LEARNING MADE EASY

2nd Edition

Cybersecurity

for dummies®

A Wiley Brand

Assess potential threats

Avoid cybersecurity breaches and plan ahead

Learn how to become cyber-secure

Joseph Steinberg

Cybersecurity

2nd Edition

by Joseph Steinberg

for dummies®
A Wiley Brand

Cybersecurity For Dummies®, 2nd Edition

Published by: **John Wiley & Sons, Inc.,** 111 River Street, Hoboken, NJ 07030-5774, www.wiley.com

Copyright © 2022 by John Wiley & Sons, Inc., Hoboken, New Jersey

Published simultaneously in Canada

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at http://www.wiley.com/go/permissions.

Trademarks: Wiley, For Dummies, the Dummies Man logo, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, please contact our Customer Care Department within the U.S. at 877-762-2974, outside the U.S. at 317-572-3993, or fax 317-572-4002. For technical support, please visit https://hub.wiley.com/community/support/dummies.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at http://booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2022933136

ISBN 978-1-119-86718-0 (pbk); ISBN 978-1-119-86719-7 (ebk); ISBN 978-1-119-86720-3 (ebk)

Contents at a Glance

Introduction 1

Part 1: Getting Started with Cybersecurity 5

CHAPTER 1: What Exactly Is Cybersecurity? 7

CHAPTER 2: Getting to Know Common Cyberattacks 23

CHAPTER 3: The Bad Guys You Must Defend Against 49

Part 2: Improving Your Own Personal Security 69

CHAPTER 4: Evaluating Your Current Cybersecurity Posture 71

CHAPTER 5: Enhancing Physical Security 93

CHAPTER 6: Cybersecurity Considerations When Working from Home 105

Part 3: Protecting Yourself from Yourself 115

CHAPTER 7: Securing Your Accounts 117

CHAPTER 8: Passwords 135

CHAPTER 9: Preventing Social Engineering Attacks 151

Part 4: Cybersecurity for Businesses, Organizations, and Government 173

CHAPTER 10: Securing Your Small Business 175

CHAPTER 11: Cybersecurity and Big Businesses 201

Part 5: Handling a Security Incident (This Is a When, Not an If) 217

CHAPTER 12: Identifying a Security Breach 219

CHAPTER 13: Recovering from a Security Breach 239

Part 6: Backing Up and Recovery 259

CHAPTER 14: Backing Up 261

CHAPTER 15: Resetting Your Device 289

CHAPTER 16: Restoring from Backups 299

Part 7: Looking toward the Future 321

CHAPTER 17: Pursuing a Cybersecurity Career 323

CHAPTER 18: Emerging Technologies Bring New Threats 337

Part 8: The Part of Tens 351

CHAPTER 19: Ten Ways to Improve Your Cybersecurity without Spending a Fortune 353

CHAPTER 20: Ten (or So) Lessons from Major Cybersecurity Breaches 359

CHAPTER 21: Ten Ways to Safely Use Public Wi-Fi 367

Index 371

Table of Contents

INTRODUCTION 1
About This Book. 1
Foolish Assumptions. 3
Icons Used in This Book 4
Beyond the Book 4
Where to Go from Here 4

PART 1: GETTING STARTED WITH CYBERSECURITY 5

CHAPTER 1: What Exactly Is Cybersecurity? 7
Cybersecurity Means Different Things to Different Folks 7
Cybersecurity Is a Constantly Moving Target 9
Technological changes 9
Social shifts. 14
Economic model shifts 15
Political shifts 16
Looking at the Risks Cybersecurity Mitigates 20
The goal of cybersecurity: The CIA Triad 21
From a human perspective 22

CHAPTER 2: Getting to Know Common Cyberattacks 23
Attacks That Inflict Damage 24
Denial-of-service (DoS) attacks 24
Distributed denial-of-service (DDoS) attacks. 24
Botnets and zombies 26
Data destruction attacks 27
Is That Really You? Impersonation 27
Phishing 28
Spear phishing 28
CEO fraud 28
Smishing 29
Vishing. 29
Pharming 29
Whaling: Going for the “big fish” 29
Messing around with Other People’s Stuff: Tampering. 30
Captured in Transit: Interception 30
Man-in-the-middle attacks 31
Taking What Isn’t Theirs: Data Theft. 32
Personal data theft 32
Business data theft 32
Data exfiltration. 33

