number and date of birth, but when exposed by KrebsOnSecurity, this portal was shut down. You can opt out of this collection, but it's tricky to do. The following article will give you more info and help you through the process:

<https://krebsonsecurity.com/2017/11/how-to-opt-out-of-equifax-revealing-your-salary-history>

Tip 10-10. ★ Plant Your Flag

There are several organizations with which most adults will automatically have an account: governmental (local and federal), utility companies (including internet service providers), banks, credit bureaus and retirement investment firms. Even if you never intend on interacting with these accounts online, you should establish and claim those accounts before the bad guys do. Below is a sample list of accounts you should claim, but think carefully about other accounts you may have along these lines.

- Social security or social insurance
- Taxes (e.g., IRS)
- Banks
- Investment firms (e.g., retirement accounts)
- Postal service (yes, you have an account there)

- Bureau/Department of motor vehicles
- Utility companies (electric, gas, water, waste, internet)
- Credit bureaus

Tip 10-11. Use Private Cloud Storage Services

Cloud storage providers like DropBox, OneDrive, iCloud, and Google Drive will encrypt your data, but they also hold the keys. Therefore, it's possible for your data to be viewed by employees, hackers, or legal authorities. And you should assume that your data could be saved forever (even if you delete it).

I reviewed many different cloud storage providers, looking for a reputable company that gave you full control over your file encryption. The winner to me was pretty clear: Sync.com. (It's highly regarded by other privacy sites, as well.) Your files are encrypted before they leave your machine using a password you choose (note that this is an optional feature—you have to specify this explicitly). Since the files are encrypted using a key only you have, Sync.com has no way to decrypt them.

<https://www.sync.com>

If for some reason this service doesn't appeal to you, you can also look at Proton Drive or pCloud.

With any service like this that uses proprietary software, you still have to trust that they're doing what they say they're doing. Unless the software is open source, it's hard to verify this. However, you can add this private encryption to *any* cloud storage service by using Cryptomator. This application allows you to create "vault" folders that are encrypted locally using your own key. It's like putting a safe inside a public storage locker. And the software is open source and has been audited by security experts.

<https://cryptomator.org>

This tool can also be used to create encrypted vault folders on your computer, as well (i.e., you're not limited to cloud storage folders).

Tip 10-12. Don't Broadcast Your Travel Plans

While it's good to give your credit card company a heads-up on travel, you shouldn't be broadcasting this information on Facebook or Twitter or any other social media (at least not as a public post). Criminals have been known to monitor social media sites looking for people who will be away from home for extended periods of time. You should also refrain from posting vacation pictures during your vacation to a public location, as well. Post them to a private service or just post them when you get home.

Similarly, you should never post pictures of your airline tickets or boarding passes online. Be careful how you dispose of paper boarding passes and any airline-printed luggage tags, even after your flight. These codes can contain things like your name, frequent flier number, record locator number, and other personally identifiable information. This information could be used to alter or even cancel your next flight or be used to gain access to your frequent flier account, among other things.

Tip 10-13. Read the Terms of Service (or Not)

How many times have you actually read the entire terms of service or the end-user license agreement (EULA) before signing up for some online service or installing an application on your phone or computer? No one does. We just check the box that said we read it and click Accept. Sadly, even if you did read it, you probably wouldn't learn much. The use of legalese and pleasant-sounding euphemisms makes it really hard to truly understand what you're agreeing to. I encourage you to try it, though—go read Facebook's or Google's or LinkedIn's privacy policy, from top to bottom.¹² See if you can figure out what data they collect and who they share it with.

On the Internet, there's a term for an executive summary: TL;DR, which is short for "too long; didn't read." There's a website called "Terms of Service; Didn't Read" that attempts to sort through these arcane privacy policies and distill them to quick bullet points. You might give that a look before you click Accept next time.

<https://tosdr.org>

¹² The website Visual Capitalist has a great infographic showing just how long these terms are. They say that Microsoft's terms of service would take as long to read as *Macbeth*: <https://www.visualcapitalist.com/terms-of-service-visualizing-the-length-of-internet-agreements>

Tip 10-14. Review Social Media Privacy Settings

It would take an entire book to tell you how to properly lock down all the social media sites, and it would be obsolete the second it was published. There are so many different settings, and they change constantly. But by default, most of the social media sites are configured to be very public. After all, it's in their best interest to maximize the number of connections and followers you have. But you should reduce the amount of information you share with your social media services as much as possible. You should also make sure that your social media posts are as restricted in scope as you can stand. Don't post for the entire world—post only to a limited group of friends and family. If possible, set your posts to expire after a reasonable amount of time.

The following links will help get you started. Most of these links are directly from the source because I want to make sure they're always up to date. However, I also strongly suggest doing a web search for "<service> privacy settings" to get third-party articles on how to properly lock down these accounts.

- Facebook: <https://www.facebook.com/help/238318146535333/>
- Instagram: <https://help.instagram.com/196883487377501/>
- Twitter: <https://help.twitter.com/en/safety-and-security/control-your-twitter-experience>
- LinkedIn: <https://www.linkedin.com/help/linkedin/answer/66/managing-your-account-and-privacy-settings-overview>
- Yahoo: <https://yahoo.mydashboard.oath.com/>
- Pinterest: <https://help.pinterest.com/en/article/edit-account-privacy>
- Google: <https://policies.google.com/technologies/product-privacy>

Here are a couple other sites that have a ton of great social media privacy resources:

- <https://staysafeonline.org/resources/manage-your-privacy-settings/>
- <https://www.internetmatters.org/parental-controls/social-media/>

Tip 10-15. Don't Share Your Email Credentials

Many social media sites offer to help you find friends by looking at your email contact lists. To do that, they just need your email ID and password. Don't worry; we won't use it for anything else, really! *Don't do it.* Just don't. You would not only be giving them access to all of your email contacts but all your emails, as well...forever (or until you change your password). On Google, it's even worse—your email account password is also the password for Google Docs, Google Calendar, and dozens of other Google services.

Some social media services might have a slightly different “log in with” sort of option, where you don't directly give away your password for the linked-to service but instead “authorize” the two services to share information. This is marginally safer—you can often decide what information you want to share, and you can revoke this sharing later without having to change your password. But I would still not allow these services to share any information at all.

Note that Facebook has a tool to help you delete your email and phone number that was posted by someone else (probably in a manner similar to the above)—even for people who don't have a Facebook account. This was probably created in response to GDPR.

<https://www.facebook.com/contacts/removal>

Tip 10-16. Don't Sign In Using Facebook, Google

You'll see many websites offer to let you sign in using your Google or Facebook account instead of setting up a new, dedicated account for the site. Sure, this is convenient (and should actually be secure), but it means that you're allowing Google or Facebook to track you on these sites and share information with the website in question. Since you have a kick-butt password manager, it's no big deal to set up a dedicated account on each of these sites with unique passwords.

Note that Sign In with Apple is actually private. Apple created this service explicitly to provide a privacy-respecting alternative to the Google and Facebook authentication services. In fact, with the Apple version, you can even hide your real email address—Apple gives you the option to create a new email alias on the fly.

You can read more here: <https://firewallsdontstopdragons.com/stop-using-sign-in-with/>.

Tip 10-17. Stop Tagging Other People in Photos

Facial recognition is fascinating from a technological perspective. Today's high-definition cameras and powerful computers make this feature quite easy to implement and deploy. Social media services use it to try to identify people in the pictures you upload. By now you should know that the reason they're doing this is to figure out who your friends and family are and who else you might know or hang around with. This builds a social graph that is extremely valuable for learning more about you and the people in your photos. They give you tools to identify or "tag" the people in your photos or others in your news feed, maybe even prompting you to do so. Don't help them add to their massive profiles they've built about us.

Tip 10-18. Scrub File Metadata Before Sharing

Files today can come with a lot of hidden data embedded in them—data about the data, which we called metadata. This can be your name, address, GPS location, camera settings, and much, much more. This data is very helpful to you and your applications that read these files but can also be valuable to marketing companies and people who may wish to take your money or even stalk you.

Photos contain a ton of info called EXIF (Exchange Image File format) data. If you upload pictures of your kids at the local park or at their school or friend's house, those pictures contain the date, time, and GPS location. You might not want to be sharing those online.

Microsoft Office files and PDF files are also known for containing a lot of metadata, including your full name and even contact information.

So, before you share a file, you should scrub out any private metadata. While some social media sites will automatically do this for you, I wouldn't count on it. And of course, there's nothing to prevent them from storing off this information for their own purposes, even if they keep others from seeing it.

You can usually see this information by looking at a file's "properties." How you do this will depend on your operating system and the type of file you're viewing.

Tip 10-18a. Windows

To view and remove metadata from most Windows files, do the following:

1. Open Windows Explorer to find the file you want to inspect.
2. Right click the file and choose “Properties.”
3. Select the Details tab to review the metadata.
4. To delete metadata, you can click “Remove Properties and Personal Information” link at the bottom of that window.
5. When you click this, you’ll be given the option to create a new file without the metadata or to just strip it from the original.

Tip 10-18b. macOS

Sadly, there isn’t a simple way to remove metadata on a Mac like there is on Windows. To remove metadata from most photo formats as well as PDF files, you can try one of these two free applications:

- <https://exifcleaner.com>
- <https://imageoptim.com>

You can also try right-clicking a file and selecting “Get Info” to view its metadata, even if you can’t remove it this way.

Tip 10-19. Stop Oversharing Personal Information

This is a tough one. For whatever reason, people love to overshare on sites like Facebook, Twitter, Pinterest, and Instagram. But just remember that this information lasts forever and could be seen by anyone, despite any restrictions you try to put on your account or whatever privacy policy the social media site claims to follow. When you forget your password, how do you recover it? Most sites will ask you to answer three questions that supposedly only you would know the answer to. Where did you go to college? What’s your mother’s maiden name? What’s the name of your first pet or car? This is precisely the sort of information people post on social media. This information can also be used to impersonate you on the phone, as well.

For financial, medical, insurance, and other important accounts, you will often have to give them complete and valid information. However, when signing up for unimportant online accounts—like any account you could just replace with a new account—you should give them as little information as possible. You can even lie, as long as you don't do this explicitly to commit fraud. Instead of signing up with your full name, say Jane Smith, try just using Jane S. Instead of giving your correct birthday, just give them something close enough. For child accounts, which often enable parental controls and age-based content, you can give a date that's closer to the actual birth date. Don't give them your full address, if you can help it. Often a ZIP code is sufficient, unless they need to ship you something.

Tip 10-20. Close Accounts You Don't Use

If you're no longer using a social media service, you should delete your account. Many of them will try to talk you into just deactivating your account, but that doesn't protect your privacy because they'll still have all your data, which may contain information about many other people, too. Remember that your data overlaps other people's data, too.

The one reason you might not want to fully delete your account is if someone else might try to reuse your username or handle for nefarious purposes. Once your account is deleted, your account ID will eventually be available for someone else to use. If this is a concern, then you can just deactivate the account instead of deleting it. You might want to delete all of your data, though.

Here are some links to get you started:

- Facebook: <https://www.facebook.com/help/224562897555674>
- Instagram: <https://help.instagram.com/448136995230186>
- Twitter: <https://support.twitter.com/articles/15358-deactivating-your-account#>
 - Note that with Twitter, you have to start by deactivating your account. After 30 days, your account should be fully deleted.
- LinkedIn: <https://www.linkedin.com/help/linkedin/answer/63/close-your-linkedin-account>
- Yahoo: <https://help.yahoo.com/kb/SLN2044.html>

- Pinterest: <https://help.pinterest.com/en/article/deactivate-or-close-your-account>
- Google: <https://support.google.com/accounts/answer/32046>

You should also go back and delete/close any other old online accounts you no longer use. You may forget about them, but your data is still there, waiting to be abused or stolen. If you've been using a password manager long enough, you can look through all your saved passwords to find old accounts. If you've had an email account for a long time, you may be able to search your emails for "welcome" messages or "verify your account" requests. Or you could check out the site Just Delete Me to help jog your memory (and get help deleting your account):

<https://backgroundchecks.org/justdeleteme>

Here's one more pro tip. I wouldn't trust these companies to delete your data fully. So you might want to clean house before you delete your account—poison the well, so to speak. Remove any profile information you can or even change it for incorrect information.

Tip 10-21. Delete Your Facebook History

Facebook recently provided a tool to delete some or all of your activity history. Until this point, your only option was to delete your entire account. Now you have a new Manage Activity tool that will let you selectively archive or trash old posts and pictures in bulk.

<https://www.facebook.com/help/289066827791446>

Tip 10-22. Avoid DNA Heritage Services

DNA ancestry/heritage kits like those from Ancestry.com, 23andme, and My Heritage have truly enticing services. As an amateur genealogist and family history buff, I understand the appeal. But your DNA is literally you—it's hard to find something more personal. And even if that doesn't bother you, you need to realize that you are also giving away the DNA of your blood relatives, too. These DNA services have revealed past infidelities and led law enforcement to arrest people related to others who are genetically related. DNA data, if stolen or abused, could also potentially be used to affect your health insurance rates or enable identity theft. Also, it was revealed that 23andMe intends to

use your DNA for drug research¹³. While I believe these companies are trying to address these privacy concerns, there's no privacy policy in the world that would make me feel comfortable giving my DNA to a for-profit company. States are scrambling to enact privacy laws around DNA, but we don't have anything yet.

Tip 10-23. Account Recovery Questions: Lie

Since password and account recovery is often accomplished by providing the answer to a few simple questions, why not protect your accounts by simply providing the wrong answers? Nothing says you have to answer these questions truthfully. You just need to be able to faithfully provide the same answers when asked again later. Whoever is trying to hack your account will be trying to give the right answer, and they can't possibly succeed if you lied.

One method would be to alter the real answers in some predictable way. Most of these questions have one-word answers, so just find some method for modifying the answer that only you know. Maybe prefix each answer word with not or some other prefix. Or repeat the word twice, or even just the first letter.

For example, let's say the security question is "What was your mother's maiden name?" If the real answer is Brown, here are some simple, easy-to-remember transformations you can use:

- *NOTBrown*: Prefix every answer with "NOT."
- *nworB*: Write the answer backward.
- *BrownBrown*: Repeat the answer.
- *BBrown*: Repeat the first letter.

If you really want to kick it up a notch, use your password manager to generate totally random answers to these questions—use the password generator. (You may need to disable special characters.)

¹³ <https://leaps.org/23andme-is-using-customers-genetic-data-to-develop-drugs-is-this-brilliant-or-dubious/>

However you lie, be sure to save your false answers in your password manager so you can faithfully recall your lies later when you need them. I would probably save them in the “Notes” section of the website’s vault entry or, if necessary, create a new secure note just for these answers.

Tip 10-24. De-Google Your Life

Google’s free email, calendar, and docs apps are really amazingly powerful and easy to use. I was an early adopter when they came on the scene many years ago. But over the years, Google has decided to mine this treasure trove for personal data, and so now you might be wanting to find some alternatives that will respect your privacy.

Google has an amazing number of free apps and services, including some you may not realize are owned by Google, like Waze, YouTube, and Android. I wrote a whole series of articles on how to replace these services with privacy-respecting alternatives:

<https://firewallsdontstopdragons.com/reducing-my-google-footprint/>

The Restore Privacy website has a lot of wonderful options, as well:

<https://restoreprivacy.com/google-alternatives>

Tip 10-25. Avoid TikTok Entirely

In case you’ve been living under a rock, TikTok is a Chinese social media platform for sharing short videos and other stuff. While most social media platforms are privacy nightmares, TikTok appears to be operating at a whole new level—reportedly stealing tons of user data without proper permission, including “draft” videos that were never officially posted.¹⁴ In June 2020, a class action suit was proposed in a California court to address these claims. Things have only gotten more concerning since then, believed by many people on both sides of the political spectrum to be a national security risk¹⁵.

It’s possible the company will address some of these issues, but their track record is extremely shady and I could never trust it, personally.

¹⁴ <https://www.cnet.com/news/tiktok-accused-of-secretly-gathering-user-data-and-sending-it-to-china>

¹⁵ <https://www.wired.com/story/tiktok-national-security-threat-why/>

CHAPTER 11

Watch over the Lads and Lasses

So far, we've been focused on cybersecurity and privacy for adults. If you're a parent, grandparent, or educator, this chapter will help you understand how to better protect the kids in your care.

The Internet Is Everywhere

I'll tell you right off the bat that this was probably the hardest chapter in the book for me to write. Why? While I'm perfectly comfortable giving you advice adult to adult, it feels like lecturing as soon as I try to give you advice on what you should do for your children. I raised two girls myself, and I know that what makes sense for my kids may not make sense for yours. Every parent, every child, and every family's social dynamic is different. Obviously, what makes sense for adults doesn't always make sense for kids. But what makes sense for a given child can change drastically just a year or two later. So, it's important to realize that the suggestions in this chapter need to be carefully considered for each child individually and continually reconsidered as they grow older.

All the risks for adults that I discuss in this book apply to kids, as well. However, kids have a lot less maturity and life experience than adults do. Kids are very focused on the now and just don't have the context required to think more than a few days into the future. Furthermore, you are not likely to be there when they have to make a decision about what to do or not do. Access to the Internet is everywhere. Even if your particular child doesn't have a smartphone, you can bet that most of their friends do. According to a Common Sense Media study in late 2019,¹ 53 percent of kids have their own smartphone

¹<https://www.commonsensemedia.org/blog/tweens-teens-and-phones-what-our-2019-research-reveals>

by the time they hit 11 years old and up to 69 percent by age 12. Overall, 85 percent of teenagers have their own phones. They probably also have access to other Internet-connected devices: tablets, smart TVs, or set-top boxes like Apple TV or Fire TV. They can even browse the Web using an e-reader like a Kindle. If it has a place to enter a Wi-Fi password, then it can connect to the Internet.

So, while you can certainly take some measured precautions and set reasonable limits on the things you can control, you just have to realize that Internet access today is everywhere. You simply cannot keep your kids from it, unless you want to move away from civilization (in which case you don't need this book).

As just one example, I heard my daughters talking several years ago about what someone had posted on their “finsta” account. I knew about Instagram, of course, but I had never heard of finsta. So, I asked what it was, and they casually explained that it's a fake Instagram account (as opposed to their “real” account, or “rinsta”). While the rinsta account is wide open and public, the finsta account is much more restricted—usually just very close friends. It's more popular with girls than boys, apparently, too. Was I worried? No, not really. I trusted my girls, but I also knew that at their ages, there wasn't much I could do to prevent things like this. The Internet is just a fact of modern-day life.

As I said before, most of the security and privacy recommendations in this book apply to people of any age, so in this chapter, I'm really just adding a few other thoughts to consider that apply specifically to children.

The Internet Is Forever

The Internet is everywhere...and the Internet is also forever. Anything that happens in cyberspace has the potential to remain there not just for the rest of your life but for as long as our race survives. Digital information doesn't decay and can be copied infinitely without degrading in quality one bit. (Get it? One *bit*?) Digital data just yearns to break free. Once you post that picture or send that message or upload that video, you should assume that one day it could be seen by someone you didn't intend to see it. And don't be fooled by any device or software manufacturer that claims they can lock this stuff down, preventing copying or transfer or whatever. Also, don't count on claims that messages will “self-destruct” or that you can delete messages after you send them. If it can be seen by the recipient, then it can be captured and shared with someone else. If you can manage to drill one thing into your kid's head about the Internet, this is it.

They should consider that anything they post on social media could someday be seen by college admissions officers, potential employers, and (eventually) their own kids. It's less likely that private messages will be made public, but especially when the recipients are also kids, I would assume that anything is possible.

This leads me to the *Grandmother Rule*:

Don't post anything online that you wouldn't gladly share with your grandmother.

I don't even have to explain that. Somehow Grandma is the gold standard on proper behavior. She just is. It's not quite WWGD (what would Grandma do) because Grandma likely doesn't have a finsta account. But tell your kids that if they would feel squeamish about showing something to Grandma, then they probably should reconsider doing it. Most laws in this country apply differently to minors, and much of your legal record may be expunged when you turn 18. That does not apply to Internet stuff. Once it's out there, you can't get it back.

Another important rule to teach your kids is not to overshare online. Personal information should stay personal. That includes full name, address, phone number, email addresses, and current location. Obviously, if they're speaking with a trusted friend or relative, this rule can be relaxed. I'm more talking about cases where they fill in forms, chat with online gamers, answer fun questionnaires, or post messages to social media. They should also be very careful about posting pictures that might include personal information in the background or other people who may not wish to have their pictures posted. Finally, this applies not just for their own personal information, but the personal information of others, as well.

Cyberbullying

One of the most amazing uses of the Internet is communication. With our smart devices and computers, we can send messages to dozens of people around the globe simultaneously and nearly instantaneously. We can have a face-to-face chat with anyone on the planet as if they were standing right in front of us. And we can share our thoughts on any subject at any time with friends as well as complete strangers. While the benefits are undeniable, this power comes with a dark side for our kids: cyberbullying.

As long as we've been a sentient species, there have been bullies—kids who take some sort of sick pleasure in harassing or embarrassing another child. But unlike traditional bullying, *cyberbullying* can happen anytime and anywhere. It's also possible for cyberbullies to act anonymously, making it hard to stop. Finally, as we've just established, it can be nigh impossible to erase this stuff from the Internet. Embarrassing pictures or hurtful messages can live forever.

The original rule of human society, the Golden Rule, applies in cyberspace just as it applies in real life: treat others the way you wish to be treated. The Internet can seem unreal to kids because it's not personal. Something you would never do or say to someone in person is somehow a lot easier to do with a web or phone app. So, tell your children to imagine that they're doing it in person...in front of their grandmother...and then see if it still feels right.

Big Brother for Little People

Thanks to repeated school shootings and the COVID pandemic, schools have significantly ramped up security protocols and forced remote students to install draconian proctoring tools. Many schools issue their students Google Chromebooks with lots of monitoring software preinstalled. I know that my daughter had to take a 360-degree video of her bedroom in high school before taking a remotely proctored exam, to make sure she didn't have people or materials handy for cheating. These proctoring programs record audio and video during the exam, as well as the laptop screen. Some of these systems even have special artificial intelligence software that raises a red flag if the test-taking student looks away from the screen too frequently².

While these new surveillance systems serve a purpose, the trade-off with regard to students' privacy can be severe, even if you assume that this monitoring is done properly and with full transparency (which it's often not).

But of course, these systems are created and used by human beings, and humans have flaws. Some of the companies who created the software have been spying on and collecting data about the students³. There have even been allegations of schools remotely enabling the webcams built into laptops to spy on kids at home⁴.

²<https://www.theverge.com/2021/1/28/22254631/university-of-illinois-urbana-champaign-proctorio-online-test-proctoring-privacy>

³<https://www.eff.org/wp/school-issued-devices-and-student-privacy>

⁴<https://www.publicschoolreview.com/blog/is-your-school-spying-on-your-child-via-webcams>

Surveillance technology isn't just popping up in schools, however. It's also showing up in daycare centers and summer camps. One such camp has an app for parents that lets them spy on their kids. The campers have to surrender their phones, but facial recognition software and a network of cameras notify their parents when their child's face comes into view⁵.

Kids have very few rights in these situations. Parents and privacy rights organizations have pushed back but have had limited success so far. As a parent (or teacher or administrator), you should know what sort of surveillance is being conducted, what data is being collected, who is collecting the data, who it's being shared with, how long it will be retained, and where to go if you need to express a concern. I'll have several resources in the checklist.