Compromised credentials 33
Forced policy violations 34
Cyberbombs That Sneak into Your Devices: Malware 34
Viruses. 34
Worms. 35
Trojans 35
Ransomware 35
Scareware 36
Spyware. 37
Cryptocurrency miners 37
Adware 37
Blended malware. 38
Zero-day malware 38
Fake malware on computers 38
Fake malware on mobile devices 38
Fake security subscription renewal notifications 39
Poisoned Web Service Attacks. 39
Network Infrastructure Poisoning 40
Malvertising 40
Drive-by downloads 41
Stealing passwords 41
Exploiting Maintenance Difficulties 43
Advanced Attacks 43
Opportunistic attacks 44
Targeted attacks 44
Blended (opportunistic and targeted) attacks. 45
Some Technical Attack Techniques. 45
Rootkits 45
Brute-force attacks 46
Injection attacks. 46
Session hijacking 47
Malformed URL attacks 47
Buffer overflow attacks. 48

CHAPTER 3: **The Bad Guys You Must Defend Against** 49
Bad Guys and Good Guys Are Relative Terms .50
Bad Guys Up to No Good 51
Script kiddies 51
Kids who are not kiddies 52
Terrorists and other rogue groups 52
Nations and states. 52
Corporate spies 54
Criminals. 54
Hacktivists. 54

Cyberattackers and Their Colored Hats 55
How Cybercriminals Monetize Their Actions 56
Direct financial fraud 56
Indirect financial fraud 57
Ransomware 59
Cryptominers 60
Not All Dangers Come From Attackers: Dealing with Nonmalicious Threats 60
Human error 60
External disasters 62
Defending against These Attackers 67

PART 2: IMPROVING YOUR OWN PERSONAL SECURITY 69

CHAPTER 4: Evaluating Your Current Cybersecurity Posture 71
Don't be Achilles: Identifying Ways You May Be Less than Secure 71
Your home computer(s) 72
Your mobile devices 73
Your Internet of Things (IoT) devices 73
Your networking equipment 74
Your work environment 74
Identifying Risks 74
Protecting against Risks 75
Perimeter defense 76
Firewall/router 76
Security software 79
Your physical computer(s) and any other endpoints 79
Backups 79
Detecting 80
Responding 80
Recovering 80
Improving 80
Evaluating Your Current Security Measures 80
Software 81
Hardware 82
Insurance 83
Education 83
Privacy 101 84
Think before you share 84
Think before you post 85
General privacy tips 86
Banking Online Safely 88
Safely Using Smart Devices 90
Cryptocurrency Security 101 91

CHAPTER 5: **Enhancing Physical Security** 93
Understanding Why Physical Security Matters .94
Taking Inventory 94
Stationary devices 96
Mobile devices 97
Locating Your Vulnerable Data 97
Creating and Executing a Physical Security Plan. 98
Implementing Physical Security 100
Security for Mobile Devices 101
Realizing That Insiders Pose the Greatest Risks 102

CHAPTER 6: **Cybersecurity Considerations When Working from Home** 105
Network Security Concerns 106
Device Security Concerns 108
Location Cybersecurity 109
Shoulder surfing 109
Eavesdropping 110
Theft 110
Human errors. 110
Video Conferencing Cybersecurity 111
Keep private stuff out of camera view 111
Keep video conferences secure from unauthorized visitors. 111
Social Engineering Issues 113
Regulatory Issues 113

PART 3: PROTECTING YOURSELF FROM YOURSELF 115

CHAPTER 7: **Securing Your Accounts** 117
Realizing You're a Target 117
Securing Your External Accounts 118
Securing Data Associated with User Accounts 119
Conduct business with reputable parties .119
Use official apps and websites 120
Don't install software from untrusted parties. 120
Don't root your phone 120
Don't provide unnecessary sensitive information 120
Use payment services that eliminate the need to share credit card numbers. 120
Use one-time, virtual credit card numbers when appropriate. . . . 121
Monitor your accounts 122
Report suspicious activity ASAP. 122
Employ a proper password strategy. 122
Utilize multifactor authentication 122
Log out when you're finished. 124

Use your own computer or phone 124
Lock your computer 124
Use a separate, dedicated computer for sensitive tasks 125
Use a separate, dedicated browser for sensitive web-based tasks 125
Secure your access devices 125
Keep your devices up to date 125
Don't perform sensitive tasks over public Wi-Fi 125
Never use public Wi-Fi in high-risk places 126
Access your accounts only in safe locations 126
Use appropriate devices 126
Set appropriate limits 126
Use alerts 127
Periodically check access device lists 127
Check last login info 127
Respond appropriately to any fraud alerts 127
Never send sensitive information over an unencrypted connection 127
Beware of social engineering attacks 128
Establish voice login passwords 129
Protect your cellphone number 129
Don't click on links in emails or text messages 129
Securing Data with Parties You've Interacted With 130
Securing Data at Parties You Haven't Interacted With 132
Securing Data by Not Connecting Hardware with Unknown Pedigrees 133

CHAPTER 8: **Passwords** 135
Passwords: The Primary Form of Authentication 135
Avoiding Simplistic Passwords 136
Password Considerations 137
Easily guessable personal passwords 137
Complicated passwords aren't always better 138
Different levels of sensitivity 138
Your most sensitive passwords may not be the ones you think 139
You can reuse passwords — sometimes 139
Consider using a password manager 140
Creating Memorable, Strong Passwords 142
Knowing When to Change Passwords 143
Changing Passwords after a Breach 144
Providing Passwords to Humans 144
Storing Passwords 145
Storing passwords for your heirs 145
Storing general passwords 145

Transmitting Passwords 146
Discovering Alternatives to Passwords 146
Biometric authentication 146
SMS-based authentication 148
App-based one-time passwords 149
Hardware token authentication 149
USB-based authentication 150

CHAPTER 9: **Preventing Social Engineering Attacks** 151
Don’t Trust Technology More than You Would People 151
Types of Social Engineering Attacks 152
Six Principles Social Engineers Exploit 156
Don’t Overshare on Social Media 156
Your schedule and travel plans 157
Financial information 158
Personal information 158
Work information 160
Possible cybersecurity issues. 160
Crimes and minor infractions 160
Medical or legal advice 160
Your location 161
Your birthday 161
Your “sins”. 161
Leaking Data by Sharing Information as Part of Viral Trends 162
Identifying Fake Social Media Connections 162
Photo 163
Verification 163
Friends or connections in common 163
Relevant posts 164
Number of connections 164
Industry and location 165
Similar people 165
Duplicate contact. 165
Contact details 165
Premium status 166
LinkedIn endorsements 166
Group activity 166
Appropriate levels of relative usage 167
Human activities 167
Cliché names 167
Poor contact information 168
Skill sets. 168
Spelling 168
Age of an account 168

Suspicious career or life path 168
Level or celebrity status 169
Using Bogus Information 170
Using Security Software 170
General Cyberhygiene Can Help Prevent Social Engineering 171

PART 4: CYBERSECURITY FOR BUSINESSES, ORGANIZATIONS, AND GOVERNMENT 173

CHAPTER 10: Securing Your Small Business 175
Making Sure Someone Is In Charge 175
Watching Out for Employees. 176
Incentivize employees. 177
Avoid giving out the keys to the castle 177
Give everyone separate credentials 178
Restrict administrators 178
Limit access to corporate accounts 178
Implement employee policies 180
Enforce social media policies. 183
Monitor employees 183
Dealing with a Remote Workforce 184
Use work devices and separate work networks 185
Set up virtual private networks 185
Create standardized communication protocols 186
Use a known network 186
Determine how backups are handled 187
Be careful where you work remotely 187
Be extra vigilant regarding social engineering 188
Considering Cybersecurity Insurance. 189
Complying with Regulations and Compliance. 190
Protecting employee data 190
PCI DSS 191
Breach disclosure laws 191
GDPR 192
HIPAA. 192
Biometric data 193
Anti-money laundering laws 193
International sanctions. 193
Handling Internet Access 193
Segregate Internet access for personal devices 193
Create bring your own device (BYOD) policies 194
Properly handle inbound access. 194
Protect against denial-of-service attacks 196
Use https. 197
Use a VPN 197