Porn and Predators

This is a tough one. The Internet is chock-full of adult content—from simple nudity to unbelievably graphic violence and pornography. There are some ways you can try to restrict their devices and your home network (and I'll discuss them in this chapter and the next), but the reality is that kids have many, many other ways to get on the Internet that you can't control. Your best approach here, in my view, is to have The Talk with your kids and include a discussion about the Internet. Encourage them to come to you with any questions they have and counsel them to use their best judgment. If you plan to set up technological restrictions on their phones and computers, explain that you're trying to protect them from seeing things you can't unsee and that there will be plenty of opportunity to explore these things when they're an adult and have the maturity to handle it.

Another online problem that gets a lot of attention is online child predators. For young kids, you need to be absolutely clear that they should not communicate with anyone online without first checking with you. For older kids, the rules can be a little more relaxed, but a good rule of thumb is that they should not communicate with anyone unless they have met them in person first.

⁵<https://www.washingtonpost.com/technology/2019/08/08/summer-camps-turn-facial-recognition-parents-demand-more-smiles-please/>

Don't Panic

I'm not trying to scare you. Like I said at the beginning of this book, any powerful tool can be used for good and for evil and everything in between. When all is said and done, the best thing you can do, for yourself and your children, is to get educated and stay involved. You can't let fear of a few bad actors cause you to deny your children the amazing benefits of a connected world and easy access to the collected knowledge of humanity. The balanced approach is to alert your children to the risks while preserving the sense of wonder and adventure that should accompany such a magnificent and powerful tool.

Summary

- Kids have all the same risks on the Internet as you do, but they don't have the same experience or maturity, which makes it harder for them to weigh the consequences of their actions.
- The Internet is forever. Don't do anything on the Internet that you wouldn't gladly do in front of your grandmother.
- Kids often don't understand what types of information are considered personal. Educate them on what things they should avoid sharing online, and make sure they know not to share the personal information of others, as well.
- Treat others on the Internet the same as you'd treat them if they were standing right in front of you, in front of all your friends (and your grandmother).
- School surveillance systems—for on-campus safety and for remote test proctoring—have gotten way out of hand. Our kids' privacy has been invaded on a scale never before seen. As parents, you need to be aware of what sorts of surveillance is happening. This includes school-issued devices like Chromebooks or iPads, as well as software that students are required to install on their own smartphones and laptops.
- The Internet is chock-full of explicit sexual and violent material, and it's really not hard to find. Talk with your kids about this sooner rather than later, revising and expanding your guidance over time as they get older.
- Don't panic! The Internet is just a tool, though a powerful one. The benefits far outweigh the risks, and you should embrace it. Focus on staying educated and engaged, and make sure your kids know they can come to you with anything.

For many people, particularly the younger generation, smartphones have replaced computers. In the next chapter, I'll give you several tips for securing these devices.

Going Further

- A comprehensive article on protecting students' privacy:
<https://www.wired.com/story/how-to-protect-yourself-school-surveillance-tech-privacy/>
- Guidelines for protecting against cyberbullying from the US Cybersecurity & Infrastructure Security Agency (CISA):
<https://www.cisa.gov/uscert/ncas/tips/ST06-005>
- A handy child online safety guide from Consumer Reports:
<https://www.consumerreports.org/privacy/protect-childrens-online-privacy-a7638021263/>
- I haven't used this one myself, but I have to say that it looks very interesting. It's an app that helps kids learn about privacy and even blocks some tracking: <https://gizmodo.com/do-not-track-kids-privacy-app-childrens-data-1849667220>

Checklist

This list is by no means exhaustive. I strongly encourage you to use the links provided at the end of this checklist and in the “Going Further” section to do further reading. Many excellent websites have been created to specifically address online safety for kids, and I am just scratching the surface with this list. However, these are some of my favorite tips for helping to keep your kids safe and happy on the Internet.

Tip 11-1. ★ Create a Dedicated Account for Each Child

Every child’s needs and maturity levels are different. Creating a computer account for each child will allow you (and the child) to customize the settings, preferences, background images, web browser bookmarks, and so on. It’s not just about custom parental controls. It’s also about giving everyone their own space and the opportunity to express their individuality. (It can also contain the damage if their account somehow gets infected with malware.) Use the steps outlined in the checklist for Chapter 6 to create these accounts. On both Windows and Mac, you have the option to designate these new accounts as “family” accounts or accounts that have “parental control.” Go ahead and select that option as you create the account. (See also the next tip.)

This is also a good tip for online accounts and streaming services. Don’t share your accounts with your kids—get them their own accounts, if possible; if not, at least give them their own profiles so you can individually control the content and usage.

Tip 11-2. Use Parental Controls for Young Children

Both Windows and macOS have built-in parental control settings. This software can be used to limit what websites your kids can access and how much time they spend on the computer. In my experience, these tools work well until your child gets to the point where they need to use the Internet consistently for schoolwork. Many perfectly normal websites that can be used for homework will be blocked by some of these utilities. While you can try to approve each of them as needed, you may find that you constantly have to tweak the settings. When I got to that point (probably when they went to high school), I just turned off the website blocking. And remember...statistically speaking, they probably have a smartphone, anyway, and access to other devices with Internet connectivity. When they reach a certain age, parental controls only go so far.

When you get into the parental controls configuration, there are lots of possible settings. Just use some trial and error here. You're going to need to tweak these settings over time anyway as your child gets older and is able to handle more mature material.

One caveat, though: *please* don't install spyware on your child's computer or smartphone. Even if your heart is in the right place and you're fully transparent with your children about this surveillance, these apps may be mining their data. Also, sometimes the software techniques used to implement the surveillance can create significant security vulnerabilities for their devices. Stick with the parental controls that are built into the operating system.

Tip 11-2a. Windows

With Windows, Microsoft requires both you and your children to have a Microsoft account to use parental controls. I personally find it ridiculous that Microsoft requires children to register to have parental controls on a home computer. If this was an added feature with extra benefits, that would be okay—but requiring it for any level of parental control seems to me like a poor policy. This means your child will need to have an email address, for example. (See the next tip for help with that.)

But if you have Windows and need parental controls, here's what you need to do:

1. Create a Microsoft account for yourself, if you haven't already (see Chapter 6 for help).
2. Create a Microsoft account for each child who will require parental controls (again, see Chapter 6 for details).
3. While signed in to Windows as the parent, go to this site:
<https://account.microsoft.com/family>

4. Sign in, if necessary. Then click “Add a family member” at the upper right (Figure 11-1).

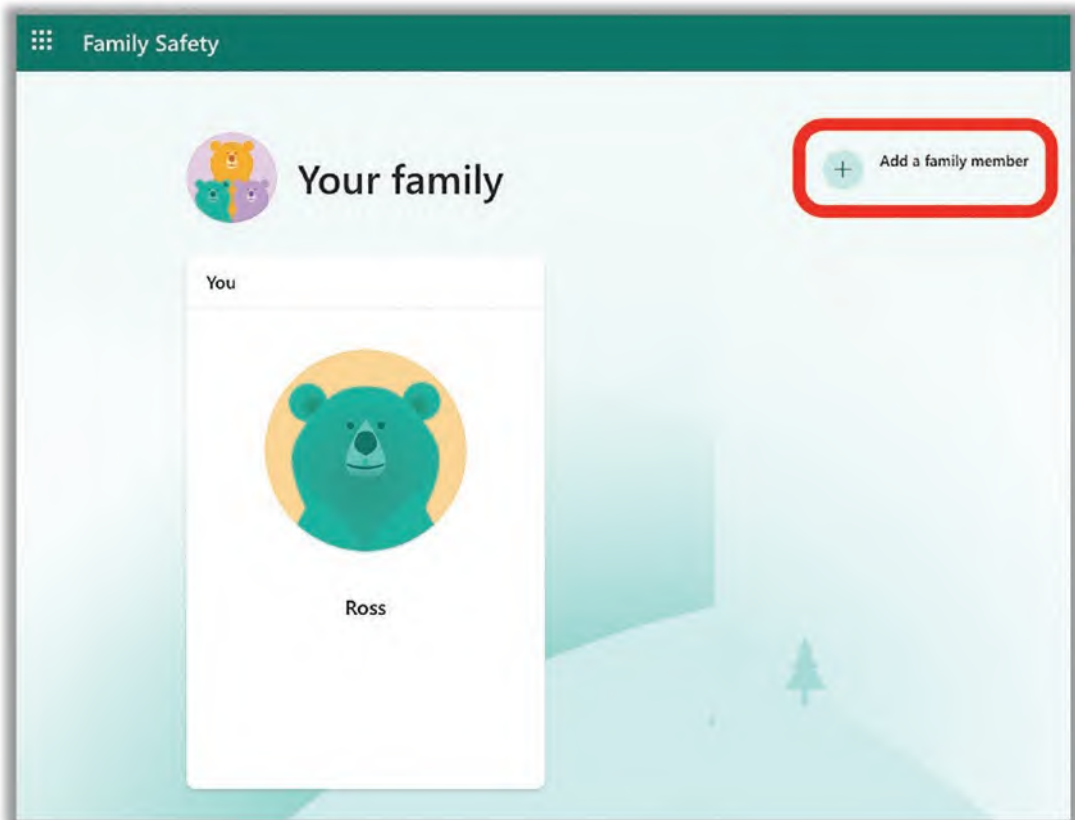


Figure 11-1. Windows Add family member

5. You will need a phone number or email address for your child. You can create one here by clicking the link “Create an email,” but I’ll assume you have one. Enter it here (Figure 11-2).

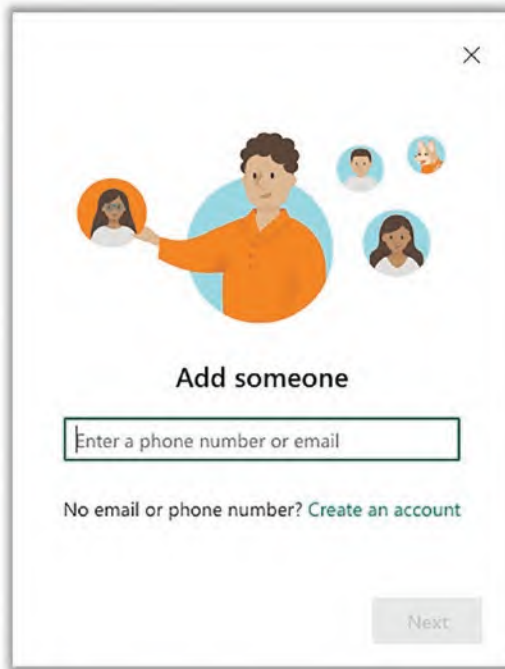


Figure 11-2. Windows Add someone

6. On the next screen, add the child as a “Member,” so you’ll be able to set controls (Figure 11-3).

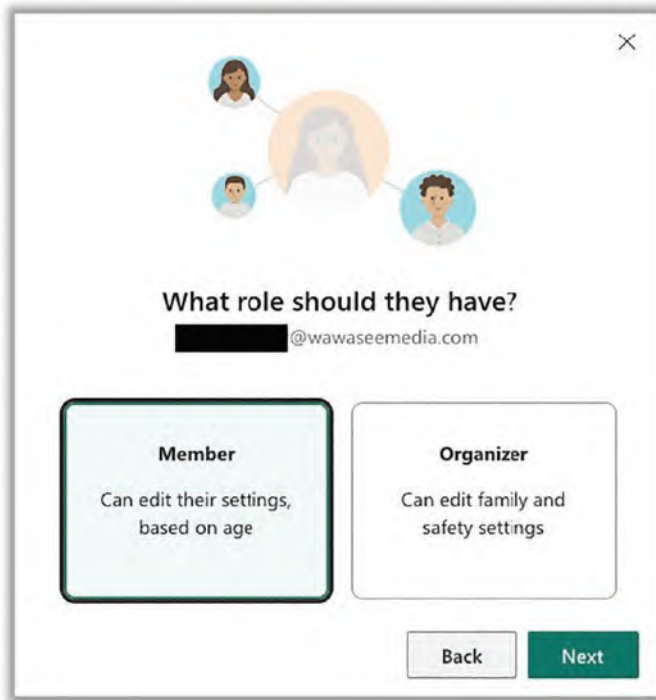


Figure 11-3. Windows Set user role

7. If asked, solve the CAPTCHA, proving you’re not a robot, and then click “Invite.” This will send an email to the child’s address. They (or you) will need to accept the invitation in the email by clicking the “Join now” button.
8. At this point, Microsoft will walk you through several steps to finish setting up the child’s account and parental control settings. You can set these as you see fit and change them at any time later. One note: I would not allow them to sign in with non-Microsoft apps. Unless you know of a specific non-Microsoft app that they’ll need to use, I would uncheck this box.
9. Repeat this process for each child account.

Tip 11-2b. macOS

On macOS, setting up parental controls has a lot of steps. This is mostly because Apple gives you lots of ways to control things—spending, screen time, content, and sharing of family purchases. And unfortunately, the steps are different for Ventura and Monterey. Capturing all the possible steps and screenshots would take up several pages.

So, instead I'll give you the highlights here and direct you to the Apple documentation for details, which does include screenshots. In all cases, be sure to look for different instructions based on the macOS version because Apple (of course) changed how things work between Monterey and Ventura.

1. If you haven't created a separate account for your child yet, do so now. See Chapter 6 for help. Be sure to make this a "Standard" account, not "Administrator." You can also get help from this Apple support document: <https://support.apple.com/en-us/HT211874>
2. To limit usage and schedule downtime, you'll need to set up Screen Time. See this Apple doc for help setting this up, with detailed information about all the various settings you can tweak: <https://support.apple.com/en-us/HT210387>
3. If you want to be able to share Apple purchases, Apple Cash, messages, and other Apple services, you'll need to set up an Apple ID for your child. I recommend that you do this—it's very convenient. This Apple doc has all the details: <https://support.apple.com/en-us/HT201084>
4. I would enable Find My on each of your child's portable devices (iPhone, iPad, MacBook). The details can be found here: <https://support.apple.com/en-us/HT210400>

Apple has a website entirely devoted to parental controls and family sharing of applications, movies, and music. Be sure to check it out:

<https://www.apple.com/families>

Tip 11-3. Creating Email Accounts for Young Children

Most kids today will prefer to using messaging and social media apps to communicate, but there will still be times when they will need to have an email account. When Gmail first came on the scene, my daughters were infants—but I decided to create accounts with their names right away, so they didn’t have to settle for dumb usernames like “grrrrrrl152” or something when they got older. Of course, data privacy wasn’t as big of an issue then. In retrospect, I wish I had also created another account for public stuff that didn’t contain their names.

There are some email services that are set up specifically for young kids. Many US laws regarding privacy for children apply to anyone under 13 years of age. For this reason, you will have to jump through special hoops in this case (which is a good thing). You can check out these services which will give you (the parent) a lot of control over who they can communicate with and what content is allowed in emails and even give you direct access to the emails. Note that while some of these services have an entry-level free account, you may end up paying a small monthly fee.

- ZillaMail: <https://zilladog.com>
- KidsEmail: <https://www.kidsemail.org>
- TocoMail: <https://tocomail.com>

You need to realize a couple things, though. First, it’s quite likely that your child’s school will require them to set up a Google email account or similar, so that students can easily collaborate online. Many teachers will assign and collect homework online this way, too. Also realize that if you are too restrictive, your kids will find a way to get their own email accounts. So the preceding options are probably only good for elementary school kids.

For older kids, I would look at the same services I recommended in Chapter 9. However, I would also assume that this email address (that doesn’t contain any identifiable information) will become their “public” email address when they get older—that is, the one they’ll give out to retailers, newsletters, and other spam-triggering stuff. For this purpose, I really like Fastmail. Yes, it costs money (about \$30/year for a basic account), but it’s a really powerful service with decent privacy protections. But the killer feature for fighting spam is that each account can have up to 600 email aliases!

Tip 11-4. Research Before Your Kids Sign Up

I can't stress this enough: don't trust what anyone else tells you when it comes to stuff for kids because most people really don't know what they're talking about. Spend the time to check out the site yourself and search the Web for parental reviews (see some of the sites I list at the end of this checklist). Also, be sure to check the date on the reviews and favor the ones that are most recent—at least within the last year or two. This stuff changes quickly and constantly.

Tip 11-5. Teach Your Kids to Protect Their Identities

When signing up for websites or social media or playing games online, give away as little identifying information as possible. Teach your kids to never give out their full name, address, phone number, email address, current location, or even school name to strangers. Tell them to leave their names and birth date out of any user IDs they create, too.

Furthermore, tell them not to give away any personal information for you, anyone else in your family, or for other people. This includes being careful of what you capture in the background of any images you upload.

Tip 11-6. Be Able to Access All Accounts and Devices

At least for young children, you should always have the login credentials to all of your kid's accounts and devices (computer accounts, smartphones, tablets, game consoles). You can use a password manager like BitWarden to share them easily. If a device has a fingerprint reader or face scanner, you can just add your fingerprint and/or faceprint as a second allowable scan. Your kids should know that at any point you can log in and see what they're up to. You might even schedule some somewhat random check-ins to drive this home and make it feel real. When they get old enough (whatever age that is for your child), you can relax this restriction. At some point, you're going to want to give them their privacy and establish an honor system.

Tip 11-7. Honor the Age Restrictions

Almost all websites and Internet services require that users be at least 13 years of age to join. This comes from the Children’s Online Privacy Protections Act, or COPPA. You can learn more here:

<https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>

You have to enter your birthday as part of the registration process, though they have no way to verify this. Nevertheless, it’s not good to teach your children to lie about their age in order to gain access to a website. Some sites and services will have overrides that allow parents to grant access after sufficient covering of their butts.

Tip 11-8. Friends Must First Be Met in Person

Teach your children that people on the Internet may not be what or who they claim to be. A good rule of thumb is to insist that they first meet someone in real life (or as the kids say, “IRL”) before they can “friend” them in social media or communicate with them via chat rooms, email, social media, or text. That is, they must have met this individual face to face, in person. You must approve any exceptions to this rule. And when kids are really young, you should probably personally approve all online connections.

Tip 11-9. Lock Down Chromebook Settings

If your school has issued your child a Google Chromebook or if you’ve decided to give them a Chromebook for home use, you should take the time to lock down the privacy settings. While the Chromebook is a secure option for surfing the Web, it can be a privacy nightmare, given that it’s made by Google (an ad company). The EFF has a great guide to these settings, which I highly recommend. This guide will walk you through protecting your passwords and synchronized data, as well as reducing the amount of information about your child that is shared with Google:

<https://www.eff.org/deeplinks/2015/11/guide-chromebook-privacy-settings-students>

In addition to these settings, you should also change the default search engine to something like DuckDuckGo or Brave Search. Just be aware that kids can be mean... when they see someone using a non-Google search engine, they may get teased. I know that sounds dumb, but I've seen it happen and kids are sensitive to ridicule.

Tip 11-10. Teach Kids the Rules of the Internet

The Golden Rule applies in virtual realms, as well. But beyond just being good policy, it's important for your children to realize that anything they do on the Internet can potentially be leaked to people they don't intend. That basically means that anything they post online could be seen by anyone, possibly many years in the future.

Also, remember the Grandmother Rule: counsel your kids not to do anything online that they wouldn't be comfortable showing their grandmother. Of course, the same should apply for you (the parent), too, but in my experience, kids are more concerned about offending their grandparents than their parents.

Tip 11-11. Beware of Connected Toys

As I've said, the Internet is everywhere. But one place the Internet should not be is in kids' toys. It's okay to have computerized toys that have internal processing, but beware of connecting any "smart" toy to the Internet. Also, don't give Internet-connected toys to others as gifts. These toys may have built-in microphones and cameras, and they probably have horrible cybersecurity. Even if you trust the company that produced the toy with whatever data that might be collected, you should also be thinking about what could happen if cyber creeps manage to hack into the device, because this has definitely happened⁶.

Tip 11-12. Keep Computers in a Common Area of the House

While children should have a certain degree of privacy in their communications, it's just asking for trouble to allow them to surf the Internet in a closed room. This applies to smartphones, tablets, and eReaders, too—not just laptops and Chromebooks.

⁶<https://www.itv.com/news/2018-11-21/new-rules-on-internet-toy-security>

You can require them to put their phones and tablets on the charger before going to bed (and that charger should not be in their rooms). I don't care how good your kids are, the temptation to respond to the chat requests and watch videos in the middle of the night will be too great to resist at some point. This rule also ensures that their phones are fully charged at the start of each day.

Tip 11-13. Use Family-Friendly DNS

As we covered earlier in this book, whenever your computer wants to talk to another computer on the Internet, it needs to first look up its address. This is done using Domain Name Service (DNS)—DNS is what converts “google.com” to an IP address that is routable.

There are a few free services that will automatically block mature content. You might consider setting this up for individual computers or your entire house (i.e., on your home router). Unfortunately, setting this up can be tricky—and if your kids are savvy enough, they can just change it to something else. If you're interested, you can check out these options:

- OpenDNS “Family Shield”: <https://www.opendns.com/home-internet-security>
- Cloudflare 1.1.1.1 for Families: <https://blog.cloudflare.com/introducing-1-1-1-1-for-families>
- CleanBrowsing: <https://cleanbrowsing.org/>

See Chapter 8 for help changing your DNS settings.

Tip 11-14. Use Device Tracking (Judiciously and Fairly)

Both Android and iOS (iPhone, iPad) have the ability to locate a device, and you should enable it for your child. You should strive to only use it if the device is lost or stolen or if you need to find your child in an emergency situation. You should also make it clear to your child that you have this ability but will use it only in these special situations and any other situations you deem valid (lay it out for them). You don't want to be oppressive, and you want to foster trust, so try to be reasonable here. The key is to be very clear about your family privacy policy and stick to it. You can revise this as time goes on, of course, and in response to misbehavior.

Tip 11-15. Create a Contract for Your Kids

Using the Internet and having a smartphone are privileges. You are the parent and you have the final say on when, how, where, and how often these tools are used. Come up with a set of simple, clear rules for using these things and print them. If you want to get formal, have your child sign it. Be sure to include things that you promise to do, as well. Here are a few you can look at for reference, but I encourage you to give this some thought and create your own.

<https://www.safekids.com/family-contract-for-online-safety>

<https://www.connectsafely.org/child-pledge>

Tip 11-16. Great Parental Resources

Here is a list of some excellent parental resources. Bookmark them in your web browser for quick access.

- *Common Sense Media*: <https://www.common sense media.org>
- *ConnectSafely*: <https://www.connectsafely.org>
- *Protecting Kids Online*: <https://www.consumer.ftc.gov/topics/protecting-kids-online>

The following resources are geared toward school privacy for kids and parents but contain information for teachers and school administrators, as well.

- *K12SIX*: <https://www.k12six.org/>
- *US Department of Education*: <https://studentprivacy.ed.gov/>
- *CISA K-12 Cybersecurity Resources*: <https://www.cisa.gov/stopransomware/k-12-resources>
- *EFF: Student Privacy Resources*: <https://www.eff.org/issues/student-privacy>
- *CDT: Student Privacy Resources*: <https://cdt.org/area-of-focus/privacy-data/student-privacy/>
- *EPIC: Student Privacy*: <https://epic.org/issues/data-protection/student-privacy/>

CHAPTER 12

Armored Carriage: Your Mobile Castle

Mobile devices have become integral parts of our lives—particularly smartphones like Apple’s iPhone and all the variants of Android phones. Unlike our desktop machines, mobile phones are mobile computers we carry with us everywhere, outside the more secure confines of our home. This chapter is dedicated to helping you make your smartphones more secure and private.

Fair warning, though... I’m an Apple person and I will admit that I carry a bias. I have several friends who are Android fanatics, and they swear by them. Of course, being privacy nerds like me, they don’t run Google’s operating system on these devices—they run third-party OSs like Calyx. That’s beyond the scope of this book. So, long story short, the advice here is going to be Apple-leaning. But don’t worry; I cover both in the checklist.

iPhone vs. Android

Smartphones contain unbelievable amounts of extremely personal information including financial data, health data, your personal address book, emails, web surfing history, and access to much more data in the cloud. They also track your location pretty much anywhere on the planet, 24/7, because frankly they have to in order to send you texts and phone calls. If that weren’t enough, smartphones have built-in microphones and cameras that can record everything you do, plus an accelerometer and several other sensors¹. Your mobile phone may have more personal information on it than any other device you own, even more than your home computer.

¹ Believe it or not, that accelerometer has been used to pick up keyboard data, just by making inferences based on the vibrations from typing: <https://www.wired.com/2011/10/iphone-keylogger-spying/>

And make no mistake—a smartphone *is* a computer, and a very powerful one at that. Do you remember the Deep Blue supercomputer that beat chess champion Garry Kasparov in 1997? The iPhone 8 (now over 5 years old) has more than *20 times* the computing power as Deep Blue, and it fits in your pocket! So, let's talk about how we can secure these wonderful devices.

iOS Is More Secure Than Android

Let's get this out of the way: in my not-so-humble opinion, iOS is safer than Android². Google is doing some fantastic work in the realm of security; don't get me wrong. But the Android ecosystem is fundamentally different than that of iPhones, and those differences make Android phones harder to secure.

When Apple came out with the iPhone, the company was really in the driver's seat. Steve Jobs knew that this device was going to completely change the smartphone world, and he managed to get all the major cell phone carriers to give him maximum control over the software on this device. The problem with Android is not that it's not secure. The problem is that Google gave too much control over the software to the cell phone manufacturers and service providers. I'm sure there were business realities at play here. Perhaps the cell phone folks felt burned by Apple's control over iOS and demanded more ability to control the Android OS on the devices they sold. So, you could argue that this isn't really Google's fault. But however it happened, the cell phone makers and cellular service providers are an integral part of the supply chain and serve as gatekeepers to many software updates to Android phones. As recently as a couple years ago, a study found that almost 30 percent of Android phones weren't even capable of getting the latest software. Even if the phone makers and service providers want to allow the updates, they have to go through a lengthy process of testing the changes on each device first.

Google has addressed some of the security update issues, but it could be years before most Android phones will be able to stay as up to date as Apple iPhones. A very notable exception would be Google's own Pixel smartphones. In this case, Google is in full control of both the hardware and the software (much like Apple), allowing these phones to be updated with the latest security fixes. So, if you're going to go with an Android phone, your best bet, in terms of security, is to get a Google-made phone.

² Actually, just about every security expert I've read or talked to believes the same thing.

iOS Is More Private Than Android

While the security issues are definitely important and the differences between iOS and Android are arguable, the starker difference is privacy. There's just no comparison: Apple wins hands down. There are two reasons for this. First, Apple's iOS is a very closed ecosystem, meaning that Apple exerts extreme control over what apps it will allow to run on the phone and what those apps are allowed to do when you can run them. People often call this a "walled garden" ecosystem. Whatever you called it, it's a major source of frustration for a lot of people. They want to be able to do whatever they want to do, even if that means taking more risks. You can have a spirited and healthy debate over the freedom and control aspects here,³ but the upshot is that Apple's closed system and restrictive permissions ultimately give you, the user, more protection from malicious and prying apps.

The other reason is that Google is an advertising company. Google's business model is tied directly to knowing as much about you as possible. It's a pure conflict of interest that I just can't reconcile, and it's the same reason I can't recommend Google's Chrome browser. While I firmly believe that Google is doing great things in the realm of security, it has shown time and time again that it will go to insane lengths to track everything you do to command top dollar for its advertising.

Apple's move to force every app to ask for your permission to track you (called App Tracking Transparency) is an excellent example of this. It's so stunningly simple and obvious: give users an informed choice, without mealy-mouthed euphemisms about "enhanced" or "personalized" experiences, and people will reject tracking. Facebook claims that this one change is costing them \$10 billion a year in lost ad revenue.⁴ As far as I'm concerned, that's a good thing—those were ill-gotten gains in the first place. But, again, I'm a privacy nerd.

Look, Apple is not perfect by a long shot. There are several things I feel they need to improve, like offering client-side encryption for data stored in iCloud and getting out of the ad business itself. But compared to Google, they're just so much better. If you have the fortitude and wherewithal to install a privacy-respecting Android variant like Calyx, then maybe we can have a debate on relative privacy. (Due to the complexity, I won't cover that here, but I will mention it in Chapter 13.)

³And both the US government and the European Union are currently doing so.

⁴<https://www.macworld.com/article/611551/facebook-app-tracking-transparency-iphone-quarterly-results.html>

Wireless Madness

While laptop and desktop computers have their share of wireless technologies, smartphones have more. Modern cell phones have Wi-Fi, cellular data, Bluetooth, near-field communication (NFC), and wireless charging. Every one of these wireless interfaces presents a potential chink in your smartphone's armor—a gap that will allow the bad guys a way into your phone. Let's quickly review each one.

For Internet access, your smartphone has two options: cellular data and Wi-Fi. Cellular data is your default connection to the Internet from a smartphone and should be available in most populated areas. Data service comes with your smartphone plan, and the amount of data you can transfer is for the most part unlimited today. However, if you do high-bandwidth activities like binge-watching your favorite Netflix series using cellular data, even most “unlimited” plans will start throttling or limiting your data usage at a certain point. Videos and movies can eat up a ton of data.

So, what if you do want to catch an episode of your favorite TV show on your iPhone? That's where Wi-Fi comes in. As we discussed in Chapter 3, Wi-Fi is a wireless networking technology, giving you access to the Internet at home and in coffee shops, hotels, airports, restaurants, and other people's homes. Wi-Fi service is generally unlimited in terms of amount of data transferred. But as we've also discussed, public Wi-Fi hotspots can be sketchy when it comes to security and privacy. If you're just going to surf the Web or read emails (things that consume very little data), I recommend avoiding public Wi-Fi and just stick to using your cellular data plan. You can also use a virtual private network (VPN) service to protect your Wi-Fi traffic, but be aware that services like Netflix will often block you if you're using a VPN (to prevent people from accessing their services from outside their home country).

Because the whole point of smartphones is to be unencumbered, they use wireless technologies for everything. This is where Bluetooth and NFC come into play. As we discussed in Chapter 3, Bluetooth is used to connect peripheral devices to your phone like headphones and keyboards without the need for pesky cords. NFC, on the other hand, is used for things like mobile payments and sometimes pairing of devices. NFC tries to limit itself by physical proximity—hence the “near” part of near-field communications. The idea is that the user has to place the smartphone near or even on the payment terminal or whatever; it can't just connect while it's in your pocket or purse. In reality, though, any radio frequency (RF) technology can work over longer distances in the right circumstances.

The last cord to cut is the power cord. Many smartphones (and other devices like the Apple Watch) have come up with clever ways to transfer power without cables. However, this usually requires very close proximity—like sitting on a special mat or stand. The appeal is that you don’t have to physically connect the power cord. Apple’s iPhone now use magnets (Mag Safe) for wireless charging, which can also make it much easier to attach your devices without having to use clamps and such.

Unfortunately, all of these wireless technologies increase your cell phone’s attack surface—they’re just more avenues for hacking. While these technologies seem fairly simple to use, they are quite complicated under the covers. To do what they need to do, they are quietly and constantly monitoring the airwaves for signals and often replying to wireless queries from other devices automatically. Most of these technologies require a unique wireless identifier to operate. But this has allowed some enterprising retailers and law enforcement types to track your device using this ID and, by extension, track you. Some stores have devices that monitor Wi-Fi and Bluetooth from phones to monitor your movements in their stores—when you enter, how long you linger in front of that sale rack and when you come back to the store a few days later to buy something. They may or may not be able to tie that wireless ID to your name, but they know it’s the same person each time because the wireless ID of your phone doesn’t change. Actually, that’s not entirely true anymore—because of this very issue, modern Apple and Google devices create random wireless IDs, rotating them frequently—though it’s not clear how effective this really is at preventing tracking.

To Hack or Not to Hack

As we’ve said, smartphones can be much more restrictive on what applications you can run or even what settings you can change. Cell phone makers and cellular providers do this mostly for security purposes—trying to protect people from themselves. But they also do this because they want to protect themselves and their business interests, often at the expense of their customers. It should be no surprise then that enterprising hackers have found ways to circumvent these restrictions, and they’ve made them available to the public via easy-to-use tools that you can find all over the Internet if you take the time to look.

The process of circumventing your smartphone’s built-in restrictions is a form of hacking called *jailbreaking* or *rooting*. Like regular computers, smartphones have different levels of permissions. Unlike regular computers, the cell phone makers and cell phone service

providers reserve the highest permissions for themselves. Needless to say, this rubs some people the wrong way. “I bought the stupid device. Why can’t I do whatever I want with it?” If you get the right phone and the right hacking tool off the Internet, you can gain full administrator privileges and do whatever you want. While this may sound very tempting, I’m here to tell you that it’s not a good idea.

If you recall, in Chapter 6, I strongly encouraged you to create and use a non-admin account on your computer. This follows the security practice of “least privilege.” You want to restrict what you can do in most cases to be the bare minimum, just in case some bad guy or piece of malware gains access to your account. By using a limited access account, you can limit the amount of damage that can be done if that account is hijacked.

This is the same basic philosophy at work on smartphones. Apple and Google have created elaborate permission schemes on their smartphones that are designed to let you do everything you need to do while simultaneously restricting the damage that can be done by a rogue application or service. While some of these restrictions are more for their benefit (or the cell phone service provider’s benefit), on the whole they are the best mechanism for protecting your data and your privacy. Removing this safety mechanism will allow you to do whatever you want... but it also opens the door for any other application on your device to do what it wants. While I think there’s a strong philosophical argument to be made in favor of removing these restrictions—and I hope in the future cell phone makers return more of this power to the user—right now it’s definitely safer for most users to leave these restrictions in place.

Third-Party App Stores

There’s one particular aspect to user choice and control that deserves mentioning: third-party app stores. On an iPhone, the only place you can download and install applications is from the official Apple App Store. The security restrictions imposed by Apple in iOS won’t allow you to install anything else.

On Android phones, the default settings require all applications to come from the Google Play Store. However, unlike iPhones, Android allows users to install and use non-Google app stores and/or install apps that don’t come from the Play Store (a process called “sideloading”).

Apple's refusal to allow apps from outside its App Store has been a hotly contested issue in the United States and in the European Union. It's seen as monopolistic practice, especially because Apple charges a hefty commission for all things sold through the App Store (usually between 15 and 30 percent of all revenue). Apple argues that app developers are getting a lot of value from this arrangement. After all, Apple provides a lot of free, high-quality software development tools, performs security audits and reviews of all apps, and provides access to a massive marketplace of buyers. Nevertheless, many app developers (like Epic, the maker of Fortnite) have claimed these fees to be onerous.

But the real issue here is choice. Government regulators believe that iPhone owners should have the option to install whatever software they want and there should be competition from other app stores, with potentially lower commissions. I think they're right: users should have this choice. I think Apple should open its devices to allow people to install whatever software they want. However...just because I think you should have the *right* to do this doesn't mean I think you should actually do it, if Apple ever is forced to give you this freedom. I believe that apps that have been vetted by Apple (and Google) are likely to be more secure than those that aren't. At some point, I think we'll find out—because I think Apple will eventually lose this fight.

A Mole in Your Pocket

For me, privacy is far and away the most important topic related to smartphones today. These devices are with us almost every hour of every day and are in constant contact with the Internet. They know where we are, where we've been, who we know, who we talk to, how to access our bank accounts, what news we read, what we buy, what games we play, what pictures we like to look at, what we text and email, what websites we use, and what's on our calendar... the list is endless. Your phone probably contains or has access to credit card numbers, phone numbers, passwords, PINs, birth dates, passport info, and social security numbers. We keep all the information of our lives on our smartphones so that we can access it anywhere at any time.

The Apple App Store now has very helpful “privacy nutrition labels” that detail what sorts of information each app collects and how it uses it. You can always go back and

check this information for each app you’ve already installed. Just as an example, here’s the information for Facebook Messenger vs. my personal favorite, Signal (Figure 12-1).

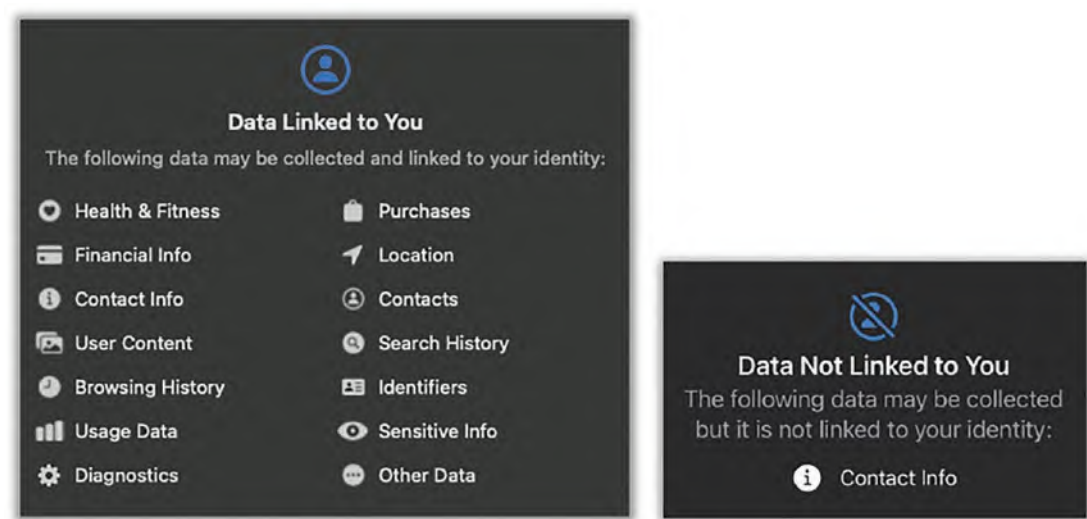


Figure 12-1. Facebook Messenger vs. Signal data collection

You’d think that with all that juicy information, people would be more incentivized to protect it. But according to a 2017 Pew poll, 28 percent of people still do not lock their smartphones with a PIN or other access control.⁵ I can only hope that with the capability to unlock your phone using touch or face ID, most people are locking their devices now—though I can’t seem to find current data on this.

Biometric vs. PIN Code Locks

But this presents an interesting dilemma. As we discussed in Chapter 5 on passwords, fingerprints and facial features are forms of biometric authentication. As opposed to something you *know* (a PIN or passcode), biometric identifiers represent something that you *are*. PINs and passcodes are a pain in the butt; there’s no doubt. Having to enter even four digits to get into your phone all the time is annoying (and honestly, you should be using at least six). Using your index finger or face is much, much easier. But is it really secure?

Let’s consider fingerprints. First, realize that there are multiple ways that someone else can use your fingerprint. The most obvious way would be somehow compelling you to

⁵<https://www.pewinternet.org/2017/01/26/americans-and-cybersecurity>

do it for them or knocking you out and pressing your finger to the sensor. In the past, hackers were able to fool fingerprint scanners pretty easily, but over the years, they've gotten more difficult to beat—at least on iPhones.

With phone makers trying to get more screen real estate, big buttons on the front of the phone have been replaced by cameras and other sensors that instead scan your face. While there are some cases where twins and siblings with very similar faces have fooled Apple's Face ID system, Apple still claims that in most cases, chances of someone else being able to unlock your phone using someone else's face is about one in a million. That's pretty good, and better than Touch ID. The odds of someone else being able to unlock your device with their finger is more like 1 in 50,000.⁶

But there's another thing to consider here. Currently, at least, there's a legal difference between a fingerprint or faceprint and a password or PIN. This is still an evolving area of law, and it probably varies country by country, but biometrics has been viewed like a physical key. If law enforcement has a warrant to search your home, they can compel you to open the door with your key. But can they compel you to use your finger or face to unlock your cell phone? The court cases in the United States are literally all over the map. A 2014 case in Virginia ruled that cops can force you to use your finger to unlock a smartphone, but a 2019 case in California ruled that law enforcement can't compel a fingerprint or face scan to unlock a phone. On the other hand, the courts so far seem to treat divulging passwords and PINs as a violation of the Fifth Amendment's protection against self-incrimination, like the combination of a safe. For now, at least, this is not settled law—but it's a distinction to be aware of.

So—as is often the case with security and privacy—you need to weigh the trade-offs with respect to convenience. While it's much more convenient to use your finger or your face to unlock your smartphone, it may not offer you protection from law enforcement or a physical attacker. That's probably not a concern for most people, however, meaning that in most cases, using biometrics to unlock your phone is a worthwhile trade-off between convenience and security (especially compared to not locking your phone at all). And both iOS and Android now have “lockdown” modes where you can quickly disable biometric access, requiring a PIN or passcode to unlock the phone.

⁶<https://www.intego.com/mac-security-blog/which-is-more-secure-face-id-touch-id-or-a-passcode/>

Give and Take

The smartphone in your pocket or purse is giving away your location constantly, in multiple ways. Your phone's location is tracked by the cell phone towers, by the phone's operating system (remember that Google owns Android), and probably by multiple different apps running on the phone. Location data is extremely revealing. I can figure out where you live (your location in the middle of the night), where you go to work (your location during each weekday), and where you worship (that church, synagogue, or mosque you drive to once every weekend). And I can see who you sleep with, too (that other phone that's with you at 3am). Several companies are collecting and selling your location data to whoever wants to pay for it. Just this year, the Federal Trade Commission (FTC) sued data broker Kochava for selling location data for hundreds of millions of mobile devices.⁷ But very often, it's government agencies purchasing this data, skirting the Fourth Amendment here in the United States, including Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), and other parts of the Department of Homeland Security (DHS).⁸

But there are also some really nasty ways in which data can be exfiltrated from your phone, too (which is just a fancy cybersecurity term for "taken"). For example, when you cross into the United States, even if you're a US citizen, the CBP has the right to inspect your phone. They have automated tools at their disposal which can siphon off all sorts of information from your phone. If they can connect a cable to the device, they have tools from companies like Cellebrite that have the capability to download phone data, even from locked devices in some cases. So, you might think this isn't that big of a deal because you never or hardly ever travel internationally. But it turns out that the laws governing the CBP's ability to conduct searches say that they can do this anywhere within *100 miles* of the US border. About two-thirds of US citizens live within this area.⁹

⁷<https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other>

⁸<https://www.aclu.org/news/privacy-technology/new-records-detail-dhs-purchase-and-use-of-vast-quantities-of-cell-phone-location-data>

⁹<https://www.bloomberg.com/news/articles/2018-05-14/mapping-who-lives-in-border-patrol-s-100-mile-zone>

It gets much worse, though. There are other companies like Israel's NSO Group who have created a spyware tool (called Pegasus) that can completely take over your cell phone from anywhere on the planet. To break into your phone, they just need you to click a link they send to you via text message. In some cases, they even have "zero touch" hacks that can compromise your phone with no interaction required from you at all. It's believed that this technology was used to locate and murder journalist Jamal Khashoggi in 2018.¹⁰

The good news, if there is any here, is that these sorts of attacks are extremely rare. This is the dragon in our castle analogy. Unless you're rich or famous or you somehow manage to anger a nation state, these highly technical and elaborate attacks are not going to be used against your phone.

¹⁰ <https://www.aljazeera.com/news/2021/12/21/uae-agency-placed-spyware-on-khashoggi-fiancees-phone-report>

Summary

- Our cell phones hold amazing amounts of extremely personal information. We need to take extra steps to protect this data.
- Cell phones are wireless in just about every way and come with a bevy of technologies that allow them to function untethered. However, that also means there are extra avenues of attacks for bad guys.
- Cell phone makers and service providers have restricted what users can do with their devices for both security and proprietary reasons. While it's often possible to download tools that will circumvent these restrictions, doing this can expose you to a great deal of risk.
- You should always lock your smartphone, either with a PIN, with a passcode, or with biometrics like a fingerprint or face scan. For most people, a biometric lock is a good balance between security and convenience, but if you're really worried about your privacy, you need to use a passcode.
- Your smartphone is constantly tattling about your location to several different listeners. Right now, there are very few legal restrictions on collecting and selling this data.

In our penultimate chapter, I'll cover several areas that didn't fit neatly into the other chapters. I'll also give you some ideas for kicking things up a notch, if you have the desire and the determination to do so.

Going Further

- This website has some interesting findings and thoughts on cell phone security: <https://securephones.io/>

Checklist

The cell phone market—particularly the Android phone market—is extremely fractured. By that I mean there are many variants of the Android operating system out there, not only in the underlying version of the operating system itself but also with respect to service providers. The cellular service companies like AT&T and Verizon often make their own customizations to the operating system. Even the smartphone manufacturers like Samsung and LG often customize the OS. This makes it very difficult to provide a definitive, specific step-by-step guide for doing anything on Android OS. Therefore, most of the advice in this checklist is somewhat generic. You may need to search the Web or talk to your cellular service provider to help you find the proper way to do these things.

Remember the following:

- Android is Google’s mobile operating system, used on devices from many different manufacturers including LG and Samsung (and of course Google). I will be focusing on the more recent versions of the Android operating system—which at the time of this writing would be Android 12 and 13.
- iOS is Apple’s mobile operating system, used on iPhones and iPads.¹¹ Like with Android, I will be focusing on the more recent versions: iOS 15 and 16.

It’s a little trickier to get useful screenshots on mobile devices, particularly for Android devices because they can differ not only by OS version but also by manufacturer and service provider. For these reasons, I will be describing the steps you need to take in this chapter rather than exhaustively trying to capture images from all the various phone types and versions. Hopefully the textual descriptions will actually be more universal.

Like with computer settings, our smartphones have a ton of configuration options, in weird places. So, just like we did in Chapter 6, I will sometimes tell you to just search for the settings you need to change. It’s often simpler than trying to walk you through multiple levels of clicking.

¹¹ Technically, Apple has renamed iOS for iPad as “iPadOS,” but for the purposes of this checklist, you can consider them to be the same.

Tip 12-1. ★ Back Up Your Phone to the Cloud

If your phone is lost or stolen, you want to be able to recover the information it held. You can often use these backups to restore all of your apps, settings, and data to a new phone. You can also use the backup to go back to a known-good state if something goes horribly wrong.

You can back up your phone to your computer or to the cloud (see the next tip for computer backups). Cloud backups are extremely convenient. Both Android and iOS have this ability built in and it's easy to enable (in fact, it's sometimes hard to avoid). However, there are a few caveats with cloud backup.

- It will probably cost you money every month. Apple and Google provide some minimal cloud storage for free, but it probably won't be enough to back up your phone. While backing up a 128GB phone will not require 128GB of cloud storage (only data is really backed up—apps and the OS are restored by re-downloading), you will still likely need to buy more storage. However, this is fairly inexpensive—from one to two dollars a month.
- While cloud storage is encrypted, you currently can't use your own key. That means that both Google and Apple can access the stuff you put in their cloud storage. This is a major privacy problem. Hopefully they will make this an option in the future.
- You may not be able to restore data from an old version of the OS to a newer version. This can be a problem if your phone is lost, it was backed up using an older OS version, and your replacement phone is a newer OS version. This is another reason to stay on the latest operating system version.

Tip 12-1a. iOS

Backing up to iCloud is very easy. Apple only gives 5GB of storage space for free, and most phones will require more than that. You may need to buy more space through Apple iCloud+ plans, but it's pretty inexpensive. You can also share this data storage with your family.