Run penetration tests 197
Be careful with IoT devices. 197
Use multiple network segments 198
Be careful with payment cards 198
Managing Power Issues 198

CHAPTER 11: **Cybersecurity and Big Businesses** 201
Utilizing Technological Complexity 202
Managing Custom Systems 202
Continuity Planning and Disaster Recovery. 203
Looking at Regulations 203
Sarbanes Oxley 203
Stricter PCI requirements. 205
Public company data disclosure rules 205
Breach disclosures 205
Industry-specific regulators and rules 206
Fiduciary responsibilities 206
Deep pockets 207
Deeper Pockets — and Insured. 207
Considering Employees, Consultants, and Partners 208
Dealing with internal politics 209
Offering information security training 209
Replicated environments 209
Looking at the Chief Information Security Officer's Role. 210
Overall security program management. 210
Test and measurement of the security program 210
Human risk management. 211
Information asset classification and control 211
Security operations 211
Information security strategy 211
Identity and access management 211
Data loss prevention. 212
Fraud prevention. 212
Incident response plan 213
Disaster recovery and business continuity planning 213
Compliance. 213
Investigations 213
Physical security. 214
Security architecture 214
Geopolitical risks 214
Ensuring auditability of system administrators 215
Cybersecurity insurance compliance 215

PART 5: HANDLING A SECURITY INCIDENT (THIS IS A WHEN, NOT AN IF) . . . 217

CHAPTER 12: Identifying a Security Breach . . . 219

Identifying Overt Breaches . . . 220
Ransomware . . . 220
Defacement . . . 221
Claimed destruction . . . 221
Detecting Covert Breaches . . . 222
Your device seems slower than before . . . 223
Your Task Manager doesn't run . . . 223
Your Registry Editor doesn't run . . . 223
Your device starts suffering from latency issues . . . 224
Your device starts suffering from communication and buffering issues . . . 225
Your device's settings have changed . . . 226
Your device is sending or receiving strange email messages . . . 226
Your device is sending or receiving strange text messages . . . 226
New software (including apps) is installed on your device — and you didn't install it . . . 226
Your device's battery seems to drain more quickly than before . . . 227
Your device seems to run hotter than before . . . 227
File contents have been changed . . . 228
Files are missing . . . 228
Websites appear different than before . . . 228
Your Internet settings show a proxy, and you never set one up . . . 228
Some programs (or apps) stop working properly . . . 229
Security programs have turned off . . . 229
An increased use of data or text messaging (SMS) . . . 230
Increased network traffic . . . 230
Unusual open ports . . . 230
Your device starts crashing . . . 231
Your cellphone bill shows unexpected charges up to here . . . 232
Unknown programs request access . . . 232
External devices power on unexpectedly . . . 232
Your device acts as if someone else were using it . . . 232
New browser search engine default . . . 232
Your device password has changed . . . 233
Pop-ups start appearing . . . 233
New browser add-ons appear . . . 233
New browser home page . . . 234
Your email from the device is getting blocked by spam filters . . . 234
Your device is attempting to access "bad" sites . . . 234

You're experiencing unusual service disruptions 234
Your device's language settings changed .235
You see unexplained activity on the device. 235
You see unexplained online activity 235
Your device suddenly restarts 235
You see signs of data breaches and/or leaks 236
You are routed to the wrong website. 236
Your hard drive or SSD light never seems to turn off 236
Other abnormal things happen. 237