1. Go to Settings and then click your name at the top to access your iCloud account.
2. Select iCloud.
3. Enable the option for “Back Up This iPhone.”

This will back up your phone daily when your iPhone is connected to power, locked, and on Wi-Fi. If you want, you can click “Back Up Now.”

Tip 12-1b. Android

Android backups are trickier, though apparently it used to be a lot worse. Because of the fractured Android marketplace, each manufacturer seems to have a slightly different way to set up Google cloud backups (and most of them offer their own cloud backup utility, to make things even more confusing). I would personally recommend staying entirely within the Google ecosystem where possible.

- *Email, calendar:* Google email and calendar data are already stored in the cloud—no need to back them up.
- *Photos, videos, music:* Use Google Photo and your pics and videos will automatically be backed up. Similarly, Google Play Music will back up your music.
- *Contacts:* This can be tricky on a non-Google phone. Your contacts may be backed up to your cellular provider or phone manufacturer. Open your Contacts app and look in the settings to see where they’re being backed up. I’d choose Google, if you can.
- *Apps and app data:* Google Play knows what apps you have and can restore those easily. App data is mostly backed up, but sounds like it’s up to each app developer how well this works.
- *Files:* The easiest option here is to save your files to a cloud service like Google Drive, Dropbox, or OneDrive.
- *Everything else:* Your settings and preferences, app data, SMS messages, and other stuff can be backed up using Google One—a subscription cloud storage service.

- See this article for more information. Honestly, Android backup just seems a mess: <https://www.computerworld.com/article/3215095/how-to-back-up-android-phones-complete-guide.html>

Tip 12-2. Back Up Your Phone to Your Computer

Cloud backups are by far the easiest way to back up your phone. However, this has some pretty significant privacy problems, as I discussed in the previous tip. So, if you'd like to back up your phone's data without paying for cloud storage subscription, here's how to back up to your computer.

Tip 12-2a. iOS

Back Up to a Mac

As of macOS, phone backups are done through the Finder.

1. Connect your iPhone to your Mac using a USB cable. You may need to unlock your iPhone and elect to “trust this computer.”
2. Open a Finder window (you can just double-click any folder or your hard drive). Select your device from the left-side panel.
3. Click the “General” tab. Select “Back up all of the data on your iPhone to this Mac.”
4. Click “Back Up Now” button and wait for the process to complete. When done, you can disconnect your iPhone.

Back Up to a PC (Windows)

On Windows, you will need to use Apple's iTunes app to back up your iPhone (or iPad). If you haven't installed this yet, download the iTunes app from Apple's website and install it.

1. Connect your iPhone to your PC using a USB cable. You may need to unlock your iPhone and elect to “trust this computer.”
2. Open the iTunes app on your PC. Click the iPhone button at the top left.

3. Click “Summary.”
4. Click “Back Up Now” button and wait for the process to complete.
When done, you can disconnect your iPhone.

Tip 12-2b. Android

For Android, there’s no one easy way to back up your entire phone to a computer, unless you use third-party apps that I can’t really recommend. If you connect your Android device to your computer with a cable, you should also be able to manually copy files from your Android device to your computer, but this is a pretty clumsy option for regular backups. Honestly, I can’t really recommend it. However, if you’d like to see what this entails, look at this article:

<https://www.androidauthority.com/backup-android-phone-708622/#3>

Tip 12-3. ★ *Keep Your Device Up to Date*

Security problems are found all the time, and mobile device makers release updates on a fairly regular basis. You should be sure to update your device’s software whenever a newer version is available—this includes the operating system as well as applications.

Tip 12-3a. iOS

Apple’s iOS is free and easy to update. On your iPhone, go to Settings ► General ► Software Updates to check your current version and see whether you have any updates. Select “Automatic Updates” and enable all three options on this page: Download iOS Updates, and Install iOS Updates and Security Response & System Files (iOS 16 only). As it will tell you on this page, updates will be downloaded automatically, and you will be notified before the updates are installed. Updates will be installed when the device is charging and connected to Wi-Fi.

For app updates, go to Settings ► App Store, look for “App Updates” button, and enable it.

Tip 12-3b. Android

Automatic OS updates should already be enabled by default, but here’s how to check it.

1. Open the Settings app and go to “Software Update” or “System Update.”
2. Tap the gear icon at the upper right.
3. Click Download & Install.
4. Tap “Wi-Fi” to enable updates when you’re connected to Wi-Fi (only). I wouldn’t go with the option for either Wi-Fi or cellular as OS updates can be big, but that’s your call.

For app updates, check the following:

1. Open Google Play Store.
2. Tap your profile image at the upper right.
3. Click Settings ► Network Preferences ► Auto-Update Apps.
4. I would select “Over Wi-Fi only,” but you can also choose “Over any network” to update even when on cellular data networks.

Tip 12-4. ★ Restrict Application Permissions

Both iOS and Android have gotten really good about forcing application makers to explicitly ask for access to various features of your phone such as the microphone, the video camera, your contact list, your location, and so on. Practice the policy of least privilege, and deny permission to any app that doesn’t absolutely need such access. It makes sense for a weather app to want access to your location because you usually care most about the weather where you are. However, why in the world would that same weather app need access to your address book or the microphone?

Usually, these apps ask for permission when you install them or perhaps when you first run them. At the time of this writing, Apple’s iOS provides a lot more flexibility on what you allow each app to access and give you the ability to change these options after the fact. With Android, it’s often all or nothing, and you may not be able to change your mind later. Both iOS and the more recent versions of Android allow you to control some things based on whether the app in question is in the foreground (i.e., it’s the app you’re using right now—the one “on top”).

Note that some applications may fail to work after removing permissions—either because they really do need access to the thing you just cut off or because they didn’t design their app to deal with people who want to protect their privacy. So, you may have to go through a little trial and error with these settings.

Tip 12-4a. iOS

For iOS devices (iPhone/iPad), go to Settings and then Privacy & Security (iOS 16) or Privacy (iOS 15). There you will find a long list of system devices and data. At the top, you’ll see “Location Services.” Under this menu, you can control which apps have access to your location and whether they can access it all the time or only when the app is the current main app (“on top”). You also have the option to only share your approximate location (within a 10-mile square area).

For the other categories like Contacts, Calendar, Microphone, and so on, you can enable or disable access for each application that has requested access. Some categories have more fine-grained controls. As tedious as it sounds, I would take the time to go through each setting and remove permissions for anything that doesn’t make sense or isn’t absolutely necessary.

Tip 12-4b. Android

All recent versions of Android provide some level of application permissions that can be disabled after first install or use, but the granularity of the permissions will vary depending on the app and your version of Android. How you make these changes seems to change a lot—part of the curse of Android. But the fastest method appears to be using the permission manager.

Go to Settings ► Privacy ► Permission manager. You will then be presented with a long list of permission types. As tedious as it sounds, I would take the time to go through each setting and remove permissions for anything that doesn’t make sense or isn’t absolutely necessary.

Tip 12-5. ★ Lock Access to Your Device

You absolutely need to secure access to your mobile devices, either with a password or a biometric lock. Anyone who picks up your device can access tons of very personal information.

Both iOS and Android should have prompted you to set this up by default. Some devices allow you to enter a full-on password, which is the most secure way to go. However, since unlocking the device requires physical access and you can set the phone to deny access after several failed attempts, a four-digit PIN is sufficient for most people. I would store your PIN or passcode in your password manager, just in case you forget it or you want to securely share this with a family member.

If your smartphone has a biometric scanner (finger or face), that's by far the easiest locking mechanism to use. It's secure and convenient, and I would recommend this method for most people. You'll still need a PIN or passcode as a backup. I would add a backup finger or face ID too. Use a different finger, for example, or set up Face ID with glasses on. You can also add prints for another person. I do this on my daughter's phones. Finally, you can change the label on each of these IDs—give them meaningful names.

If your phone has the option to wipe all data after a certain number of incorrect attempts to unlock, I encourage you strongly to enable this feature, as well. To enable this, see the following instructions.

Tip 12-5a. iOS

Go to Settings, then either “Touch ID & Passcode” or “Face ID & Passcode,” depending on the type of device you have. It should force you to enter your PIN or password to make any changes. Scroll all the way down to the bottom to find the “Erase Data” option and enable it.

Tip 12-5b. Android

Android does not appear to have the same set of lockdown features that iPhones have. I've searched extensively, and at best I've found that some manufacturers offer similar features and there are some third-party applications you can install that will provide similar features.

Tip 12-6. Enable Emergency Lock Mode

Unlocking your phone with your finger or face is very convenient. But if you are at all worried about someone else accessing your device by compelling you to use these biometric scanners, you shouldn't use them. However, both Android and iOS have a

“lockdown” feature that lets you disable biometric unlocking quickly, requiring your PIN or passcode. This can be very useful in an urgent situation where you want to quickly disable biometric locks—maybe when going through a border security check or when you’ve been pulled over by a police officer or for any situation where you think your phone may be taken from you.

Note that you can also just completely power off your device, if you have the chance. That’s even more secure than just locking it.

Tip 12-6a. iOS

You can force your iPhone to require a PIN code and disable biometric unlocking temporarily without even having to look at it. In both the following cases, the technique will bring up the power off screen. Once this screen appears, you’ll need to enter a PIN to unlock it the next time. How you do this depends on the type of biometric scanner you have:

- *Face ID:* Press and hold both the power button and one of the two volume buttons for a few seconds.
- *Touch ID:* Press and hold the power button for a few seconds.

Tip 12-6b. Android

To lock down your device, present and hold the power button for a second or two, which will bring up the standard menu to power off or restart. But there will now be an option for “Lockdown.” Next time you try to unlock it, you’ll be asked for your PIN or passcode (biometric unlocking will be disabled for this one time).

This option should already be available on your power down screen. If not, you may need to enable this feature. Go to Settings ► Lock Screen ► Secure lock settings. Enter your PIN or password. Tap “Show lockdown option.”

Tip 12-7. ★ *Use Secure Messaging Apps*

While Apple’s Messages has end-to-end encryption, Apple can still read these messages if they’re backed up to iCloud. There are better apps out there, if you really want your messages to be private. Unfortunately, everyone you want to communicate with will also need to download and install the same app—because these communication protocols aren’t (and may never be) standardized. These apps are available for both iOS and Android, as well as for your computer, so you can actually message from any device to any device.

I personally recommend using Signal. It's extremely secure, and the people who wrote and maintain this app are zealous privacy advocates and extremely talented at cryptography. It's the most popular messaging app among the handful that are truly secure and private. The app is free and easy to use. You can do group chats, voice calls, and video chats too. It will run on Mac, Windows, iOS, and Android. Give it a try—and find a few friends to try it with you, so you'll have someone to use it with.

<https://signal.org/>

If this app doesn't do it for you, try one of the following:

- Session: <https://getsession.org/>
- Threema: <https://threema.ch/en>
- Matrix: <https://matrix.org/>

There are several other messaging apps that claim to be secure and encrypted, but in many cases the messaging service provider holds the encryption keys—meaning that they can read your messages. And that means they can hand over your messages to law enforcement or intelligence agencies—and they're open for abuse by employees with proper access. WhatsApp is arguably the most popular “secure” messaging app, but you may not realize that it's owned by Facebook. The creators of WhatsApp left Facebook after the buyout largely because they didn't like the way Facebook removed privacy protections.

Tip 12-8. ★ Limit Ad Tracking

Google and even Apple, sadly, both have some form of ad tracking. You can turn some of this off or down, however.¹²

Tip 12-8a. iOS

Go to Settings and then Privacy & Security (iOS 16) or Privacy (iOS 15). Go to Settings ► Privacy. Scroll all the way down to the bottom, and then select “Apple Advertising.” Disable Personalized Ads.

¹² You might be interested to read this article, which talks a bit about the history of tracking on iOS and Android: <https://www.eff.org/deeplinks/2022/05/how-disable-ad-id-tracking-ios-and-android-and-why-you-should-do-it-now>

While you're here, you can check the settings for Analytics & Improvements (just above Apple Advertising the privacy settings). I would disable all of these.

With iOS, Apple requires apps to ask for permission to track you—a wonderful feature called App Tracking Transparency. Note that this isn't foolproof—many apps have figured out clever ways to still track you, despite Apple's best efforts to give you control. To review which apps you may have granted this permission to (maybe by accident), go to the Tracking section of the privacy settings. Here I would disable "Allow Apps to Request to Track" and delete any apps you see listed here who you've granted permission to track you.

Finally, Apple also gives you a privacy report to see what information you've been sharing and which apps have been using that information. At the bottom of the privacy settings, review your personal App Privacy Report.

Apple isn't perfect, but they're way ahead of Android when it comes to data privacy.

Tip 12-8b. Android

On Android, your options for limiting tracking are...well, limited. Start by deleting your advertising ID. Go to Settings, then Privacy, and then Ads. Click "Delete advertising ID." If you don't see this option, you may be on an older version of the OS—instead, you may see "Reset advertising ID" and then be given an option to opt out of ads personalization.

Some of these settings can be changed online for your entire Google account. Check this website and disable as much activity tracking as you can:

<https://myactivity.google.com/activitycontrols>

Tip 12-9. Remove Unused Apps

How many apps do you actually use on your smartphone? If you're like most people, you've probably accumulated dozens of "free trial" or "free today only" apps that you never use. Or maybe you have multiple utility apps that do the same thing (calculator, converter, weather, etc.). You might think it's harmless to leave those apps sitting dormant on your device, but the truth is that those apps are probably getting automatically updated all the time—and who knows what version 2.0 does? Maybe it has a cool new "friends" feature that contacts everyone in your address book or starts recommending recipes depending on your current location. With every software update, there are potential risks of software bugs that bad guys can exploit too.

The opposite problem may also bite you. Maybe the app is abandoned and will *never* be updated. What if there's a known security bug that goes unfixed?

Bottom line: if you're not using an app, delete it. You can always reinstall it later if you find that you want it back. In most cases, once you buy it, it's yours for life, and the app store will allow you to download it again. This will have the added benefit of saving precious space on your device.

Tip 12-10. Enable (Self) Tracking

Both iOS and Android have a built-in utility to help you find a lost device. This feature will even allow you to remotely lock or wipe that device. Note that for these features to work, your device must be

- Turned on
- Signed in to your Google or iCloud account
- Connected to mobile data or Wi-Fi
- Have location services turned on

Tip 12-10a. iOS

Go to the iCloud settings by clicking your name at the top of the Settings app. Then scroll down to “Find My.” Open these settings and enable “Find My iPhone.” I would also enable the other options: “Find My network” and “Send Last Location.”

If you lose your device, you can use another Apple device or the iCloud website to find your device, make it play a sound, or remotely wipe or lock it. (You can also just use this to check that the services are working.)

<https://www.icloud.com/find/>

Tip 12-10b. Android

For Android devices, you may need to install the Google Find My Device application. You can find it in the Google Play Store.

To enable Find My Device, go to Settings. You may have to dig around to find the “find my” settings. Look under Security, or Security & location, or Google ► Security.

If you lose your device, you can use another Android device or the Google “Find My Device” website to find your device, make it play a sound, or remotely wipe or lock it. (You can also just use this to check that the services are working.)

<https://www.google.com/android/find>

Tip 12-11. Use Firefox Mobile Browser

Of course, both iOS and Android devices come with a built-in browser: Safari and Chrome, respectively. Apple’s Safari mobile browser is actually pretty good from a privacy perspective. It has some pretty powerful anti-tracking technology built in. If you’re happy with Safari, you can keep using it. However, you can install a different browser on iOS or Android, if you wish—and I would definitely do this on Android to avoid using Chrome. I would suggest installing Firefox from the app store. If you want even more privacy, you might try Firefox Focus (an even more private version of Firefox), DuckDuckGo Privacy Browser, or Brave Private Web Browser apps.

Note that on mobile phones, many apps actually come with their own built-in web browsers. When you click a link in Facebook, for example, you are probably taking to Facebook’s web browser—not your system-defined default web browser. And of course, these in-app browsers are almost surely tracking everything you do there—that’s the whole point. I think this is horrible, personally, but as of this writing, it’s not something you can easily prevent. You can, however, try to check if this is happening. From the browser, just go to this website:

<https://inappbrowser.com/>

It will attempt to tell you if your browser is either an in-app browser or if the app your’re using has tried to inject some tracking JavaScript into the link you clicked. This site also has a long article with many more important details on how this all works.

Tip 12-12. Avoid Cheap Android Phones

There have been several reported cases of cheap Android phones coming preinstalled with adware, spyware, and even straight-up malware—right out of the box. Some of the best-known manufacturers are ZTE, Archos, myPhone, and BLU. Don’t cut corners when buying a smartphone. Stick to well-known name brands. If you’re going to choose Android, I would suck it up and pay for a Pixel so that you’re sure to get immediate security updates.

Tip 12-13. Get a Burner Number

I spoke at length about email aliases in Chapter 9. Having a “split personality” is a great way to throw off the trackers and data miners. While creating email aliases is free, cheap, and easy, getting a functional phone number alias is basically none of those things. But it’s still possible.

Ideally, you want to get a second “burner” phone number that you can give away to marketers, restaurant reservation systems, online contests, charities, rewards cards... you get the idea. Today, you really want that number to be capable of sending and receiving text messages, but sometimes you need the ability to receive phone calls too (or at least voicemails).

Of course, you could simply get a second cellular phone number. If you go the prepaid route, it might not be that expensive. Note that you wouldn’t necessarily need a second physical phone—many phones today can accommodate two SIM cards, basically having two different numbers on a single device.

There are a handful of other services you can consider, each with different features. I don’t have a particular recommendation because it will really depend on your budget and specific needs. I believe any of these are good options.

- MySudo: <https://mysudo.com/>
- Burner App: <https://www.burnerapp.com/>
- Hushed: <https://hushed.com/>

Tip 12-14. Use a Mobile VPN

Virtual private networks aren’t just for laptops. While most banking and shopping apps on your phone already use encrypted connections, some of your other apps may very well be completely open and unencrypted. And when you’re using the free Wi-Fi at Starbucks or McDonald’s, your hotel lobby, or wherever, any unencrypted data is completely visible to anyone else in the area with a simple wireless monitoring application. If you have a VPN app installed, it should automatically kick in whenever your device tries to connect to an unknown (and therefore untrusted) network.

However, there are a few gotchas with mobile VPNs. First, mobile VPNs are even more finicky than computer VPN services. I guarantee you will find situations where it will frustrate you because it simply will not connect, forcing you to either go without an Internet connection, disabling your VPN, or using cellular data.

Second, mobile VPNs aren't perfect—they've been shown to leak information. In other words, not all your Internet traffic goes through the VPN connection. Apple iOS has been shown to completely bypass VPN connections for Apple's own apps.

Like computer VPNs, good mobile VPN services cost money. You should avoid any free VPN, unless maybe it's provided by a privacy advocacy organization that has a sustainable business model that allows them to offer a basic free tier of VPN service. See my recommendations in Tip 7-19 for reputable VPN providers—most of them have mobile clients, as well.

Personally, I just use cellular data whenever I'm away from trusted Wi-Fi.

Tip 12-15. Don't Use Mobile Antivirus

All my research tells me that you don't need a mobile antivirus (AV) app. Smartphones, by their very nature, are more secure than computers—that is, they're less susceptible to viruses and hacking in general, particularly iPhones. While I can respect the argument that some people might want a computer AV program, I think most smartphone AV apps are pointless—and many are just snake oil. And like computer AV apps, they can actually create new security problems. I would avoid them. If you follow the other tips here, you shouldn't need this.

Tip 12-16. Disable Wi-Fi Auto-Connect

Many mobile devices can connect to Wi-Fi, but sometimes they can be set to automatically connect to any open Wi-Fi (no password) or any Wi-Fi network that they have connected to previously. That can be very convenient for your house or work location, but it can be dangerous for public Wi-Fi like "Starbucks" or "McDonald's" or "Airport Free Wi-Fi" or whatever. Because these Wi-Fi network names are well known, bad guys have been known to create their own networks using the same names. If your device is set to automatically connect to remembered networks, you could be inadvertently connecting to a hacker's network. They could just snoop on your web

surfing or perhaps even use this connection to hack your phone. iPhones and Android phones have ways to mark specific Wi-Fi networks as “trusted” or “saved” in their Internet settings. Use this method to determine which networks your phone auto-connects with.

Tip 12-17. Know Your Rights When You Travel

For some reason, normal property and privacy laws seem to be thrown out of the window when you cross a border. For example, current US law gives border agents broad authority to search an electronic device for any reason and for as long as they want. Because of our preoccupation with terrorist threats, border guards have been given a lot of leeway, shall we say. What’s even more disturbing is that the area covered by this law is anywhere within 100 miles of the US border. There are laws in the works to curb this, and even a recent US District Court ruling saying baseless searches are unconstitutional. But until these rights are clear, you can find some great information at this EFF website:

<https://www.eff.org/wp/digital-privacy-us-border-2017>

When you travel, I would take only what you absolutely need to carry. Maybe bring a tablet instead of a laptop, for example. When you cross borders, I would lock your devices such that they require a PIN code to unlock (see Tip 12-5) or even just turn them completely off. You should research the border search laws for each country you intend to enter (including your own, for when you return). Sometimes devices can be confiscated if you refuse to unlock them—and in some cases, you could even be detained or denied entry into the country.

Tip 12-18. Disable Wireless When You Can

Bluetooth is the odd name of a versatile, short-range, low-power wireless technology that allows your mobile device to connect wirelessly to external devices such as speakers, hands-free headsets, keyboards, and more. You can even use it to unlock your front door! However, leaving Bluetooth on all the time means that rogue devices can also try to connect to your device without your knowledge. These connections can be used to steal your data and potentially even compromise your device. While Bluetooth is fairly secure and these attacks are not common, it’s still a good idea to just disable Bluetooth if you never use it. It will also help you save your battery.

Near-field communication (NFC) is another wireless technology built into many mobile devices, though used less often and at much shorter distances. While Bluetooth can work at distances of dozens of feet, NFC is generally limited to maybe an inch or less (hence the “near” part). It’s usually used to pair your phone with another device—maybe to get a Wi-Fi password or trigger a mobile payment app or even transfer a file from one phone to another. Like any wireless technology, it can be broadcasting and listening all the time to any nearby device, making it a possible “way in” to your phone. Disable this feature if you’re not using it. (This doesn’t seem to be possible on newer iPhones.)

Finally, Wi-Fi is something we use all the time on our phones, and it can be hard to live without. But it’s just another avenue of attack and signal with a unique ID that can be used to track you. If you know you’re going to be using it for an extended period of time, disable it. For example, I only use Wi-Fi when I’m at home, so I will often disable it when I travel out of town.

Tip 12-19. Erase Your Device Before Getting Rid of It

Like our home computers, our mobile devices are chock-full of detailed personal information. In fact, our cell phones arguably have way more info in (or accessible by) them. So, before you give away or sell or even recycle your smartphone, you should be sure to wipe it completely. If you’ve encrypted the contents, you’re most of the way there already. But it’s still good to wipe it clean.

Tip 12-19a. iOS

There are a lot of important steps to take to cleanse an iPhone or iPad before you get rid of it. I’ll go over the key ones here, but you should also take a look at this Apple document for a complete and up-to-date list of steps to take:

<https://support.apple.com/en-us/HT201351>

Here are the main steps:

1. Back up your data and transfer everything to your new device first. If you’re buying your iPhone from an Apple Store, they can help you through this process in the store. (They can also help you erase your old device.)
2. If you have an Apple Watch paired to this phone, unpair it.