CHAPTER 13: **Recovering from a Security Breach**. 239

An Ounce of Prevention Is Worth Many Tons of Response 239
Stay Calm and Act Now with Wisdom. 240
Bring in a Pro 240
Recovering from a Breach without a Pro's Help 241
Step 1: Figure out what happened or is happening 241
Step 2: Contain the attack 242
Step 3: Terminate and eliminate the attack. 243
Reinstall Damaged Software 247
Restart the system and run an updated security scan 247
Erase all potentially problematic System Restore points 248
Restore modified settings 248
Rebuild the system 249
Dealing with Stolen Information 250
Paying ransoms 251
Learning for the future 253
Recovering When Your Data Is Compromised at a Third Party 253
Reason the notice was sent 254
Scams 254
Passwords. 255
Payment card information 256
Government-issued documents 256
School or employer-issued documents 257
Social media accounts 257

PART 6: BACKING UP AND RECOVERY. 259

CHAPTER 14: **Backing Up** 261

Backing Up Is a Must. 261
Backing Up Data from Apps and Online Accounts 262
SMS texts 263
Social media 263
WhatsApp 264
Google Photos 264
Other apps 264

Backing Up Data on Smartphones 265
Android 265
Apple 265
Conducting Cryptocurrency Backups 267
Backing Up Passwords 267
Looking at the Different Types of Backups 267
Full backups of systems 267
Original system images 269
Later system images 269
Original installation media 269
Downloaded software. 270
Full backups of data 270
Incremental backups. 271
Differential backups 271
Mixed backups 272
Continuous backups 272
Partial backups. 273
Folder backups. 273
Drive backups. 274
Virtual drive backups 274
Exclusions 275
In-app backups 276
Figuring Out How Often You Should Backup 277
Exploring Backup Tools 278
Backup software 278
Drive-specific backup software 279
Windows Backup 279
Smartphone/tablet backup 280
Manual file or folder copying backups 280
Automated task file or folder copying backups 280
Creating a Boot Disk 281
Knowing Where to Back Up 281
Local storage 282
Offsite storage 282
Cloud 282
Network storage 283
Mixing locations 284
Knowing Where Not to Store Backups 284
Encrypting Backups 285
Testing Backups 286
Disposing of Backups 286

CHAPTER 15: **Resetting Your Device** 289

Exploring Two Types of Resets 289

Soft resets. 290

Hard resets 292

Rebuilding Your Device after a Hard Reset 298

CHAPTER 16: **Restoring from Backups**. 299

You Will Need to Restore 299

Wait! Do Not Restore Yet!. 300

Restoring Data to Apps. 300

Restoring from Full Backups of Systems 301

Restoring to the computing device that was originally backed up 301

Restoring to a different device than the one that was originally backed up 302

Original system images 303

Later system images 303

Installing security software 303

Original installation media 304

Downloaded software. 304

Restoring from full backups of data 305

Restoring from Incremental Backups. 306

Incremental backups of data 306

Incremental backups of systems. 306

Differential backups 307

Continuous backups 308

Partial backups. 308

Folder backups. 309

Drive backups. 309

Virtual-drive backups 310

Dealing with Deletions 311

Excluding Files and Folders 311

Understanding Archives 312

Multiple files stored within one file. 312

Old live data 313

Old versions of files, folders, or backups 314

Restoring Using Backup Tools 314

Restoring from a Windows backup. 315

Restoring to a system restore point 315

Restoring from a smartphone/tablet backup 315

Restoring from manual file or folder copying backups 316

Utilizing third-party backups of data hosted at third parties 317

Returning Backups to Their Proper Locations 317
Network storage 317
Restoring from a combination of locations 318
Restoring to Non-Original Locations 318
Never Leave Your Backups Connected 318
Restoring from Encrypted Backups 319
Testing Backups 319
Restoring Cryptocurrency 319
Booting from a Boot Disk 320

PART 7: LOOKING TOWARD THE FUTURE 321

CHAPTER 17: Pursuing a Cybersecurity Career 323
Professional Roles in Cybersecurity 324
Security engineer 324
Security manager 324
Security director 324
Chief information security officer (CISO) 324
Security analyst 325
Security architect 325
Security administrator 325
Security auditor 325
Cryptographer 325
Vulnerability assessment analyst 326
Ethical hacker 326
Security researcher 326
Offensive hacker 326
Software security engineer 327
Software source code security auditor 327
Security consultant 327
Security expert witness 327
Security specialist 327
Incident response team member 328
Forensic analyst 328
Cybersecurity regulations expert 328
Privacy regulations expert 328
Exploring Career Paths 328
Career path: Senior security architect 329
Career path: CISO 329
Starting Out in Information Security 331
Exploring Popular Certifications 332
CISSP 332
CISM 333

CEH 333
Security+ 334
GSEC 334
Verifiability 335
Ethics 335
Overcoming a Criminal Record 335
Overcoming Bad Credit 336
Looking at Other Professions with a Cybersecurity Focus 336

CHAPTER 18: **Emerging Technologies Bring New Threats** 337
Relying on the Internet of Things 338
Critical infrastructure risks 339
Computers on wheels: modern cars 340
Using Cryptocurrencies and Blockchain 340
Cloud-Based Applications and Data 342
Optimizing Artificial Intelligence 343
Increased need for cybersecurity 344
Use as a cybersecurity tool 345
Use as a hacking tool 345
Where Was This Laptop Really Made? Supply Chain Risks 346
Nothing Is Trustworthy: Zero Trust 347
Genius Computers Are Coming: Quantum Supremacy 347
Experiencing Virtual Reality 348
Transforming Experiences with Augmented Reality 350

PART 8: THE PART OF TENS 351

CHAPTER 19: **Ten Ways to Improve Your Cybersecurity without Spending a Fortune** 353
Understand That You Are a Target 353
Use Security Software 354
Encrypt Sensitive Information 354
Back Up Often 356
Do Not Share Login Credentials 356
Use Proper Authentication 357
Use Social Media Wisely 357
Segregate Internet Access 357
Use Public Wi-Fi Safely (Or Better Yet, Don’t Use It!) 358
Hire a Pro 358

CHAPTER 20: **Ten (or So) Lessons from Major Cybersecurity Breaches** 359
Marriott 359
Target 361

Sony Pictures 362
U.S. Office of Personnel Management 363
Anthem 363
Colonial Pipeline and JBS SA 364
Colonial Pipeline 364
JBS 365

CHAPTER 21: **Ten Ways to Safely Use Public Wi-Fi** 367
Use Your Cellphone as a Mobile Hotspot 368
Turn Off Wi-Fi Connectivity When You're Not Using Wi-Fi 368
Don't Perform Sensitive Tasks over Public Wi-Fi 369
Don't Reset Passwords When Using Public Wi-Fi 369
Use a VPN Service 369
Use Tor 369
Use Encryption 370
Turn Off Sharing 370
Have Information Security Software on Any Devices Connected to Public Wi-Fi Networks 370
Understand the Difference between True Public Wi-Fi and Shared Wi-Fi 370

INDEX 371

Introduction

In the course of just a single generation, the world has undergone some of the greatest changes since the dawn of mankind. The availability of the Internet as a tool for consumers and businesses alike, coupled with the invention of mobile devices and wireless networking, have ushered in an Information Revolution that has impacted just about every aspect of human existence.

Humanity's reliance on technology, however, has also created enormous risks. It seems that not a day goes by without some new story emerging of a data breach, cyberattack, or the like. Simultaneously, because society's reliance on technology increases on a daily basis, the potential adverse consequences of cyberattacks have grown exponentially to the point that people can now lose their fortunes, their reputations, their health, or even their lives, as the result of cyberattacks.

In fact, since the publication of the first edition of this book, Americans have seen cyberattacks cause fuel shortages, spikes in meat prices, financial losses, and even death. And societal changes resulting from the COVID-19 pandemic — including the dramatic increase in the number of people who, at least sometimes, leverage computers and computer networks in order to work remotely — have upped the stakes even more. While people all around the developed world outsource a large portion of their national security to their countries' respective armed forces, their fire safety to trained fire departments, and their protection from criminals to law enforcement agencies, ensuring that one remains safe from cyber threats requires far more personal involvement.