3. Sign out of iCloud and the App Store. Go to Settings and click your name/picture at the top to access your iCloud settings. Scroll down to the bottom and tap “Sign Out.” Follow the instructions to delete all your iCloud data from your iPhone.
4. Go to Settings ► General and scroll all the way down to the bottom. Select “Reset.” Then select “Erase All Content and Settings.” If you’ve signed up for Find My iPhone, you may have to enter your Apple ID and password to disable this feature. Follow any other prompts to enter passwords, PIN codes, and so on.
5. If you have a physical SIM card, remove it. There’s a little SIM removal tool that came with your iPhone, if you still have it. Otherwise, you may need to use a tiny paper clip or similar to open the tiny SIM slot on the side of your phone.

Tip 12-19b. Android

Unfortunately, as I’ve said many times already, Android devices can be very different from one another in terms of settings. If you have trouble with any of these steps, go into your local cell phone provider and ask for help.

- Be sure to run a full backup of your phone or tablet before you do anything. Assuming you’re getting a new Android device, you should transfer that data to the new device before erasing your old one.
- If you have a removable SIM card (the little card the cell phone service provider put in there to identify you), remove it.
- If you have any removable storage (SD card), be sure to remove it.
- Log out of any services and accounts you use: email, messaging, social media, cloud storage, music services, and so on. You may do this through Settings, or you may have to do it through each application.
- If you haven’t encrypted your device, do that now. It will make sure that even if you miss something here, no one else will be able to find it. This should be under the Security settings.

- Perform a factory reset. Find the Backup and Reset area under Settings (try Settings ► Personal ► Security). There may be lots of options here—select the ones that make sense. Then find and click the “Reset device” or “Reset phone” button.

Tip 12-20. Enable Medical ID

Because everyone has a smartphone these days, first responders now know to check an unconscious person’s phone for emergency medical information—like the old medical ID bracelets. Here’s how to enter this information on your phone. Just realize that when you enable this, anyone will be able to get this information without unlocking your phone. That’s kinda the point, of course, but this feature isn’t somehow magically limited to first responders.

Tip 12-20a. iOS

There are some good descriptions of these settings in the app—review them so you understand what you’re doing here.

1. Open up the Health app and click the summary tab.
2. Tap your profile image at the upper right.
3. On the next screen, tap Medical ID and then Edit.
4. Add all the relevant information here that you’re comfortable doing.
5. Be sure to also add at least one emergency contact.
6. Enable the Emergency Access options at the bottom.

Tip 12-20b. Android

1. You will need to install the Google Personal Safety app, if it’s not already installed. (Note that it may just be called “Safety” on list of phone apps.)
2. You should see a “Start Setup” button. This will walk you through setting up your information.

3. I would share your location here and be sure to set at least one emergency contact.
4. There are several other interesting features—enable whichever ones you’re comfortable with.

Tip 12-21. How to Safely Lend Someone Your Phone

How often has someone asked to borrow or use your phone? More than likely, it’s your young nephew wanting to play a game, or maybe you’re sharing vacation pics with a co-worker. Both iOS and Android have interesting options for limiting access to an unlocked phone for cases like this.

Tip 12-21a. iOS

Apple has an accessibility feature called Guided Access that will restrict the user to using a single app.

1. Open Settings and go to Accessibility.
2. Click Guided Access and turn it on.
3. Read the information there for the various options. You can change the authentication mode required to turn off Guided Access, set time limits, and more.

When you’re ready to give someone your phone, do the following:

1. Bring up the one app you want to let the other person use.
2. Triple-click the side (power) button. This should now prevent you from getting to any other app.
3. When done, double-click the side button to stop Guided Access.

Note If your phone has a Home button, you’ll use this instead of the side button.

Tip 12-21b. Android

Android has a feature called App Pinning that will restrict the user to using a single app.

1. Finding this setting will be a little different depending on your make and model. Try searching settings for “App Pinning.” On Pixel, go to Security ► Advanced Settings ► App Pinning.
2. Enable App Pinning.
3. Also, be sure to enable “Ask for PIN before unpinning.”

When you’re ready to give someone your phone, do the following:

1. Swipe up and hold from the bottom of the screen until you see thumbnails of your recent apps.
2. Find the app you want to pin, tap its icon, and choose “Pin” from the drop-down menu.
3. When done, you can disable pinning by swiping up and holding, or touch and hold Back and Home buttons or Back and Overview buttons (depending on your model).

Tip 12-22. Don’t Hack Your Device

Because mobile devices have so many restrictions on what you’re allowed to do, what apps you can install, and so on, many people have turned to *rooting* or *jailbreaking* their devices to get around these constraints. Having “root” privileges on a computer means you can basically do anything you want. The problem is that once you’ve hacked a device and given yourself root access, you have opened the door for other apps to abuse that same privilege level. This exposes you to all sorts of foul play. I strongly recommend you do not jailbreak or root your mobile device.

Tip 12-23. Periodically Restart Your Phone

Smartphones are just small computers, and like computers, they can get a little slow and confused over long periods of time. The memory can get cluttered with junk that isn’t properly cleaned up, and you may have many, many apps running in the background. It’s just good hygiene to periodically restart your phone—like maybe once every couple weeks.

Furthermore, if you're worried about malware or spyware, many types of malicious software programs are not permanently stored. Restarting your phone will often erase them completely.

Tip 12-24. Never Install Spyware

There are several “security” or “nanny” apps you can install on your phone that will allow you to remotely monitor just about everything that happens on that device, including viewing messages, pictures, location, emails, and more. Some will even let you turn on the camera or microphone remotely. You may be suspicious of your spouse or significant other, or maybe you want to keep tabs on your child. But at the end of the day, this is just spying, plain and simple.

Even if you're okay with the ethics of doing this, you should also know that in order to do all of the invasive things these apps do, they often use very shady or risky software techniques that can compromise the overall security of the device.

If you're worried that someone may have installed spyware on your phone, see the next tip.

Tip 12-25. Check Your Phone for Spyware

Spyware can be tough to spot—to do its job, it needs to hide from you and prevent you from finding and removing it. Sometimes it will pretend to be another common app, copying its name and icon. But there are more insidious ways to hide.

You can find some more resources at these sites. Even though these sites are geared toward domestic violence, I believe the antispyspyware tools and tips would apply more broadly.

- Coalition Against Stalkerware: <https://stopstalkerware.org/information-for-survivors/>
- National Network to End Domestic Violence: <https://www.techsafety.org/resources-survivors>

Tip 12-25a. iOS

With iOS version 16, Apple has added a marvelous new tool called Apple Safety Check. Its main purpose is to review all the information you’ve shared with other people and give you a handy way to revoke that sharing. However, in the process, it also will check for misconfigurations that are often used by spyware and correct them. See this article for more information:

<https://support.apple.com/guide/personal-safety/how-safety-check-works-ips2aad835e1/1.0/web/1.0>

Note that Safety Check has a sub-feature called Emergency Reset. If you are a victim of domestic abuse and/or your personal safety is at risk, use Emergency Reset to quickly cut off all ties with someone you’ve previously shared with.

Tip 12-25b. Android

For Android, according to an expert on spyware from the Electronic Frontier Foundation, the best app for detecting and removing this malware is G Data’s Mobile Security (personal).

Tip 12-26. Use Lockdown Mode (Apple Only)

With iOS 16, Apple introduced a special security feature called Lockdown Mode. It’s specifically designed for high-profile spying targets like dissidents, activists, journalists, politicians, and so on to prevent malware and spyware infections. In this mode, Apple disables a lot of fancier convenience features that have been exploited by top-tier hacking tools often used by nation state intelligence agencies and the like. However, I personally think this might be useful for “normal people” in some situations too—like maybe when traveling abroad, attending a political protest, or in any situation where you might be arrested.

In this mode, your Messages app won’t show you web link previews, and most attachment types will be blocked. Some website technologies will be blocked, which may cause some sites to load slowly or even break completely. Incoming FaceTime calls will be blocked unless you have previously called them. There are several other changes, but in my mind they’re not that severe. You can read more here:

<https://support.apple.com/en-us/HT212650>

To enable this mode, perform the following:

1. Open Settings, and tap Privacy & Security.
2. Under Security, turn on Lockdown Mode.
3. This will require a phone restart.

You can disable Lockdown by reversing the preceding process.

Tip 12-27. Use a USB Condom

This is going to sound ridiculous, but it's a real thing—and it's actually becoming more common. Public cell phone charging ports can be hacked, and hacked USB ports can hack your phone. It's called "juice jacking." Public charging stations are becoming much more common these days—at airports; on airplanes, bookstores, coffee shops, and restaurants; and in the back of taxis and rideshare vehicles. Even my grocery store has them. USB devices can contain small chunks of software, and often our devices trust this software implicitly. And sometimes USB interfaces can be used to bypass security controls.

So, what to do? Well, your best bet is to bring your own charger with you—either one that plugs into a wall socket (standard AC plug) or a portable battery charger. But there's another option you may not have heard about: a USB "condom." The idea for the USB condom is the same as for a regular condom—you can catch a virus if you're not prudent about where you stick that thing.

USB cables have four wires in them, two for data and two for power. If you look inside a USB plug (like your cell phone charger cable), you'll see them. You want to block the data lines but leave the power lines. For this purpose, you can buy a special data blocker adapter or cable—a USB "condom." Just search Amazon or your favorite electronics online store for a "data blocker." They're not expensive. If you get the adapter version, then you just have to put this adapter between your regular phone charging cable and the public USB port. You know, like a condom.

CHAPTER 13

Odds and Ends

At this point in the book, I've covered most of the technical topics that require background and longer explanations. However, there are a handful of other topics that I want to touch on because I feel they're important or interesting, topics that didn't neatly fit into the broader categories covered by previous chapters.

In this chapter, each section will have its own checklist with just a brief introduction. It'll be sort of like a lightning round—so, here we go!

Privacy for Cars

Almost all modern cars now come with a built-in cellular modem, meaning that they are constantly connected to the Internet. You may have to pay money to get access to that connection (a Wi-Fi hotspot built into your vehicle), but it's not just there for you. It's there so that your vehicle's manufacturer can keep tabs on your car and, by extension, on you. Often these Internet connections are used for helpful things like crash reporting and software or configuration updates, but they can also easily be used to collect your personal data.¹

What sorts of personal data? Besides location and speed, your car could theoretically report what satellite radio channels you listen to, what podcasts or audiobooks you like, and any data from your phone that you've synced to your vehicle. When you pair your cell phone to your car, you very often upload your contact list, which may contain a lot of very personal information.

¹ Sadly, these cellular connections also open cars to malicious remote hacking, too: <https://samcurry.net/web-hackers-vs-the-auto-industry/>

I'll give you some tips for guarding your privacy, but you should also check this wonderful site for even more useful information:²

<https://privacy4cars.com/>

Tip 13-1. Erase Phone Data Before Selling Your Car

When it comes time to get rid of your car, be sure to purge any personal data you may have uploaded via your cell phone. Look through the entertainment system settings to find a list of all paired cell phones. You should delete any data there and then unpair the phone(s). If you need help with this, check your car's user manual or go to your local car dealership.

Tip 13-2. Don't Pair Phones with Rental Cars

When you rent a car for travel, you should avoid pairing your cell phone, either via Bluetooth or USB cable. Pairing your phone may upload a lot of personal data to the car's memory, which will then be available to the next person who rents this car (as well as the rental car company's employees). You'd think that rental car companies might purge this information when you return the car, but they don't.

Just for fun, next time you rent a car, poke around in the settings and see if you find other people's cell phones paired there. I've heard stories of people who try to pair their phones with rental cars only to find that the system is full—too many paired phones already!

If you want to play music, podcasts, or audiobooks through the rental car's speakers, try using a simple 3.5mm auxiliary (AUX) cable. You can buy adapters that will convert from the USB-C or Lightning port on your phone to a standard 3.5mm audio jack.

Tip 13-3. Don't Use Insurance Trackers

Insurance companies often advertise special smartphone apps that will save you money on your auto insurance by being a "good driver." Basically, let us track where you go, when you go, how fast you drive, how hard you hit the brakes, and so on, and maybe

²You can also check out the fascinating podcast interview I had with the founder of this organization: <https://podcast.firewallsdontstopdragons.com/2021/09/13/driving-data-privacy-for-cars/>

we'll give you a discount on your insurance. Of course, the opposite is also possible... if you consistently go over the posted speed limit or are constantly slamming on the brakes, they could also *raise* your rates. Regardless, I would assume that by using this app, you're agreeing to giving them lots of personal information that they may even resell to others.

Older versions of this technology involve installing physical adapters that talk directly to your vehicle's computer system using the On-Board Diagnostic (OBD) port, which is usually somewhere under the dashboard. I would have the exact same reservations about using these devices, though they may be less privacy-invasive than a smartphone app.

Tip 13-4. Don't Install Car Maker Apps

Like the previous tip, many car makers and auto dealerships will push you to install their special smartphone app so you can track your car's location and status, get notifications when you need an oil change or gas, and other fun entertainment features. In the absence of meaningful privacy regulations, I would assume that these apps are also mining your data—not just from your car but potentially from your phone, as well. Again, maybe you don't care—you feel you have nothing to hide. But when that data is collected, even if the auto maker or dealership doesn't abuse it, it's still sitting there waiting to be stolen by cybercriminals. In 2022, Toyota announced that personal information for almost 300,000 customers was exposed for a five-year period due to poor security on a database connected to their vehicle smartphone app.³

When Bad Things Happen

Up until this point, the entire book has pretty much been about preventing bad things from happening. Sometimes, despite our best efforts, we still get bitten by misfortune. In this section, I will walk you through the recovery process for some common cyber-calamities or at least point you to websites that can help you.

³<https://www.bleepingcomputer.com/news/security/toyota-discloses-data-leak-after-access-key-exposed-on-github/>

Tip 13-5. Recovering a Hacked Account

If one of your online accounts gets hacked, you need to act quickly to minimize the potential damage. How would you know your account is hacked? Maybe you can no longer log in to the account, even though you know you're using the correct ID and credentials. Maybe you see activity on the account that you know isn't yours, or maybe you received a notification of strange activity from the company associated with the account or even from a friend or family member.

Regardless of how it happened, the first thing you need to do is recover access to your account. If you still can, immediately log in and change your password—you can use a password manager to generate a strong, unique one. Until you change your password, the bad guys can continue to use your account for their nefarious purposes, all the while pretending to be you.

If you can't log in, try using the password reset feature on the account ("forgot my password"). If you still can't log in, contact the support or fraud department for the affected account—a phone call would be the most expedient method, if that's available. You want to regain control of your account as quickly as possible or at least freeze the account until you can get things sorted out.

After dealing with access to your account, here are some other steps you should take:

- If you used this same password anywhere else, you need to change the passwords on those sites, as well. Again, let your password manager create strong, unique passwords for those sites.
- Review your account carefully for suspicious activity, especially recent activity. For email and social media accounts, look for messages or posts that you didn't send. Check both your "sent" folder and your "archive" or "trash" folders. For financial accounts, look for purchases, transfers, charges, or other transactions that you didn't instigate.
- Warn your friends and family about the hack, particularly for any accounts that might be used for communication (email, messengers, social media). This will keep them on their toes in case they get something from your hacked account that might be a scam or phishing attempt.

- This might be a good time to change your account security questions, too—if the bad guy got in there, they could have changed them or jotted down that info. So, if you used that information elsewhere, you might want to change the account recovery questions for those accounts too.
- Check your account profile and settings for any suspicious changes. For example, maybe a malicious web link was added to your email signature or online profile.
- Think about any other accounts or people that might be associated with the hacked account. You need to think like the attacker. What mischief could they get up to?
- If you suspect that your computer itself might be compromised, check your iCloud, Google, or Microsoft account for suspicious activity and maybe change that account password. Also, consider running an antivirus app like Malwarebytes which can do a free, on-demand scan.
- Finally, this would be a good time to enable two-factor authentication, if the affected account supports it. If you had had this enabled, it probably would have prevented the hack in the first place.

Tip 13-6. Website Password Breach

If you get a notice saying that there has been a “security breach” with one of your accounts, they will usually tell you that you should change your password. That’s precisely what you should do, right away. As a further precaution, don’t click any links in the notification email (just in case it’s a fraud). Log in to your account by manually entering the web address or using a browser bookmark or favorite. If the notification was legitimate, you’ll probably see a notice when you log in to the account.

What the email may not tell you is that if you use this same password on any other websites, then you better change your password on those sites too (and make it unique this time). If the website breach email says that credit or debit card numbers were also lost, you should keep a close eye on your account, looking for purchases that you didn’t make.

There's a great website that helps people figure out whether their account info has been leaked in a breach called Have I Been Pwned:⁴

<https://haveibeenpwned.com>

The term *pwn* (rhymes with “own”) is hacker lingo for dominating or defeating someone. If you've been pwned, you've been successfully hacked. This site maintains an up-to-date catalog of all the known server breaches, indexed by email address. You enter your email address or even your phone number on the site, and it will tell you whether that contact information was part of a known breach.

Tip 13-7. Your Computer Has a Virus

Your best move here is to just not get the virus in the first place because getting rid of malware once your system is compromised can be really tricky. How do you know if you have a virus? Well, if you've received a ransom message asking for money, then it's pretty obvious—see the next tip for help with that. Otherwise, it can be hard to determine this definitively. But here are some symptoms that might indicate a compromise:

- Your computer is suddenly more sluggish or less responsive.
- Your computer appears to be working hard even when you're not using it. For example, the fans are blowing full tilt or the hard drive light is flashing constantly.
- Unwanted windows or applications are popping up all the time.
- Computer or web browser settings change inexplicably.
- You're getting windows popping up out of nowhere, including ads or warnings of computer problems.

If recently installed some software, you might try to uninstall it. Maybe it's just junkware. But if you think you might have a virus, you can do an on-demand virus scan. Even if you have AV software installed, you can use these tools to get a second opinion:

- Malwarebytes “for home” version (Mac or Windows):
<https://www.malwarebytes.com/mwb-download>
- If you have a Windows machine, try running Microsoft Safety Scanner:
<https://www.microsoft.com/en-us/wdsi/products/scanner>

⁴I've actually interviewed the owner of this site a few times: <https://podcast.firewallsdontstopdragons.com/?s=troy+hunt>

If you can't seem to shake the virus, you might have to completely delete this user account. (If the account was your admin account, you might even need to completely wipe the entire computer and start over.) If you are pretty sure you know when things started going haywire, you can try using your backup software to bring your entire computer back to a point in time prior to the suspected infection date.

If you're pretty sure your computer is infected, I would remove it from your home network until you get things sorted out. Otherwise, your computer may be trying to actively compromise other devices on your network or communicating with command-and-control servers. To download the preceding AV tools, use a friend's computer to download the installers, and copy the files to your infected computer using a portable storage device (flash drive, thumb drive, external USB drive).

Tip 13-8. You've Got Ransomware!

If you get a pop-up dialog or big scary full-screen message telling you that all your files have been encrypted and you must pay money to get them back, congratulations—you are the victim of ransomware. If you have a full backup of your system (see Chapter 4), you can simply restore your system to a point in time prior to the ransomware infection and you're done. That's why backups are so crucial.

If your backup is only for your files (and not your entire system), then you'll need to delete and recreate the infected user account and then restore the files from backup.

If you do not have a backup, then you really have just one hope of getting your files back without paying: maybe the bad guys screwed up somehow. It happens more often than you'd think. There are at least two websites devoted to helping victims of ransomware, usually by finding flaws in the bad guy's malware that will allow you to recover your files *without* paying. So before you pay the ransom, check out these sites (using a different computer or device, since your device is compromised and possibly unusable):

<https://www.nomoreransom.org>

<https://id-ransomware.malwarehunterteam.com>

If all else fails and you really need those files back, then you can always pay the ransom. In most cases, you will get your files back. I know it may seem naïve to trust cybercriminals, but in reality, they actually need to maintain their reputations. If they didn't return people's files after the victims paid the ransom, word would get around, and then no one would pay. It's in their best interests to bend over backward helping you. Some of these

guys actually have tech support that you can call for help in paying the ransom money, like how to buy and transfer Bitcoin. I'm not kidding. Again, it's in their best interests to help you. Note that you can sometimes negotiate lower ransoms too.

Sometimes, particularly for business ransomware attacks, the bad guys add another twist: if you don't pay, they will release your files to the public. That is, they don't just encrypt all your files, but they download copies of them too. This is something that having a backup can't fix. If this happens to you, you'll have to decide if the ransom is worth paying. Of course, that doesn't guarantee that they won't come back again later for more money, if they feel you're really concerned about the files being put on public display.

If you're a business, you might consider buying cyber insurance. Not only can they help you cover the ransom payment, but they also employ negotiators and computer specialists that can help you recover your data, sometimes without paying. Sadly, the existence of cyber insurance has probably prompted more ransomware attacks because the bad guys know they'll get paid. In fact, it's not uncommon for the cyber insurance companies to have established relationships with the bad guys, having worked with them to recover from attacks on other clients.

Tip 13-9. Restoring a Lost or Messed-Up File

Back at the beginning of this book, we talked about setting up an automated backup for your most important files. This allows you to recover files that you accidentally delete or screw up somehow. We discussed two ways to do this: either an external hard drive or using a cloud backup utility like Backblaze. Use the following links to find detailed steps for restoring files from a backup:

- Mac OS Time Machine: <https://support.apple.com/en-us/HT203981>
- Windows File History: <https://support.microsoft.com/en-us/help/17143/windows-10-back-up-your-files>
- Backblaze: <https://www.backblaze.com/restore.html>

And When I Die...

So, what happens to all your various online accounts when you die? That's a question most people probably never ask themselves until it's too late. While most people are aware that they should have a will and healthcare directives, only about 40 percent of Americans have any estate docs.

But how many people take the time to prepare their *digital* estates? I'm guessing very few. What should happen to all your emails, photos, music, forum posts, dating site info, social media accounts, and so on? In this section, I'll give you some tips on how to manage your digital affairs.

Tip 13-10. Get a Will

I can't stress this enough. If you have a spouse or children, you really need to have a will in place. Every state has different rules about what happens to your stuff if you die without a will, but these processes can take a long time, and the default rules may not suit your needs at all.

When you go to get your will, talk to your lawyer about handling your digital assets, as well. They should at least be able to tell you what your state law says about this subject. Be aware, however, that this area of law is still evolving. Also, most of your accounts are probably governed by those terms of service you read completely and carefully before you clicked "I agree" and are not governed by state laws.

Tip 13-11. Add a Backup to Your Safety Deposit Box

Again, this is not really a digital thing, but it's important. Some banks will not honor a will or power of attorney to allow access to a safety deposit box. I have no idea why this one thing is sometimes treated specially, but it is. So, make sure that your spouse and perhaps one of your children have been approved to access your safety deposit box.

One weird caveat to this. At least my bank, in order to *remove* someone from this access list, all parties on the list must be present. So don't go too crazy.

Tip 13-12. Ensure Access to Your Accounts

Your successors may need immediate access to things like bank accounts, investments, insurance, computer accounts, and so forth. You should therefore print off a list of your most important passwords and keep them in a safe place. You might put these printouts in your safety deposit box or in a fireproof safe. You could also give this to your lawyer, as part of your estate documents.

BitWarden also has an emergency access feature, sort of dead man's switch.⁵ If you die or become incapacitated, your designated backup person can request access to your password vault. If you don't deny the request within the configurable time period, they're granted full access.

Just make sure that whoever needs these passwords knows where they are and knows how to get to them.