It is no wonder, therefore, that people living in the modern world understand the need to protect themselves from cyber-dangers. This book shows you how to do so.

About This Book

While many books have been written over the past couple decades on a wide variety of cybersecurity-related topics, most of them don't provide the general population with the information needed to properly protect themselves.

Many cybersecurity books are directed toward highly technical audiences and tend to overwhelm people who are not computer scientists with extraneous information, creating severe challenges for readers seeking to translate the knowledge that they acquire from books into practical actions. On the flip side, various self-published introduction-to-cybersecurity books suffer from all sorts of serious deficiencies, including, in some cases, having been written by non-experts and presenting significant amounts of misinformation. Anyone interested in cybersecurity often shouldn't trust these materials. Likewise, many security tip sheets and the like simply relay oft-repeated clichés and outdated advice, sometimes causing people who follow the recommendations contained within such works to worsen their cybersecurity postures rather than improve them. Furthermore, the nearly constant repetition of various cybersecurity advice by media personalities after news stories about breaches ("Don't forget to reset all your passwords!"), coupled with the lack of consequences to most people after they do not comply with such directives, has led to *cybersecurity fatigue* — a condition in which folks simply don't act when they actually need to because they have heard the "boy cry wolf" one too many times.

I wrote *Cybersecurity For Dummies* to provide people who do not work as cybersecurity professionals with a foundational book that can teach them what they need to know about cybersecurity and explain why they need to know it. This book offers you practical, clear, and straightforward advice that you can easily translate into actions that can help keep you and your children, parents, and small businesses cybersecure. The second edition of this book contains updates to help people understand and address cybersecurity risks created by changes to our world in terms of technological advances, societal changes, and new geopolitical realities.

Cybersecurity For Dummies is divided into several parts. Parts 1, 2, and 3 provide an overview of cybersecurity and give tips on protecting yourself and your loved ones from both external threats and from making dangerous (and potentially disastrous) mistakes. Topics such as how to secure your online accounts, how to select and protect passwords, and how to safely work remotely fall into these parts of the book.

Part 4 offers tips on securing small businesses, which may be especially pertinent for small business owners and employees. Part 4 then also discusses some of the unique security needs that face firms as they grow larger and touches on cybersecurity-in-government related matters.

Part 5 shows you how to identify security breaches. Part 6 covers the process of backing up, something that you should do proactively before the need to recover arises, as well as how to recover from security breaches.

Part 7 looks toward the future — both for those interested in potentially pursuing a cybersecurity-related career (or who have children or other relatives or friends considering doing so) as well as those interested in how emerging technologies are likely to impact their own personal cybersecurity.

Part 8 gives several lists of ten items that you may want to keep as tip sheets.

Please keep in mind that while internalizing all the information in this book, and putting it into practice, will likely dramatically improve your cybersecurity posture, reading this book will no more make you an expert in cybersecurity than reading a book on the workings of the human heart will quickly transform you into a competent cardiologist.

Cybersecurity is a complex, rapidly changing field whose professionals spend years, if not decades, studying and working full-time to develop, sharpen, and maintain the skills and expertise that they utilize on a constant basis. As such, please do not consider the advice within this book as a substitute for hiring a professional for any situation that reasonably warrants the latter.

Also, please keep in mind that technical products change quite often, so any screenshots included within the book may not be identical to the screens that you observe when you perform similar actions to those described in the text. Remember: Cybersecurity threats are constantly evolving, as are the technologies and approaches utilized to combat them.

Foolish Assumptions

In this book, I make some assumptions about your experience with technology:

- You have experience with using a keyboard and pointer, such as a mouse, on either a Mac or Windows PC and have access to one of those machines.
- You have experience with using a so-called “smartphone” running the Android or iOS operating systems.

  You know how to use an Internet browser, such as Firefox, Chrome, Edge, Opera, or Safari.
- You know how to install applications on your computer and have adequate rights to do so.
- You know how to perform a Google search.