Tip 13-13. Ensure Access to Your Two-Factor Device

If you've followed my advice on setting up two-factor authentication where you can, that means your successors will also need access to your two-factor authentication device. This will most likely be your cell phone. So, make sure that your cell phone account can remain active (so your phone can receive SMS messages) and that your authenticator app is accessible. If your cell phone is locked (and it should be), you should write down your PIN or passcode somewhere. You can also usually add a second biometric signature to unlock your device, but biometrics can be flaky. You should use a PIN or passcode here to be safe.

If by some misfortune your loved one dies without doing this, your best bet will be to try to access their accounts from known devices and in known locations. This might prevent the two-factor code from being requested. 2FA is often not required from "trusted" devices, at least for some period of time.

If you can get into the account, you might want to add your cell phone as the two-factor authentication device. If the deceased used Authy or a similar authenticator app that allows for transfer to a new device, you should try to transfer it to your phone. If they printed off their 2FA "seed codes," you can scan/enter those codes to set up your own app on your own device for their accounts.

Tip 13-14. Appoint a "Digital Executor"

While you might want to simply hand over all your passwords to your beneficiaries when you die, you might have some parts of your digital life that you want to die with you. The only way to accomplish this is to appoint some third party whom you trust to take care of this for you after your death. Your lawyer might be a good choice. You will need

⁵I love this term. Comes from old times when a train would stop if the engineer died or fell unconscious: https://en.wikipedia.org/wiki/Dead_man's_switch

to carefully document what you want done with each online account and any digital data. You will only want these passwords and instructions to be opened after your death, which is something your lawyer should be able to arrange for you.

If you do a little web searching, you can find articles about what to do with your digital life when you die. Try searching for “digital estate planning.”

Note that social media accounts can be particularly finicky. Their policies can be weird, and they’ve been changing their policies and procedures as this issue has become more prevalent.

Here are a few articles you can start with:

- <https://lifehacker.com/how-to-preserve-your-digital-legacy-and-why-you-should-1848900489>
- <https://gizmodo.com/how-to-decide-what-happens-to-your-data-when-you-die-1848124116>
- <https://www.theverge.com/2021/11/10/22774873/apple-digital-legacy-program-comes-to-ios15-iphones-macs>
- <https://www.bloomberg.com/news/articles/2020-03-03/this-is-what-happens-to-your-emails-after-you-die>

Tip 13-15. Stop ID Theft After Death

Not everyone will get the memo when your loved one has passed, and that can allow unscrupulous people to steal the deceased person’s identity. Here are a few steps you should take to prevent this:

- Send a copy of the death certificate to the IRS.
- Send a copy of the death certificate to the Social Security Administration.
- Cancel their driver’s license (and any other professional license they may hold).
- Notify the big credit bureaus: Equifax, Experian, TransUnion, and Innovis.
- Notify their banks and financial institutions.
- Notify their health insurance provider(s).

Gold Stars and Tinfoil Hats

We've covered well over 180 different tips so far—mostly simple and free things you can do to improve your computer safety and privacy. In this last checklist, I've collected some tips for those of you who really want to go above and beyond, or maybe just like a challenge.

These are for the tinfoil hat and black helicopter crowd.⁶ I am by no means saying that you need to do any of these things. For that reason, I'm not going to painstakingly lay out the steps required. However, I thought it would be fun to show you the lengths that some people go to in order to be super secure. These tips are in no particular order.

Tip 13-16. Nuke Your Hard Drive Data

If you have a computer whose hard drive was not encrypted or if you're just that paranoid that you want to be really sure, you're going to want to use a nifty little free utility called DBAN (short for Darik's Boot and Nuke). With this app, you will boot your computer from a CD or USB drive and then scribble all over the hard drive. When you're done, all the data will be completely unreadable—in fact, the computer won't even boot because the operating system will be wiped too.

<https://www.dban.org>

Tip 13-17. Install Haven on an Old Android Phone

Investigative journalists, human rights advocates, dissidents in repressive regimes, and whistleblowers are constantly looking over their shoulders. Being discovered or having their data stolen could result in being jailed or even “disappeared.” Love him or hate him, Edward Snowden knows a thing or two about this situation, and he has created a free Android application called Haven that acts as a super-duper intruder alarm. Using the smartphone's sensors and communication links, the app will monitor your room or personal space for movement, lights, sounds, and power loss and report these events securely to people who may be able to help, should you become incapacitated. Or just use it as a kick-butt baby monitor.

<https://guardianproject.github.io/haven>

⁶These are terms associated with overly paranoid people. Search the Internet for more information, if you're curious.

Tip 13-18. Add a Dedicated Guest Wi-Fi Router

While most modern routers provide a “guest network” option, you still have to trust that the router software maker implemented that security feature properly. If you have some Internet-enabled devices in your home that you don’t fully trust (like Internet of Things devices) or if you have a lot of strangers in your house who want to use your Wi-Fi, you might want to consider beefing up your security and having a dedicated Wi-Fi router for your guests and IoT devices. Having a dedicated router for this untrusted traffic is the safest way to make sure that guests and rogue devices cannot access your private home network.

To do this right, you actually need three routers. You’ll hook them up in a “Y” pattern. You’ll have one wired router connected to your cable modem (or whatever box you use to connect to the Internet), and then you’ll hook two Wi-Fi routers up behind that wired router. This will guarantee that devices on the guest Wi-Fi router will have zero access to the devices on your private Wi-Fi router. Confused? Check out this video podcast for the full details:

<https://twit.tv/shows/know-how/episodes/315>

Tip 13-19. Install Custom Router Software

When you buy a Wi-Fi router, you’re actually getting two things: the hardware and the software that controls it (often referred to as firmware for appliances like this). Like a computer’s operating system, it’s possible to replace this software.

There are three main projects out there for this purpose: DD-WRT, OpenWRT, and Tomato. (The guys at Tomato definitely won the marketing war here... DD-WRT and OpenWRT just do not roll off the tongue.) These projects offer completely free, open source software that you can install on many modern Wi-Fi routers, replacing the stock firmware. This isn’t for the faint of heart, but if successful, you can add lots of great security features to your router that would normally be found on more costly routers. The security of these products is probably better, as well.

- DD-WRT: <https://dd-wrt.com>
- OpenWRT: <https://openwrt.org>
- Tomato: <https://www.polarcloud.com/tomato>

There's another great router software package called pfSense that you can run on a minicomputer that has router and firewall functions, plus many other network functions via plug-ins. You can buy pre-built systems at the following link, or you can use this site to help you build your own system. It's not cheap and you'll still need a wireless access point to pair with this if you want Wi-Fi.

<https://www.pfsense.org/products/>

Tip 13-20. Install a Reverse Firewall

Sometimes the apps you install on your computer like to “phone home,” providing the software maker or some third party with information you'd rather they not have. Remember that normal firewalls only prevent unsolicited network connections coming in from the outside. If you've installed software on your machine, that software is able to communicate freely with anyone or anything on the outside.

What you need is a *reverse firewall*. These apps will notify you of all outgoing connections and give you the opportunity to allow or block them. Fair warning: shortly after install, you're going to find out that many of your apps want to access the Internet, and you're going to have to go through a lengthy initial process of determining which of those apps you want to allow to make outgoing network connections.

- Lulu (Mac, free): <https://objective-see.org/products/lulu.html>
- Portmaster (Windows, free version available): <https://safing.io/>

Tip 13-21. Install and Use PGP

Though PGP stands for “Pretty Good Privacy,” that's an extremely modest name. PGP is industrial-strength encryption, mostly used for sending secure email but can also be used to encrypt files. Unfortunately, it's a real pain in the butt to set up and use. To make matters worse, everyone you need to communicate with must also set this up. I would actually recommend looking into GPG (GNU Privacy Guard), which is a free, open source implementation of the common OpenPGP standard. Alphabet soup, I know. But if you're at all curious, check out this website:

<https://emailselfdefense.fsf.org/en>

Tip 13-22. Host a PGP Key-Signing Party

For some real nostalgia, you can find some geeky friends to join you on your PGP project. After all, it takes two to communicate encrypted messages. In the old days, you would host a PGP key-signing party to exchange your public keys. As part of this process, each of you would positively and affirmatively vouch for each other's true identities and digitally "sign" each other's public PGP keys. This creates what is called a web of trust. See this site for everything you need to host a PGP key-signing party.

<https://www.socallinuxexpo.org/scale/18x/pgp-key-signing-party>

Phil Zimmerman once told me that the higher purpose for these key-signing parties was to socialize and to discuss and debate important topics like the right to privacy and activist causes.

Tip 13-23. Use Tor to Protect Your Identity

In Chapter 8, I mentioned using the Tor Browser for truly private web browsing. The Tor Browser uses the Tor network, which was created specifically for the purpose of providing anonymity on the Internet. Tor uses an impressive array of techniques called "onion routing" to hide the location and identity of its users. While Tor is well known and trusted by many, it's also a magnet for authorities because they pretty well assume that if you're using Tor, you're up to no good. However, it's still worth checking out, even to just understand how it works and how hard it really is to protect your anonymity.

<https://www.torproject.org>

Tip 13-24. Need to Blow the Whistle? Use SecureDrop

While you can debate whether people like Edward Snowden are heroes or traitors, there's no denying that whistleblowers have exposed some pretty egregious behavior by governments and corporations. SecureDrop is a communication system specifically designed to protect the anonymity of whistleblowers and confidential news sources, allowing them to securely communicate with news organizations. For more information, visit the following website. Note that many of the big investigative journalists will have a SecureDrop web page that you can use to communicate with them. So, you might try searching on the organization's name plus "SecureDrop."

<https://securedrop.org>

Tip 13-25. Set Up a Virtual Machine

One way to contain some secret or risky activities is to have a whole separate computer specifically for this purpose (see the next tip). However, this will obviously incur some significant costs. You can get many of the same benefits by having a virtual computer running on your regular computer. This is called creating a virtual machine (VM). A VM runs its own operating system that is separate from the OS running on the host computer. So, all the web surfing, file downloads, emails, and so on will exist in a sort of container or “sandbox.”

VMs have the capability of creating snapshots. This allows you to capture the current state of the virtual computer and return to that state at any time. So, you can do your dirty deeds and then revert to the snapshot... it's like it never happened! While you can pay money for VM software, there's a perfectly good free alternative called VirtualBox. This software runs on both macOS and Windows.

Note that you'll need to install some sort of operating system on this VM, and Windows generally won't allow you to reuse a license key for free (meaning you would need to buy another copy of Windows for the VM). I recommend Ubuntu, which is a totally free operating system with plenty of security features. See these websites for more info:

- VirtualBox VM utility: <https://www.virtualbox.org>
- Ubuntu OS: <https://ubuntu.com/tutorials/how-to-run-ubuntu-desktop-on-a-virtual-machine-using-virtualbox>

Tip 13-26. Use a Dedicated Secure Computer

While a VM is cheap and easy, you can never really be certain that there won't be some sort of information leakage between your VM and your host operating system. If you want to go full tilt, you really need a dedicated machine that is completely separate from anything you would normally use. You can save money by buying a used machine, but of course you can't be 100 percent sure that the person you bought it from hasn't somehow compromised it, so you'd better just get a new one from a big-box store.

However, if you just want to do simple things like surfing the Web and checking email, there's a nifty and dirt-cheap minicomputer called Raspberry Pi. For just \$35, you can have a fully functional Linux computer that's about the size of a deck of cards! Of course, you'll need to buy a case and a power supply for it, plus an SD card for the "hard drive," but you can get all of that in a kit for about \$60. All you need is a monitor, keyboard, and mouse, and you're set! These are fantastic little project devices (see the next tip), and they come in several other sizes and configurations.

<https://www.raspberrypi.org/>

If you go the laptop route, you'll want to replace the operating system with something secure. Look no further than Tails⁷! If it's good enough for Edward Snowden, it should be good enough for you.

<https://tails.boum.org>

Tip 13-27. Shut Your Pi Hole

Here's another fun use for a Raspberry Pi: create a custom DNS server that will block all ads for your entire household. There's an open source software project called Pi Hole that acts as a custom DNS server that blocks unwanted domains (sometimes called a "DNS sinkhole"). Not only can it block tracking and advertising domains, but it can even block known malicious websites. And when you set this up as the DNS server for your home network, all the devices in your home will automatically get the benefits.

<https://pi-hole.net>

These computers have lots of other fun uses, as well, like creating a little VPN server or a Minecraft server or a media server. The possibilities are nearly endless. Check this site for more fun ideas:

<https://pimylifeup.com>

⁷ As of this writing, Tails is only supported on standard X86 computers, not ARM computers. Raspberry Pi is an ARM-based computer. But keep checking—the RPi is very popular, and Tails may eventually support it.

Tip 13-28. Use Open Source Hardware

I've told you about open source software—software code that is available for anyone (including security experts) to review and vet. But what about the hardware? What if China is slipping in little hacking chips into the motherboard⁸? This is called a *supply chain attack*: compromise a part of a computer before it's even assembled.

There is at least one company I've found that strives to address this niche market: Purism. I'm not claiming that these devices are impervious to supply chain attacks or that the software they put on this hardware is perfectly secure. But I can tell you that these guys are trying really hard to do these things.

<https://puri.sm>

Tip 13-29. De-Google Your Android Phone

If you're willing to expend some time and effort, you can replace the stock Android operating system with a privacy-focused, open source alternative that still attempts to maintain the security of the regular Google OS. There are actually a few of these, but the one I would recommend is CalyxOS. You can use non-Google app stores like FDroid to find more private versions of Google's stock apps. You can also use the Aurora app store to download Google apps without a Google account.

<https://calyxos.org/>

⁸ Bloomberg asserted this very thing back in 2018. It caused quite the stir, but it was never really proven: <https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies>

CHAPTER 14

Parting Thoughts

Congratulations! You have just read an entire book on computer security! We've covered a ton of ground in this book. Give yourself a hearty pat on the back for reading through it all! I hope I managed to teach you some things you didn't know, in a way that wasn't boring. More than anything, I hope I've managed to convince you that cybersecurity and personal privacy are both vitally important and along the way helped you to protect your computer castle. Before I wrap things up, I wanted to share with you a few last thoughts.

Keep Calm and Carry On

While the picture this book paints might seem bleak, I don't want you to go away feeling overwhelmed or despondent. Armed with the tips and techniques in this book, you can protect yourself and your loved ones against the most of the common threats out there. Imbued with this knowledge, you should feel confident about using your computer, your smartphone, and the Internet. These tools have already changed innumerable things for the better, and we have truly only just scratched the surface of their potential.

Remember: you don't have to do every tip in this book! I haven't. Not every tip makes sense for every person. But I've given you the information you need to make the right decisions. Now it's up to you. Don't feel like you have to rush through all of these tips, either. Focus on the starred tips first, and then start working your way through the rest. I would start with the easiest ones. No reason not to pick that low-hanging fruit first.

The More the Merrier

I'd like to strongly suggest that you work through these checklists with a friend or three. Maybe create a little *Firewalls Don't Stop Dragons* book club. I'm recommending this for two reasons. First, like finding a workout buddy for the gym or a study group for a class you're taking, it's much easier to stay motivated when you're sharing the experience with others, and it's just way more fun.

Second, I wasn't kidding about the herd immunity thing. The more people that implement these sorts of basic protections, the better off we will all be. It's imperative that we educate ourselves on these topics. A functioning capitalist marketplace requires informed consumers. A functioning democracy requires informed citizens. Cybersecurity and privacy are vitally important today in both of those realms. Therefore, we need to consciously work to understand these important issues so that we create a future with products and services that protect us from cyberattacks and respect our right to privacy. I know that sounds lofty and maybe even a little overly dramatic, but I firmly believe that to be true.

Once you've worked through these checklists yourself, I encourage you to help others to implement some of the top tips in this book, as well. That can range from just giving them a copy of this book to sitting down with them at their computer to make some of these changes for them. If you want to formalize this, I've created a free set of downloadable coupons you can print off and give as gifts. It's a commitment of time and effort to help your loved ones to be more secure and private.

<https://fdsd.me/coupons>

The Case for Optimism

In the past decade or so, as the bad guys have turned to the Internet for their nefarious deeds, computer and software makers have been forced to focus more on security and privacy. However, with the revelations from Edward Snowden and all the massive data breaches at big-name companies in the last few years, security and privacy concerns have increased exponentially. Google and Apple in particular have kicked things into high gear. Google is using its dominance in web search and cloud services to push websites into adopting secure communications by default, as well as creating tools to make it easier and cheaper for them to do so. Apple has already included some great tools in macOS for encrypting your data and securely backing it up. In the wake of recent events, they've taken effective steps to lock down their mobile devices against prying eyes, as well.

Global companies like these and others need to be able to sell their products worldwide, and that requires convincing their customers that they are willing and able to secure their data. There are already multiple competitors cropping up to fill this need. This competition should light a fire under the existing corporations to get their respective acts together. Or maybe they'll just end up buying up some of these security-focused startups (like Zoom buying Keybase). But either way, we should be seeing a lot of innovation in the areas of security and privacy, and this will benefit everyone.

While there have certainly been some colossal security breaches in recent years, this is causing people to wake up and take notice. Unfortunately, things often need to get worse before they can get better. I don't think we've bottomed out yet—it takes time to implement security and privacy changes at large corporations and in computer products—but I think things have already gotten bad enough that we're on the road to recovery. While the US government seems incapable or unwilling to protect the privacy of its citizens, the European Union and states like California have implemented meaningful privacy laws that will benefit all of us.

Furthermore, the private sector has profits to protect, and they won't be waiting around for legislation. We've already seen this happening, and I expect to see a lot more in the next year or two. The cases involving the FBI and Apple that hit in early 2016 and late 2019 are prime examples. When these high-profile incidents occur, they will force us to debate these issues and take action. So, while we are not out of the woods yet, I think we're making progress. At the very least, privacy rights are finally being debated openly and earnestly.

Don't Take This Lying Down

Despite the market pressures that are driving increased security, there are still plenty of places where maximizing corporate profits does not directly align with maximizing consumer protections—particularly in the area of privacy. For this reason, it's absolutely essential that regular people like you get educated and get involved. If consumers and citizens don't demand security and privacy, then corporations and governments will be free to put their own interests first, protecting their profits and power.

Regardless of what you believe is the proper balance between freedom, privacy, capitalism, and democracy, you can't really participate in the debate or make informed choices unless you understand the underlying issues. I don't mean you have to

understand all the deeply technical details, but you need to know enough to evaluate competing products and different policies. I've tried to give you a good foundation with this book, but I urge you to seek out more information and stay informed. See the checklist in this chapter for several suggestions.

I encourage you to take it one step further, however. Don't just get educated; get involved. I'm not encouraging every reader to put down this book and go march in protest (though that would be wonderful). There are many simpler ways you can make a difference. For one thing, you can pay others to do it for you. That is, you can donate to groups that are already fighting for your rights and putting pressure on corporations and governments to do the right thing. You don't have to donate a lot, either—even a little money can make a big difference, if enough people do it. Just being an enrolled member of these organizations helps to give them more clout. It gives them a long list of everyday people who made a point to say, "I agree with what these guys are doing; please listen to them." Again, see the list at the end of this chapter for some ideas.

You can also spread the word to others. As these issues inevitably hit the news, discuss and debate them with coworkers at the water cooler (or on Zoom), at home with the family over the dinner table, or with friends at the next party or sports event. It doesn't have to be confrontational—keep it friendly and informative. But it's essential, as a society, that we address these issues. We can't ignore them any longer.

Of course, in a representative democracy, the people who are supposed to be your advocates are the people you elect to represent you in the halls of government. However, with campaign finance laws being what they are, these folks are unfortunately much more likely to listen to the needs of their largest donors. Nevertheless, you cannot let that stop you from trying. The real problem in the United States is that many people have given up. Voter turnout in this country, though increasing, is still low compared with other democracies. I think people are just tired of the mudslinging and backroom dealing. To paraphrase an old hippie mantra, they've tuned out, turned off, and dropped out. The problem with disengaging is that it leaves the more extreme factions and wealthy people in charge. Security and privacy are not partisan issues; they affect us all, no matter what your particular leanings may be. I encourage you to stay involved and to vote every chance you get—not just in national elections but in local ones, as well. If we could get just 5 percent to 10 percent of the people who have given up on voting to get back out there, it could easily turn the tide.

In the meantime, write your elected representatives. For those of you in the United States, you can use the following link to find out who represents you and how to contact them. While online notes are convenient, real “snail mail” letters and phone calls still hold more sway—precisely because they take effort.

<https://www.eff.org/congress>

Finally, as you see companies trying to do the right thing and bringing new products to market, support them with your pocketbook whenever you can. We need to shift away from an Internet economy that is based on advertising. That’s going to mean paying for things that used to be “free.” Also, when given the choice, we need to favor products that do a better job of protecting our privacy and enhancing our security.

Similarly, you should support politicians who stand up for individual privacy and stand against the rampant, unregulated gathering of personal data by corporations. The first step is awareness—these companies simply must be 100 percent transparent about what data they collect, what they do with it, and who they share it with. Once we understand the true breadth and depth of this campaign to Hoover up all our highly personal data, I think we’ll find the political will to make necessary changes.

Summary

- Remember that this book is a lot like sex ed class: by nature, it focuses on the possible negative outcomes and takes most of the positive ones for granted. Don't let this frighten you. Don't avoid technology. Now that you understand it, you can embrace it and proceed with confidence, respecting risks and girding yourself with commonsense precautions.
- Work your way through the top tips first, and then circle back to the rest. Start with the lowest hanging fruit and work your way up. Find some friends to do it with you—you'll have more fun and get more done.
- When you have your own digital house in order, help your friends and family next. When the opportunities arise, have conversations about cybersecurity and privacy. Spread the word.
- Stay educated and get involved where you can. Favor products and services that try to do the right thing, even if they cost more money. Favor elected representatives who will protect your privacy rights and fight for laws to improve our collective cybersecurity.

So...did you find the Easter egg? Okay, I'll give you a hint: it's in one of the QR codes.

Checklist

There are several other ways for you to make a difference and gain further knowledge. In this checklist, I've gathered together some key resources you can use to continue your education and get a different perspective on the topics I've covered in this book. I'll also tell you about organizations that you can support that are out there working hard to protect your rights.

Many of the items in the following tips are also listed in the Resources section of my website. I've posted reviews of some of these books in my blog (also on this website).

<https://firewallsdontstopdragons.com/resources/>

Tip 14-1. Expand Your Security and Privacy Education

Books

If you liked this book, you should seriously consider reading some of the following books:

- *Data and Goliath* by Bruce Schneier (W. W. Norton & Company, 2016). Schneier literally wrote the book on cryptography but in recent years has become a leading voice on public policy. He's testified many times before Congress. His (recent) books are easy to read, extremely insightful, and compelling. If you like this book, you might also try *Click Here to Kill Everybody* or *A Hacker's Mind*.
- *Privacy is Power* by Carissa Véliz (Melville House, 2021). If you're still not convinced of the importance of privacy in society, you need to read this book. The author breaks it down for you and clearly explains why privacy is a human right and why it matters.
- *No Place to Hide* by Glenn Greenwald (Metropolitan Books, 2014). Glenn Greenwald was selected by Edward Snowden to manage the release of highly sensitive information regarding warrantless NSA mass surveillance. This book chronicles this engagement and helps to explain the importance of Snowden's bombshell revelations.

- *The Code Book* by Simon Singh (Anchor, 2000). If you find the concept of cryptography as interesting as I do, this book traces the history of ciphers and cryptanalysis in an engaging and entertaining way.
- *Little Brother* by Cory Doctorow (Tor Teen, 2010) (fiction). If you prefer to be entertained while you learn about cryptography and why it's so crucially important to democracy and society, this is a must-read. This book talks about a not-too-far-fetched future where law enforcement agencies overreact to a terrorist attack and trample civil liberties in a quest for "security." Seriously, just read it—it's short and fun.
- *Extreme Privacy* by Michael Bazzell (independently published, 2022). This book is exactly what it sounds like and is overkill for most people. However, you might still find it interesting to see the kinds of techniques that can be used to aggressively scrub your data and minimize your digital profile.