Icons Used in This Book

Throughout this book, small images, known as icons, appear in the margins. These icons mark important tidbits of information:

TIP

The Tip icon identifies places where I offer additional tips for making this journey more interesting or clear. Tips cover some neat shortcuts that you may not have known about.

REMEMBER

The Remember icon bookmarks important points that you'll want to keep in mind.

WARNING

The Warning icon helps protect you from common errors and may even give you tips to undo your mistakes.

Beyond the Book

In addition to what you're reading right now, this product also comes with a free access-anywhere Cheat Sheet that covers important cybersecurity actions. To get this Cheat Sheet, simply go to `www.dummies.com` and search for *Cybersecurity For Dummies Cheat Sheet* in the Search box.

Where to Go from Here

Cybersecurity For Dummies is designed in such a fashion that you don't have to read the book in order or even read the entire book.

If you purchased this book because you suffered a cybersecurity breach of some sort, for example, you can skip to the chapters in Part 5 without reading the prior material (although reading it afterwards may be wise, as it may help you prevent yourself from becoming the victim of another cyberattack).

1

Getting Started with Cybersecurity

IN THIS PART . . .

Discover what cybersecurity is and why defining it is more difficult than you might expect.

Find out why breaches seem to occur so often and why technology alone does not seem to stop them.

Learn how societal changes can dramatically impact cybersecurity.

Explore various types of common cyberthreats and common cybersecurity tools.

Understand the who, how, and why of various types of attackers and threatening parties that aren't officially malicious.

IN THIS CHAPTER

- **Understanding the difference between cybersecurity and information security**
- **Showing why cybersecurity is a constantly moving target**
- **Understanding the goals of cybersecurity**
- **Looking at the risks mitigated by cybersecurity**

Chapter 1

What Exactly Is Cybersecurity?

To improve your ability to keep yourself and your loved ones cybersecure, you need to understand what cybersecure means, what your goals should be vis-à-vis cybersecurity, and what exactly you're securing against.

While the answers to these questions may initially seem simple and straightforward, they aren't. As you see in this chapter, these answers can vary dramatically between people, company divisions, organizations, and even within the same entity at different times.

Cybersecurity Means Different Things to Different Folks

While *cybersecurity* may sound like a simple enough term to define, in actuality, from a practical standpoint, it means quite different things to different people in different situations, leading to extremely varied relevant policies, procedures, and practices. Individuals who want to protect their social media accounts from hacker takeovers, for example, are exceedingly unlikely to assume many of the approaches and technologies used by Pentagon workers to secure classified networks.

Typically, for example:

- For **individuals,** *cybersecurity* means that their personal data is not accessible to anyone other than themselves and others they have authorized, and that their computing devices work properly and are free from malware.
- For **small business owners,** *cybersecurity* may include ensuring that credit card data is properly protected and that standards for data security are properly implemented at point-of-sale registers.
- For **firms conducting online business,** *cybersecurity* may include protecting servers that untrusted outsiders regularly interact with.
- For **shared service providers,** *cybersecurity* may entail protecting numerous data centers that house numerous servers that, in turn, host many virtual servers belonging to many different organizations.
- For **the government,** *cybersecurity* may include establishing different classifications of data, each with its own set of related laws, policies, procedures, and technologies.

REMEMBER

The bottom line is that while the word cybersecurity is easy to define, the practical expectations that enters people's minds when they hear the word vary quite a bit.

Technically speaking, cybersecurity is the subset of information security that addresses information and information systems that store and process data in electronic form, whereas *information security* encompasses the security of all forms of data (for example, securing a paper file and a filing cabinet).

That said, today, many people colloquially interchange the terms, often referring to aspects of information security that are technically not part of cybersecurity as being part of the latter. Such usage also results from the blending of the two in many situations. Technically speaking, for example, if someone writes down a password on a piece of paper and leaves the paper on a desk where other people can see the password instead of placing the paper in a safe deposit box or safe, that person has violated a principle of information security, not of cybersecurity, even though those actions may result in serious cybersecurity repercussions.