Documentaries and Movies

If you prefer to learn by watching, here are some excellent documentaries about privacy and cybersecurity:

- *The Great Hack*: This Netflix documentary gives a behind-the-scenes look at the Cambridge Analytica scandal. Lax policies by Facebook allowed this company to amass a treasure trove of personal data that let them influence the 2016 US election, Brexit in the United Kingdom, and elections all around the world.
- *Terms and Conditions May Apply*: This is about online privacy and what sorts of things you're signing away in end-user license agreements (EULAs).
- *CITIZENFOUR*: This is about Edward Snowden and how his initial information was given to reporter Glenn Greenwald.
- *Frontline: The United States of Secrets*: This is a great two-part show from PBS.

- *Code 2600*: This is a great film about the humble beginnings of the hacker culture and how cybersecurity has become much more serious with the advent of the Internet.
- *Anon*: This Netflix movie shows a dystopian future where no one is allowed to be anonymous. Every human has a built-in scanner and display in their eyeballs, allowing them to identify anyone they meet. Trouble comes when a hacker starts deleting memories and people.
- *Minority Report*: Tom Cruise plays a detective in a future where “pre-cogs” can see crimes before they happen. The cops swoop in and arrest people for these “pre-crimes.” But apparently the visions of the three oracles don’t always agree.

Blogs and Websites

The following websites are chock-full of useful information and not super technical:

- Techlore: <https://techlore.tech/>
- Privacy Guides: <https://www.privacyguides.org/>
- Hitchhiker’s Guide to Online Anonymity: <https://anonymousplanet-ng.org/>
- Spread Privacy blog: <https://spreadprivacy.com>
- The New Oil: <https://www.thenewoil.org/>
- Restore Privacy: <https://restoreprivacy.com>
- All Things Secured: <https://www.allthingssecured.com/>
- Defensive Computing Checklist: <https://defensivecomputingchecklist.com/>

Podcasts

If you haven’t tried podcasts before, they’re basically radio shows that you can download from the Internet. Most people listen to them using a smartphone app while they commute or travel or perform some mindless task. Some podcasts have video, as well, making them more like TV shows. There are thousands of them out there on every topic imaginable, for every taste and education level.

- *Firewalls Don't Stop Dragons*: My podcast! You can find it on my website (on the Podcast tab) as well as the usual podcast outlets (Apple Music, Google Play, Spotify, Stitcher, Amazon, etc.). The show comes out once a week on Mondays and runs about an hour. I toggle back and forth between news and interviews of top experts in the field of security and privacy.

<https://podcast.firewallsdontstopdragons.com>

- *Security Now!*: This is where I really got into security, and I listen to this podcast religiously. While it can get a little technical and often times the hosts get off on sci-fi tangents, it's always fun. It comes out once a week on Tuesdays and runs over two hours.

<https://twit.tv/shows/security-now>

Tip 14-2. Fight the Good Fight (or at Least Fund It)

The following organizations are doing some excellent work on behalf of everyday people. Take a look at their websites, and if you like what you see, send them a little money. If they send you a sticker or magnet, proudly display it where others will see.

- Electronic Frontier Foundation: <https://www EFF.org>
- Electronic Privacy Information Center (EPIC): <https://epic.org>
- Center for Democracy and Technology (CDT): <https://cdt.org>
- Fight for the Future: <https://www.fightforthefuture.org/>
- Mozilla Foundation (Firefox): <https://foundation.mozilla.org/>

Tip 14-3. Spread the Word, Help Others

As I've been wrapping up production of this book, I've found myself wondering how we can reach more people and build up that "herd immunity." In the process, we need to have more discussions about privacy and the dangers of surveillance capitalism. I mentioned a couple ideas in this chapter, like spreading the word and helping others directly. You could host a book club around this book or even put together an informal seminar around the top tips in this book. If you have the time, you should help others to implement the top tips too.

But I got to thinking that I could do more to facilitate these activities. I have several ideas in my head for free, downloadable workbooks that can assist with the preceding ideas. If these turn out to be popular, I'll probably add more over time. So, check out the book's website to see what I've cooked up, and check back periodically for additional content. You can also scan the QR code (Figure 14-1).

<https://firewallsdontstopdragons.com/book-updates>



Figure 14-1. QR code for book updates

Glossary

Application (app). Pieces of software that you launch on your computer to help you do something. Examples include Microsoft Word, Internet Explorer, Firefox, iTunes, Photos, and Outlook. On smart devices, applications are usually just called “apps.”

Bandwidth. Used to describe how fast data can travel over a given connection. You most often see this when your Internet service provider tells you how fast you can download something from the Internet.

Bit. The smallest piece of computer data. This can be either a 0 or a 1, making it binary.

Bitcoin. A virtual currency (or cryptocurrency) that maintains its global integrity and accounting ledger using cryptographic methods. Often requested as ransom payments because it’s difficult to track.

Bluetooth. A short-range, low-power wireless technology mostly used to remove the need for wires. Commonly used with wireless headsets, computer mice, keyboards, and sometimes remote controls.

Browser. See web browser.

Byte. A chunk of computer data equal to eight bits. When talking about many bytes, we use metric prefixes like kilo- (thousand), mega- (million), giga- (billion), and tera- (trillion).

Cloud, the. Refers in a general, vague way to all the services and servers out on the Internet. When you store data “in the cloud,” it’s stored on some big computer on the Internet that’s run and owned by a company or service provider.

Credential stuffing. When bad guys manage to hack or guess someone’s password on one site, they immediately try this same login on other sites. This process is usually automated.

CPU. Central processing unit (or sometimes just “processor”). This is basically the “brain” of your computer or smart device. It controls everything else and runs the operating system.

Download. If you think of the Internet as the “cloud,” then it should make sense that data coming from the Internet to your computer or smartphone would be coming “down” (downloading). When you send data to the cloud, this direction is “up” (uploading).

Encryption. This is a process that turns regular text into unreadable gibberish to keep it private. If you have the right password or key, and you know the encryption algorithm, you can reverse this process to get the original plain text back—called *decryption*.

Ethernet. The technical name of the standard used to connect computers to a network using wires. Ethernet cables look like home phone cables, but the rectangular clip connector at the end is wider.

File manager. The name for the operating system tool that lets you view, move, copy, rename, or delete files. On Windows, this is called the File Explorer; on Mac, it’s called the Finder.

Firewall. A firewall is sort of a one-way data valve: you use it to block data transfers in a particular direction. Most commonly, this is a function of your router that allows requests to leave your home network and their responses to come back but blocks any unsolicited requests coming into your network.

Gigabyte. One billion bytes.

Hardware. The parts of a computer that you can see and touch: the computer, monitor, keyboard, mouse, printer, webcam, and so on.

GPU. Graphics processing unit. This is sort of a specialized CPU that is dedicated to doing all the video processing. Simple GPUs can be built into the motherboard, but high-power GPUs often used by PC gamers come on dedicated, separately installed circuit boards.

HTML. Hypertext Markup Language. This is a format specification for web pages. What you see in a web browser is *rendered* HTML. Want to see the real thing? Right-click any web page and select “view page source.”

HTTP/HTTPS. Hypertext Transfer Protocol (Secure). This is the first part of most web addresses (URLs). This is the protocol, or standard, that defines how you send data to and from a server on the Internet. If the “s” is present, that means the connection is secure (encrypted).

Internet/intranet. The Internet refers to the massive global network of computers that allows us to surf the Web, stream Netflix, send email, and so on. The intranet is a private network, inside your home or a business. (See also WAN and LAN.)

IP address. Internet Protocol address. IP is an even more basic protocol than HTTP—it's the really low-level standard for transferring data over a network. Data is transferred between two network points, and each point has a unique network address, like a mailing address. IP version 4 (IPv4) addresses look like 10.0.0.1 or 192.168.0.59. IP version 6 (IPv6) addresses are much longer and look like 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A.

ISP. Internet service provider. This is the company that gets you connected to the Internet. Examples are Comcast, Spectrum, Verizon FiOS, and Google Fiber. When you connect to the Internet with your smartphone, your ISP is your cellular provider.

Kilobyte. One thousand bytes.

LAN. Local area network. Your home network is a LAN, as is the network at the office where you work. LANs are smaller, private networks or intranets (as opposed to the Internet).

Malvertising. Web advertising that contains links to malicious websites or actual malicious software that runs in the ad itself.

Malware. Software that is built to do “bad” things, ranging from giving you annoying advertisements to actually corrupting or controlling your computer. Examples include viruses, spyware, and Trojan horses.

Megabyte. One million bytes.

Modem. A small box that converts your Internet service provider's special type of connection (cable, phone line, fiber optic, or satellite) to a standard network connection (Ethernet). You usually rent this box from your ISP. Sometimes these modems will also include a built-in Wi-Fi router.

Motherboard. This is the main circuit board inside a computer that holds the CPU and RAM and has connections to other internal parts like video cards, network cards, fans, power supply, and so on. (Smaller circuit boards that connect to the motherboard are often referred to as daughterboards.)

GLOSSARY

Multifactor authentication (MFA). Requiring more than one form of authentication. Single factor is usually just a password. Two-factor authentication (2FA) adds something like a rolling time-based PIN code. In most cases, it doesn't really go past two factors, but some people still prefer to call it "multifactor" instead of "two-factor."

Net neutrality. A concept that says everyone should have equal and fair access to everyone else on the Internet—companies with more money shouldn't be able to get privileged access.

Network. Two or more computers or devices that are connected and communicate using a common language, or protocol. Networks today use Internet Protocol (IP).

Operating system. A special piece of software that runs the entire computer. Examples include Microsoft Windows and Mac OS X.

Phishing. A scheme to trick you into giving up secret information like your password, credit card number, social security number, and so on. This is usually done with a fake email asking you to log in or provide info to fix a nonexistent problem.

Ransomware. A particular type of malware that surreptitiously encrypts all of your computer's files and then demands payment to decrypt them.

Router. The box on your network that separates your local area network (LAN) from the Internet. In most homes today, the router is a Wi-Fi router.

Sandboxing. In security terms, this means running software in a virtual software container to prevent it from accessing files or making changes to anything outside the container.

Server. Fancy name for a big computer out on the network whose job it is to do something for you. It might hold your email or let you buy something online or stream you a movie. Your computer (the one requesting something) is the *client*.

Software. The general term for any program that runs on your computer, including applications and the operating system.

Spam. Unwanted or junk email.

Terabyte. One trillion bytes.

Two-factor authentication. See "multifactor authentication."

Upload. See download.

URL. Universal Resource Locator. This is a web address like <https://google.com>. When pronounced like a word, it rhymes with “earl.”

WAN. Wide area network. This usually refers to the Internet, but it may also refer to a large corporate network that spans many sites.

Web browser. The software application we use to surf the Web, on a computer or a smart device. Examples include Chrome, Firefox, Safari, and Edge.

Wi-Fi. The wireless communication standard used by computers and smart devices to connect to the network. This is also referred to by the technical name 802.11.

WLAN. Wireless LAN. This is the type of network created by a Wi-Fi router.

Index

A

- Abagnale, Frank, 79
- Account recovery, 483, 484, 545
- Active advertising, 367
- Ad blocking, ethics, 366–368
- Admin account
 - Mac OS
 - administrator password dialog, 272, 277
 - logout menu, 273, 277
 - remove administrator confirmation dialog, 274, 278
 - restart menu, 275, 279
 - users/groups preferences, 138, 250, 252, 271–273, 275, 276, 278, 427
 - users login options, 252
 - Windows 10
 - accounts search, 263
 - add user, 264
 - answer security questions, 266
 - change account type dialog, 266, 270
 - change account type, to administrator dialog, 267
 - change account type, to standard user dialog, 271
 - create account dialog, 265
 - family and other users settings, 263
 - local account, creation, 263
 - login screen, 269
 - sign-out menu, 267, 268
- Adult content, 489
- Adware, 76, 175, 529
- Alexa, 46, 72, 326, 344, 345
- Alias, 83, 200, 201, 204, 413, 414, 421, 434–436, 470, 471, 478, 499, 530
- Alphabet character mappings, 87
- Amazon, 10, 40, 46, 72, 81, 321, 326, 337, 344, 345, 347, 354, 357, 358, 365
- AMD, 79
- Ancestry, 449, 451, 482
- Android, 16, 30, 40, 41, 56, 111, 185, 205, 218, 339, 405, 419, 432, 453, 484, 503, 505–507, 510, 513, 514, 517–529, 532, 534–537, 539, 552, 558
- Antivirus (AV) software, 5, 6, 233, 241, 242, 279, 280, 282, 283, 546
 - installation
 - Mac OS, 282, 283
 - Windows 10, 280
- AOL Instant Messenger, 404
- Apple, 10, 15, 16, 25, 28, 30, 46, 56, 64, 108, 110–112, 116–118, 121, 125, 126, 128, 129, 132, 133, 138, 164, 169, 172, 173, 175, 176, 185, 214, 218, 234, 236–240, 244, 246, 271, 273–275, 277, 279, 283, 285, 286, 291, 302, 306, 309, 312, 318, 326, 327, 345, 347, 349, 368, 369, 374, 404, 405, 409–411, 419, 431, 434, 435, 441, 442, 445, 453, 462–469,

INDEX

Apple (*cont.*)

471, 472, 486, 498, 505–507,
509–511, 513, 517, 518, 520–522,
525–529, 531, 533, 534, 536, 539,
560, 561

Apple Cash, 442, 472, 498

Apple credit card (Apple Card), 471

Apple online account

lock down

disable Keychain backup, 464, 468

iCloud settings, 462, 463, 466, 467,
528, 534

security & privacy settings, 285, 287,
462, 465, 469

Apple Pay, 441, 442, 451, 471, 472

Apple's drive encryption utility (FileVault),
240, 293–297

ASCII, 65

Asus, 25, 335, 336

Asymmetric encryption, 93, 95, 96,
184, 416–418

AT&T, 44, 72, 404, 517

Attackers, 2, 5, 6, 73, 90, 113, 190, 239, 322,
324, 338, 353, 545

Attack surface, 113, 245, 509

Authentication, 84, 95, 101, 179–182, 184,
197–200, 203, 204, 213, 216, 246,
247, 322, 470, 478, 512, 536,
545, 550

Authentication and message integrity, 95

Authenticator, 213, 215

Authy, 213, 216–218, 470, 550

Automatic Content Recognition (ACR),
326, 347

Automatic voltage regulation
(AVR), 164

Automobiles, 8

Auto-update

Mac OS, 175

Microsoft Windows 10, 173, 174

Availability, 85, 100

B

Backblaze, 109, 147–159, 161–163, 211,
286, 288, 548

Backups

cloud service

Mac OS, 240, 453, 462, 463, 466, 480

Windows 10, 519

data, 107–109

encryption, Mac OS, 125, 128–131

system preferences, 142, 159, 172,
253, 275, 287, 290, 295–297, 307,
375, 465, 466, 469

time machine backup password
dialog, 140, 145

time machine disk selection
dialog, 138

time machine preferences, 142

external hard drive

connect to computer, 133

drive size, 133

Mac OS configuration, 133

Microsoft Windows 10

configuration, 133

USB version, 132

online, 109, 110, 132, 146, 445

options, 132

software, 108, 133, 547

UPS, 163, 164

viruses/malware, 108, 109

Bandwidth, 68, 71

Banking/shopping online, 439–443

Belkin, 335, 336

Biometric *vs.* PIN, 512, 513

Biometrics, 35, 181, 219, 246, 247, 512, 513, 516, 524, 525, 550
 Bitcoins, 75, 78, 85, 325, 412, 548
 BitLocker, 240, 292
 Bitly, 407
 Bits, 64–66, 68, 71, 81, 83, 103, 109, 112, 242, 297, 298, 360
 BitWarden
 account sign-up form, 207
 App installation, smartphone, 218
 authenticator, 213
 browser icons, 217
 copy password, 220, 223, 228
 deleted saved passwords, 222–223
 disable password saving, 222–223
 “Fill” button, 219, 220
 generate strong passwords, 139, 151
 offline passwords, 239–230
 one-time passwords
 generation, 230–231
 passwords adding, 209
 password vault, 209, 210
 saved passwords, 219
 security challenge, 226
 security, country restrictions, 234
 store credit cards, 225
 two-factor authentication, enabling
 authenticator setup, 215
 multifactor options, 214
 QR code, initializing
 authenticator, 216
 vault tour, 217
 web browser, installation, 208
 welcome message, 206
 Bletchley Park, 91
 Blogs and websites, 567
 Bluetooth, 3, 69, 323, 508, 509, 532, 533, 542

Bluetooth wireless technology, 182
 Bob’s public key, 100
 Bot, 76, 77, 239, 325
 Botnets, 77, 78, 325, 332
 Brave browser, 370, 374
 Broadband, 34, 71, 109, 237, 315
 Brute-force attack, 190, 203
 Built-in security features, 152, 157, 238–240
 Bytes, 64, 65, 68, 81, 83, 103, 109, 242, 297, 298

C

Cable modem, 316, 336, 553
 California Consumer Privacy Act (CCPA), 48
 California Privacy Rights Act (CPRA), 48
 Calyx, 505, 507
 Cambridge Analytica (CA), 12, 53, 355, 447
 CAPTCHA, 77, 331, 497
 CA scandal, 41, 447, 566
 Cash App, 441, 471
 Castle guards, 5, 6, 61–106, 234
 Central processing unit (CPU), 79, 80
 Certificate authorities (CAs), 351, 353, 354, 372
 Certificates, 351–354, 372, 382, 551
 Children’s Online Privacy Protections Act (COPPA), 501
 A Christmas Story, 88
 Chrome, 41, 56, 64, 208, 221, 223, 246, 349, 366, 368–370, 373, 374, 396, 407, 529
 Chrome browser, 56, 370, 374, 507
 Chrome OS, 111, 349
 CIA Triad, 85, 100
 Cipher, 86–92, 299, 566

INDEX

Cipher text, 86, 89, 90
Clean up
 Mac OS, 167, 168
 Microsoft Windows 10, 165–167
Clearview AI, 46
Client, 70, 185, 322, 407, 434, 531, 548
The cloud, 25, 34, 70, 81, 107, 109–112,
 146–163, 213, 326, 328, 332, 349,
 402, 445, 446, 505, 518, 519
Cloud backup, 108–112, 119, 133, 146, 518,
 520, 548
Cloud computing, 70
Cloudflare, 397–399, 503
Cloud storage services, 439, 445, 446, 464,
 467, 475
Coalition Against Stalkerware, 538
Comcast, 318, 319, 344
Comey, James, 34
Common Sense Media, 485, 504
Communications
 e-mail, 402–404, 431
 secure, 354, 355, 416, 421, 423, 560
 text messaging, 401, 404, 405, 414, 415,
 419, 421, 431, 470
Computer
 beware cold calls, 313
 sale and donation, checklist
 Mac OS, 302
 Windows, 301, 302
 unplug webcams, 313
Confidentiality, 85, 95, 100, 103
Controlled folder access, 236, 282,
 284, 285
Cookies, 45, 48, 330, 359, 360, 362, 372,
 391, 394
Cortana, 326, 345
Credential stuffing, 12, 189
Credit bureaus, 360, 443, 444, 473, 474, 551

Credit card fraud, 10
Credit freeze, 444
Cryptanalysis, 89, 566
Cryptographic hashing function, 96, 97
Cryptography, 53, 84–86, 89, 91, 102, 104,
 526, 565, 566
Cryptomining, 78
Customs and Border Protection
 (CBP), 514
Custom Wi-Fi router software, 553
Cyberbullying, 487, 488, 492

D

Darik's Boot and Nuke (DBAN), 552
Data at rest, 93, 110
Data brokers, 42, 47, 114, 448, 514
Data in motion, 93, 110
Data minimization, 113–115, 120
Decryption algorithm, 91, 92
Dedicated guest Wi-Fi router, 553
Dedicated secure computer, 184, 556
Deep Blue, 506
Deep fakes, 58
Default SSID, 342, 343
Defense in depth, 5, 6, 213
Department of Homeland Security
 (DHS), 514
Detection, 4, 6, 73, 78
Device encryption, 292, 293
Differential privacy, 51
Digital basket, 192, 213
Digital estate planning, 551
Digital executor, 550, 551
Digital information, 486
Digital mailbox, 83
Discord, 404
Disk encryption

- Mac OS, 293, 295–297
- Windows 10, 292
- Distributed denial of service (DDoS), 77
- D-Link, 335, 336
- DNA, 449–452, 482, 483
- DNS settings
 - Firefox settings search, 398
 - IPv4, 397
- Documentaries, 566
- Domain Name Service (DNS), 83, 331, 354, 364, 372, 396–399, 503
- Downloading, 19, 56, 81, 173, 241, 312, 394
- Dox-Ray machine, 96–100
- Dropbox, 70, 111, 446, 464, 467, 475, 519
- DuckDuckGo, 384, 413, 435, 502, 529
- Dynamic Host Configuration Protocol (DHCP), 320, 364
- DynDNS, 325

E

- E2EE, 414, 418, 419, 431
- Echo, 72
- Eero, 337
- 802.11, 67, 317
- Electronic frontier foundation (EFF), 23, 361, 539, 568
- Elliptic curve cryptography, 102
- E-mail
 - account activity info, 437
 - attachments, 74, 106, 418, 433
 - encrypted service, 423, 424
 - hacking, 11
 - unused accounts, 436, 437
- E-mail account is hacked, 544
- Encrypted communications
 - mechanism, 415
- Encrypted E-mail service, 423, 424

- Encryption, 33, 34, 53, 54, 80, 84–86, 92, 93, 96, 101–103, 110–112, 138, 143, 147, 150, 151, 156, 157, 162, 163, 193, 292, 293, 298, 300, 322, 329, 338, 403, 404, 414–420, 424, 425, 431, 432, 446, 475, 507, 525, 526, 554
- Encryption algorithm, 91, 92, 101
- End-to-end encryption (E2EE), 405, 414, 415, 419, 420, 431, 433, 525
- End-user license agreement (EULA), 45, 238, 476, 566
- Enigma, 91
- Equifax, 12, 443, 444, 474, 551
- Ethernet, 67, 317, 322, 340, 347
- Ethernet cable, 67, 317, 322, 340, 347
- Exchange Image File format (EXIF) data, 449, 479
- Experian, 443, 474, 551
- Exploit, 72, 73, 79, 90, 113, 115, 242, 279, 368, 434, 527
- External backup hard drive, 108
- External hard drive, 67, 108, 109, 111, 112, 119, 132–134, 136, 291, 548

F

- Facebook, 7, 12, 20, 36, 38, 41, 42, 46, 47, 50, 53, 56, 71, 114, 186, 189, 257, 265, 313, 355, 361, 368, 447, 451, 476–478, 480–482, 507, 526, 529, 566
- Facebook Messenger, 404, 419, 431, 512
- Fake email, 409–412
- Fast Identity Online (FIDO), 182–184
- Fastmail, 435, 436, 499
- FIDO hardware key (YubiKey), 182
- File deletion, 108

INDEX

File manager, 64
FileVault, 240, 293–297
Find My, 241, 304–309, 464, 468, 498,
 528, 534
Find My Mac, set up, 306
Finsta, 486, 487
Finsta account, 486
Firefox, 222, 223
 add-ons menu, 393
 DNS over HTTPS setting, 399
 extension, 385
 installation, 206, 375, 383, 391, 393, 399
 security and privacy settings
 certificates settings, 382
 data collection and use settings, 381
 do not track setting, 378
 enhanced tracking
 protection, 376–378
 forms and passwords settings, 390
 history settings, 379
 permissions settings, 380, 381
 security settings, 382
 updates settings, 383
 send files securely
 secure download link, 430
 settings search for DNS, 398
Firewall, 5, 196, 239, 321, 322, 324, 332,
 341, 554
Firmware, 338, 553
Fitbit, 41
Frequency analysis, 90
Full hard drive encryption, 240

G

GCHQ, 84, 322
General Data Protection Regulation
 (GDPR), 48, 56, 478

Gigabits per second (Gbps), 68
Gigabyte, 65, 112, 132
Gmail, 41, 56, 189, 197, 402, 434, 499
GNU Privacy Guard (GPG), 416, 554
Going dark, 34
Google, 16, 24, 36, 38, 40–42, 47, 50, 56, 57,
 64, 70, 71, 76, 81, 111, 114, 185,
 197, 213, 246, 323, 326, 345, 349,
 353, 354, 366, 368–371, 373, 374,
 384, 391, 395, 396, 402, 403, 405,
 434, 437, 441, 451, 462, 466,
 476–478, 482, 484, 499, 505–507,
 509–511, 514, 517–519, 522,
 526–529, 535, 545, 558, 560
Google Assistant, 326, 345
Google Authenticator, 470
Google Drive, 70, 111, 475, 519
Google Pay, 441, 451, 471
Google's search engine, 384
GPG Suite, 416
Grandmother Rule, 487, 502
Guest network, 338, 339, 553

H

Hard drive, erase, 298, 300, 552
Hardware, 3, 63, 64, 79, 101, 104, 116, 134,
 182, 183, 215, 292, 311, 320, 334,
 506, 553, 558
Hardware and software
 bandwidth, 68
 bits/bytes, 64
 bluetooth, 69
 clients and servers, 70
 cloud, 70
 file manager, 64
 IoT, 72
 net neutrality, 71

- networks (wired and wireless), 67, 68
- storage, 66
- Hardware bugs, 79
- Hashing, 95, 97, 103, 188
- Have I Been Pwned, 546
- Health Insurance Portability and Accountability Act (HIPAA), 41
- Homomorphic encryption, 51
- HTTPS everywhere, 485, 486, 502
- Hypertext Transfer Protocol (HTTP), 94, 328, 350, 365, 382

I

- iCloud, 111, 112, 237, 238, 240, 241, 254, 294–297, 302–307, 309, 411, 419, 434, 453, 462–464, 466–468, 475, 507, 518, 519, 525, 528, 534, 545
- Identify theft, 443
- Identity fraud, 11
- Identity theft, 11
- ID theft after death, 551
- Immigration and Customs Enforcement (ICE), 514
- Information leakage, 364–368, 556
- Infrared (IR) remotes, 69
- Instagram, 46, 56, 447, 477, 480, 481, 486
- Instant messaging (IM), 404
- Integrity, 85, 95, 97, 100, 103
- Intel, 63, 79
- Internet
 - adult content, 489
 - downloading, 19, 81, 173
 - HTTP, 94, 329, 350, 365
 - mailbox, 81, 83
 - packets, 84, 94, 103, 316, 350, 396

- routing, 68, 82
- uploading, 81
- USPS, 81
- Internet is everywhere, 485, 486, 502
- Internet of Things (IoT), 72, 77, 318, 323–328, 332, 340, 553
- Internet Protocol (IP), 67, 82, 316, 319, 320, 327, 329, 342, 437, 503
- Internet Protocol address (IP address), 56, 82–84, 316, 320, 321, 329, 335, 342, 345, 354, 364, 396, 437, 503
- Internet service provider (ISP), 44, 56, 68, 71, 110, 315, 316, 318–321, 328–331, 334, 336, 342, 344–346, 364, 396, 402, 436
- Intranet, 315
- Intrusion detections systems (IDSs), 6
- IP version 6 (IPv6) versions, 82, 327, 342, 397

J

- Jabber, 404
- Jailbreaking, 509, 537
- Jitsi, 433
- Juice jacking, 540
- Junk emails, 10, 57, 76, 201, 343, 405, 407, 412

K

- Keka, 426–429
 - compression preferences, 427
 - encrypted archive, creation, 429
 - file save dialog, 429
 - password-protected archive
 - settings, 428
- Key loggers, 310

INDEX

L

LastPass, 205, 245, 254, 257, 264, 265, 272, 276, 295, 297, 337
Least privilege, 234–236, 242, 245, 510, 522
LibreOffice, 434
LinkedIn, 41, 46, 56, 447, 458, 476, 477, 481
Linksys, 335, 336, 346
Local area networks (LANs), 67, 315, 317, 324, 332
Lockdown Mode, 309, 310, 513, 539, 540

M

Mac configuration, 128
Mac OS Time Machine backup, 145
Macs Are Safer Than PCs, 233
Mailbox, 37, 81, 83, 84, 411
Mailbox.org, 431
Malicious software
 malware, 7, 11, 73, 75–78, 108, 109, 176, 199, 233, 235, 241, 244, 246, 253, 254, 262, 271, 282, 283, 309–311, 313, 337, 344, 367, 394, 405, 408, 421, 423, 434, 493, 510, 529, 538, 539, 546, 547
Malvertising, 367, 368
Malware, 7, 10, 73, 77, 78, 108, 109, 176, 199, 233, 235, 241, 244, 246, 253, 254, 262, 271, 282, 283, 309–311, 313, 324, 337, 344, 367, 394, 397, 405, 408, 421, 423, 434, 493, 510, 529, 538, 539, 546, 547
 bot, 76
 components/behaviors, 241
 cryptomining, 78
 potentially unwanted program (PUP), 76
 Ransomware, 75
 rootkit, 78

 Scareware, 75
 spyware, 76
 Trojan, 74
 virus/worm, 73, 74
Man-in-the-middle attack, 95, 354
Marketing data analysis, 360
Mastercard, 41, 442, 471
Master password, 192, 194, 195, 198, 203, 206, 207, 209, 215, 217, 218, 245
McAfee, John, 449
Megabits per second (Mbps), 68, 109
Megabyte, 65
Meltdown, 79
Metadata, 38, 329, 331, 346, 355, 402, 449, 479, 480
Microsoft, 15, 64, 70, 81, 104, 106, 111, 112, 115–118, 121–124, 164, 166–169, 173, 174, 176, 185, 234, 236–240, 246, 247, 254, 255, 257, 262, 265, 283, 284, 291, 298, 300, 303, 304, 326, 345, 349, 366, 370, 396, 434, 445, 447, 453, 458, 459, 462, 466, 476, 479, 497, 545, 546
Microsoft account, 237, 238, 254–256, 262, 264, 292, 303, 453, 459, 494, 545
Microsoft online account
 lock down
 activity history settings, 458
 diagnostics & feedback settings, 456, 460
 general privacy settings, 455, 460
Microsoft's encryption utility, 240
Mint.com, 442
Mirai botnet, 325
Mobile-oriented messenger apps, 404
Mobility, 8
Modem, 237, 239, 315–319, 327, 328, 332, 334, 336, 341, 344, 541, 553

Moderate password, 245
 Modern cryptography, 89, 91, 93
 Moore, Gordon, 63
 Moore's law, 63
 Multifactor authentication, 197
 Multiparty video chats, 432

N

National Consumer Telecommunications
 and Utilities Exchange
 (NCTUE), 444
 National Network to End Domestic
 Violence, 538
 National Security Agency (NSA), 2–4, 13,
 37, 84, 301, 565
 Near-field communication (NFC),
 508, 533
 Netflix, 37, 71, 72, 81, 326, 331, 332, 340,
 345, 347, 447, 508, 566, 567
 Netgear, 335, 336
 Net neutrality, 71
 Network, 9, 34, 44, 49, 64, 67, 68, 70, 71, 74,
 77, 82, 86, 198, 238, 239, 244, 279,
 315–325, 327–329, 331, 332, 334,
 337–340, 344–346, 356, 364, 371,
 397, 399, 440, 489, 532, 547,
 553–555, 557
 cable modem, 316, 336, 553
 Wi-Fi router, 317–320, 322, 336–338,
 342–344, 553
 Network Address Translation (NAT), 320,
 321, 327, 332
 Networks, 332, 367
 Nitty-gritty certificate
 information, 351
 Non-admin accounts, 234–236, 244,
 253, 510

O

Offline attacks, 185, 186, 191, 245
 On-Board Diagnostic (OBD) port, 543
 OneDrive, 111, 112, 237, 280,
 458, 475, 519
 Online accounts
 freeze your credit, 473
 lock down
 Apple, 453
 Microsoft, 453
 restrictions, financial accounts, 472
 terms of service, read, 476
 turn on account alerts, 473
 use credit cards, 470
 virtual credit card number, 470, 471
 Online attacks, 185, 186, 190, 245
 Online backups, 109, 110, 146, 445
 Online banking, 439–441, 451, 453
 Ooma, 334
 Open Source Intelligence
 (OSINT), 45, 57
 Open source software, 553, 557, 558
 Operating system (OS), 63
 Mac, 64, 237, 238, 253, 255, 294,
 346, 548
 Microsoft Windows 10, 174, 238
 Optimism, 560, 561
 Opt out of tracking, 44, 57
 Orwell, George, 40
 Owly, 407

P

Packets, 84, 94, 103, 316, 320, 321, 323,
 329, 350, 396
 Panopticon, 38–41, 363
 Paper shredder, 177
 Parental guidance

INDEX

Parental guidance (*cont.*)

- able to access all accounts and devices, 500
 - age restrictions, 501
 - computers in common area, house, 502
 - contract creation, kids, 504
 - dedicated account for each child, 493
 - device tracking, use, 503
 - email accounts creation, children
 - Mac OS, 498
 - windows 10, 494–497
 - family friendly DNS, 503
 - Golden Rule, 488, 502
 - Grandmother Rule, 487, 502
 - lock down chromebook settings, 501
 - resources, 504
 - teach your kids, 500, 502
 - young children, 493, 494
- Passive advertising, 366
- Passkey, 184, 185, 192, 203
- Passphrase, 195, 196, 206, 338, 415, 416, 419
- Password haystacks, 195
- Passwordless, 184, 185, 203
- Password manager, 140, 145, 151, 156, 162, 192–194, 198, 203, 205, 206, 210, 216, 231, 232, 385, 387, 407, 440, 446, 478, 482, 524
- Passwords
- computer accounts
 - Mac OS, 250, 251
 - Microsoft Windows 10, 247, 248
 - haystacks, 195
 - manager, 140, 145, 151, 156, 162, 192–194, 205, 206, 210, 231, 232, 385, 407, 440, 446, 478, 482, 524

- master, 192, 194, 195, 203, 206, 207, 209, 215, 218, 245
 - periodically changing, 198, 199
 - router, 337
 - scrambling process, 188
 - somewhere safe, 140, 145, 206, 549
 - special characters, 194, 196
 - strength, 185, 186, 188, 189, 203
 - two-factor authentication, 198, 199, 204, 213, 391, 470
- PayPal Mobile Cash, 441, 471
- PDF reader app, 312
- Peripherals, 4, 63, 64, 69, 291, 311, 508
- Personal identification number (PIN), 14, 180, 182, 184, 189, 197, 204, 213, 217, 219, 247, 248, 512, 513, 516, 524, 525, 532, 534, 537, 550
- Personally identifiable information (PII), 36, 476
- Petzold, Charles, 63
- PGP key-signing party, 555
- Phishing, 10, 405, 409–411, 423, 544
- Pi Hole, 557
- Pinterest, 56, 361, 447, 477, 480, 482
- Plaid, 443
- Plain text, 86, 89–92, 419
- Podcast, 20, 63, 373, 404, 422, 431, 541, 542, 553, 567, 568
- Pop-ups offering/requiring plug-ins, 394
- Portable Document Format (PDF) file, 106, 176, 312, 416, 417, 423, 479, 480
- Post-quantum cryptography (PQC), 102
- Potentially unwanted program (PUP), 76, 175
- Pretty good privacy (PGP), 403, 404, 415–418, 422, 431, 554
- Prevention, 4–7

Privacy
 matters, 33–59, 324, 511, 513
 vs. Security, 33–35
 threats, 34, 41, 324
 Private browser, 368–370
 Private key, 93, 98–100, 184, 415
 Private network, 338
 Professional cybersecurity, 78
 Project Nightingale, 41
 Proton, 346, 435, 475
 ProtonMail, 431, 436
 Pseudonymous, 200, 201
 Pseudonyms, 200, 412–414
 Public charging stations, 540
 Public Internet, 70, 103, 317, 319, 340
 Public key, 93, 98–100, 102, 184, 351,
 415–418, 555
 Public network, 67, 315
 Public/private key pairs, 100
 Punycode, 406
 Punycode misleading web address, 406

Q

QR code, 184, 215, 216, 339, 343, 442, 472,
 564, 569
 Quality of service (QoS), 322, 323
 Quantum computing, 101, 103

R

Radio frequency (RF) technology, 508
 Random access memory (RAM), 66, 67,
 114, 312, 344
 Ransomware, 75, 107, 236, 283, 547, 548
 Raspberry Pi, 557
 Recover files, 548
 Recovery key, 294–297

Restrict access to folders and files, 236,
 283–286, 288
 Reverse location search warrant, 40
 Rich Communications Services (RCS),
 405, 419
 Ring, 40, 401
 Rooting, 509, 537
 Rootkit, 78
 ROT13, 87
 ROT13 rotational cipher, 87
 Rotational cipher, 87, 88
 Router, 5, 67, 239, 317, 503, 553
 default SSID, 342
 disable external admin, 340
 disable external services, 340
 firmware update, 338
 guest Wi-Fi network, 553
 IP addresses and admin
 credentials, 335
 passwords, 337

S

Safari, 208, 221, 222, 349, 368–370, 374,
 375, 391, 464, 468
 Safety Check, 539
 Sandboxing, 434, 556
 Scams, 10, 11, 76, 313, 339, 350, 394, 409,
 411, 412, 423, 544
 Scareware, 75
 Scrambled passwords, 186, 188
 Secure browser, 368, 369
 SecureDrop, 555
 Secure enclave, 184
 Secure messaging apps, 431, 432, 525, 526
 Secure, Quick, Reliable
 Login (SQRL), 183
 Security by obscurity, 85, 86, 322

INDEX

- Security threats, 34
- Security through obscurity, 233, 321, 343
- Self-signed certificate, 353
- Sensitive files, securely erase
 - Mac OS
 - empty trash, 297
 - secureErase command, 301
 - terminal search in Spotlight, 300
 - Windows
 - empty recycle bin, 244
 - free space, 298
 - PowerShell search, 298, 299
- Server, 6, 12, 70, 71, 77, 79, 81, 94, 100, 147, 185, 186, 193, 215, 288, 322, 327, 328, 351, 354, 362, 366, 372, 382, 396, 397, 402, 403, 407, 413, 414, 417, 418, 421, 423, 430, 431, 546, 547, 557
- Service set identifiers (SSIDs), 338, 339, 342, 343
- 7-Zip, 424–426, 429
 - archive creation, 425
 - password-protected archive
 - settings, 426
- Shelf security and privacy tools, 371, 374, 378, 464, 468
- Shields Up, 341, 342
- Short message service (SMS), 198, 204, 213, 404, 405, 419, 431, 470, 550
- Signal, 4, 58, 86, 240, 241, 337, 378, 432, 433, 509, 512, 526, 533
- SIM jacking, 198
- SimpleLogin, 435
- Siri, 46, 326, 327, 344, 345
- Smartphone
 - Apple's iOS *vs.* Android OS, 506, 517
 - avoid cheap android phones, 529
 - back up
 - Android, 519–521
 - iOS, 518, 520
 - biometric locks, 523
 - device up to date, 521
 - disable Bluetooth and NFC, 532
 - disable Wi-Fi auto-connect, 531
 - enable (self) tracking, 528
 - enabling lockdown mode, 524, 525, 539, 540
 - erase data
 - Android, 534
 - iOS, 533
 - hackers, 509, 513
 - iOS is way safer than Android, 506
 - jailbreaking, 509, 537
 - limit ad tracking, 526
 - lock, 512, 513, 523
 - medical ID, enable, 535
 - permission schemes, 510
 - privacy, 507, 511, 513
 - remove unused apps, 527
 - restrict application
 - permissions, 522
 - secure messaging apps, 525, 526
 - USB condom use, 540
 - use Firefox browser, 529
 - VPN install, 530, 531
 - wireless madness, 508, 509
- Snopes, 58
- Snowden, Edward, 3, 13, 37, 53, 403, 552, 555, 557, 560, 565, 566
- Social media, 20, 36, 38, 43, 45, 46, 52, 57, 61, 114, 119, 189, 204, 361, 421, 433, 439, 447–449, 451, 453, 470, 476–481, 484, 487, 499–501, 534, 544, 549, 551
- avoid TikTok, 484
- close accounts, 481, 482

- delete Facebook history, 482
 - DNA services, 482, 483
 - don't broadcast your travel
 - plans, 476
 - don't divulge too much personal info,
 - 480, 481
 - don't give out your e-mail
 - credentials, 478
 - enable two-factor auth, 470
 - lock down, accounts, 453
 - privacy-respecting alternatives, 478
 - scrub your files before sharing, 479
 - who can see your stuff, 477
 - Software, 5, 45, 62, 183, 205, 233, 403, 475,
 - 486, 506, 541, 560
 - Solid-state drive (SSD), 132, 298, 300
 - Spam, 10, 12, 57, 76, 201, 343, 405,
 - 407–409, 412, 414, 437
 - deal properly, 437
 - favored delivery mechanism, 408
 - filters, 437
 - phishing, 10, 241, 409–411, 423, 544
 - solutions, 408
 - stopping, 408
 - Special characters, 179, 189, 194, 196, 203,
 - 407, 483
 - Spectre, 79
 - Spoofed messages, 405
 - Spring cleaning, 114
 - Spyware, 76, 309, 494, 515, 529, 538, 539
 - StartMail, 431
 - Storage, 46, 52, 66, 70, 74, 107, 109, 111,
 - 112, 117, 119, 133, 147, 193, 237,
 - 244, 291, 298, 350, 362, 363, 431,
 - 439, 445, 446, 451, 464, 475,
 - 518–520, 534, 547
 - Store and forward, 402, 404
 - Strip-cutting shredders, 177
 - Substitution ciphers, 86, 89, 91
 - Supercookie, 44
 - SuperLock, 98–100
 - SwissTransfer, 430
 - Symmetric cipher, 92, 93
 - Symmetric encryption, 92, 184, 415, 416
 - Symmetric locking mechanism, 94
- ## T
- Target, 2, 11, 19, 36, 42, 43, 76, 132, 146,
 - 183, 186, 309, 324, 325, 353, 354,
 - 357, 366, 407, 419, 539
 - Telegram, 404, 431
 - Telnet, 341
 - Terabyte, 65, 109
 - Texas Instruments TI-99/4A personal
 - computer, 62
 - Text messaging, 401, 404, 405, 414, 415,
 - 419, 421, 431, 470
 - Third-party cookie tracking
 - method, 360
 - Threat analysis
 - credit card fraud, 9
 - email hacking, 11
 - identity theft, 11
 - phishing, 10
 - spam and scams, 10
 - tracking and surveillance, 11
 - viruses and malware, 11
 - Threat model, 1, 22, 23
 - 3-2-1 Rule, 107, 111, 119
 - Throwaway e-mail accounts
 - e-mail aliases, 435
 - Firefox private relay, 435
 - shared logins, 431
 - sign-in with Apple, 478
 - TikTok, 36, 56, 447, 484

INDEX

A time-based one-time passcode (TOTP),
197, 213, 215, 216
Too much information (TMI), 365
Tor, 555
Tor Browser, 371, 555
Tracking, 44, 57, 59, 202, 303–309, 330,
347, 349, 355–357, 359, 360, 362,
363, 367, 368, 370–372, 374, 377,
378, 384, 391, 397, 492, 503, 507,
509, 526, 527, 529, 557
Tracking cookies, 45
Transport Layer Security (TLS), 350–352
TransUnion, 443, 474, 551
Trojan, 74, 447
Trustworthy certificate, 353
Turing, Alan, 77, 91
Tutanota, 431, 436
23andMe, 449, 451, 482
Twitter, 47, 56, 361, 447, 451, 476, 477,
480, 481
Two-factor authentication (2FA), 197–199,
204, 212–218, 225, 470, 545, 550

U

uBlock Origin, 391, 392
Unbreakable encryption, 445
Uniform Resource Locator (URL), 105, 411
Uninterruptible power supply (UPS), 113,
163, 164
Unique password, 12, 189, 192, 203, 413,
436, 478, 544
Universal Plug and Play (UPnP), 322, 341
Unlimited overdraft protection, 441
Uploading, 81
USB devices and ports, 311
US Office of Personnel Management
(OPM), 181

V

Venmo, 46, 414, 441, 442, 451, 471, 472
Verizon, 44, 72, 404, 517
Video chat, 401, 420, 433, 526
Virtual credit card number, 470, 471
Virtual machine (VM), 556
Virtual private networks (VPNs), 43, 49,
328–332, 345, 346, 364, 397, 398,
402, 431, 530, 531, 557
Virus, 9, 11, 22, 73, 233, 235, 242, 281, 282,
284, 311, 434, 540, 546
Visa, 41, 223, 301, 442, 471
Vonage, 334

W

Wake word, 72, 326
Waze, 40, 41, 56
Web address, 19, 94, 105, 193, 211, 351,
354, 364, 365, 407, 411, 545
Web browsers
advertising, 369
e-mail read, 434
Firefox, 208, 222, 223, 368–371,
373–395, 398, 399, 407, 435, 455,
459, 529
security and privacy, 368, 372, 374
Web CAPTCHA form, 77
Web of trust, 350, 555
Website password breach, 545, 546
Web tracking
Lightbeam, 356
Panopticon, 363
Wikipedia graph, 356
Wikipedia + Yahoo graph, 357
Yahoo + Amazon + CNN graph, 358
Yahoo + Amazon graph, 358

WeChat, 404
 WhatsApp, 404, 419, 431, 526
 Wide area network (WAN), 315, 317, 332,
 340, 342
 Wi-Fi 6, 317
 Wi-Fi Alliance, 317
 Wi-Fi hotspot, 317, 318, 331, 346, 508, 541
 Wi-Fi network, 320
 Wireless encryption protection (WEP), 338
 Wireless Fidelity (Wi-Fi), 3, 67, 86, 193,
 240, 324, 327, 331, 338, 340, 344,
 346, 347, 486, 508, 509, 519, 521,
 522, 528, 530, 531, 533, 554
 disable auto-connect, 346
 hotspots, 317, 318, 331, 346, 508, 541
 network, 86, 320, 338–340, 342, 343,
 346, 531
 routers, 68, 239, 317–320, 322, 336–338,
 342, 344, 399, 553
 Wireless LANs (WLANs), 317, 332
 Wireless madness, 508, 509

Wireless Protected Access (WPA), 338
 Wireless Protected Setup (WPS), 337, 340
 Work Number, 444, 474
 Worm, 74
 WPA2, 338

X

Xfinity, 318, 319, 344
 Xfinity Wi-Fi, 318, 319, 344

Y

Yahoo Messenger, 404

Z

Zelle, 441, 451, 471
 Zero-day exploit, 73
 Zimmermann, Phil, 403, 422
 Zoom, 81, 420, 432, 433, 561, 562