

# Contents

About the Author	xix
Acknowledgments	xxi
Foreword	xxiii
<b>CHAPTER 1</b>	
<b>The Need for Cybersecurity</b>	<b>1</b>
Why This Book?	2
What You Should Do Right Now	3
How This Book Is Organized	4
You <i>Can</i> Improve Your Own Cybersecurity	5
<b>CHAPTER 2</b>	
<b>The Black Market for Your Data: The Cybercrime Economy</b>	<b>7</b>
A. Introduction	7
B. It Is a Big Business	8
C. It Is International	9
D. Digital Currency	10
E. Payment Card Fraud: An Example of the Cybercrime Economy	11
F. Other Cybercrime and Identity Theft Schemes	17
1. Financial Account Takeover	17
2. New Financial Account Opening	17
3. Infected Computers	18
4. Phishing, Spam, and Internet Account Takeover	20
5. Other Ways to Obtain Passwords	21
6. E-mail Account Compromise (Hack)	23

7. Ransomware	25
8. Scareware and Technical Support Scams	27
G. Government and Law Enforcement Response	28

## **CHAPTER 3**

### **Advertising: Another Market for Your Data 31**

A. Introduction	31
B. Corporate Collection and Use of Your Information and Data	32
C. What (or Who) Is the Product?	34
D. Privacy Policies and the Consumer	34
E. Corporate Data Storage	36
F. Conclusion	38

## **CHAPTER 4**

### **Basic Information Security Principles 39**

A. Introduction	39
B. Physical Security	40
1. Theft and Damage	40
2. Controlling Access to Your Devices at Home	41
C. Confidentiality	43
1. Authentication	43
2. Encryption	50
D. Availability	51
1. “If It Ain’t Broke, Don’t Fix It.” But Maybe It Is Broken After All?	51
2. Availability, Authentication, and Confidentiality	52
3. Availability and Ransomware and Other Malicious Destruction	52
4. Availability and Backup	53
5. Business Continuity and Disaster Recovery Planning	53
E. Integrity	55
F. The Principle of “Least Privilege” and “Need to Know”	58
1. Data Access	58
2. Administrator Rights and Accounts	58

G. Information Classification	59
H. Conclusion	60

**CHAPTER 5**

**Basic Computer Principles 61**

A. Introduction	61
B. The Evolution of Computing	61
1. Storing Information	62
2. Processing Information	63
C. Computer Hardware	64
1. Case	66
2. Power Supply	66
3. Display	67
4. Ports: USB, Parallel, Serial, VGA, DVI, HDMI, DP	68
5. Input Devices (Keyboard, Mouse, Microphone, Camera, and More)	69
6. Network Interface Controller	69
7. Processor (Central Processing Unit, Microprocessor)	70
8. Random Access Memory	70
9. Motherboard (System Board)	72
10. Internal Data Storage	73
11. External Data Storage	74
12. External Devices Such as Scanners and Printers	75
D. Programs That Run on Your Computer: BIOS, Operating System, Applications	76
1. BIOS	76
2. Operating System	76
3. File System	77
4. Applications (Software)	77
5. Virtual Ports	78
E. From Desktop to Miniature: Laptop, Notebook, Tablet, Smartphone, Smartwatch, IoT	78
F. Computers on Steroids: The Cloud and Data Centers	78
G. Encryption of Data at Rest	80
H. Conclusion	81

**CHAPTER 6****Basic Networking and the Internet 83**

A. Introduction	83
B. Network Interface Controller	83
C. Internet	84
1. Dial-up	85
2. Cable Internet (Broadband)	86
3. Phone Company Internet (DSL, FiOS)	87
4. Cellular Company Internet	87
5. Satellite Internet	88
D. Modem	89
E. Router	89
F. Internet Communication 101	90
1. IP Addresses on the Internet	90
2. IP Addresses on Your Local Network: Network Address Translation	92
3. Ports: Virtual Router Ports and Computer Ports	93
4. TCP/UDP Internet Protocols (Language)	94
5. Network Layers	96
G. Wired Networking	98
H. Wireless Networking	99
I. Encryption in Transit	100
J. Conclusion	103

**CHAPTER 7****Start Securing Yourself 105**

A. Introduction	105
B. Set Your Cybersecurity Dial	105
C. Turning Up Your Security Dial Is an Investment	107
D. There Is No Perfect Product or Solution	108
E. Let's Get Started (If You Haven't Already)	109
1. Put a Password on All of Your Computing Devices	109
2. Enable the "Auto Lock" Feature	110

3. Run an Anti-Malware Scan on Your Laptop and Desktop	110
4. Disconnect from the Internet When You Don't Need It	111
5. Use Complex and Unique Passwords	111
6. Enable "Two-Step" Login	111
7. Ensure That Your Home Wi-Fi Network Is Password Protected	112
F. Conclusion	112

## **CHAPTER 8**

### **Secure Your Devices 113**

A. Introduction	113
B. Mentally Assess Your Devices	114
C. Getting Started	115
D. Device Inventory (Scavenger Hunt)	115
1. Device Description	116
2. Ownership and Expectation of Privacy	116
E. Access: Physical Control	117
F. Access: Electronic (Technical)	118
1. Device Password Complexity	119
2. Auto Lock Feature and Affirmatively Locking Your Device	120
G. User Accounts: Usage by Whom and for What Purposes?	121
1. Administrator Accounts vs. User Accounts	123
2. Segregation of User Accounts	125
H. Operating System	128
I. Applications (Software)	131
J. Data Stored on Device	134
K. Data the Device Can Access (Cloud Data)	136
L. Anti-Malware	136
M. Internet Access	139
N. Firewall	140
O. Decommissioning Your Device	141
1. Basic Decommissioning Steps	142
P. Conclusion	143

**CHAPTER 9****Secure Your Data****145**

A. Introduction	145
B. Mentally Assess Your Data and What It Means to You	147
1. Assess Your Own Skills and Memory	148
2. Assess by Data Type	149
3. Assess by Data Importance and Risk	150
4. Assess by Data Storage Location and Provider	151
5. Assessment Wrap-Up	152
C. Getting Started	153
D. Secure Your Devices (Encore)	153
E. Back Up Your Data	153
1. Manually Back Up Data to an External Hard Drive	156
2. Make Incremental Backups of Your Most Important Documents	157
3. Manually Back Up Data from Your Cloud Accounts to a Local Device or External Hard Drive	158
4. Backup Using Your Operating System's Native Backup Application	158
5. Automatic Backup vs. Manual Backup	159
F. Secure Your Cloud Data and Internet Accounts (and Back Them Up)	159
1. Secure Your Important Online Accounts	160
2. Secure Your "Unimportant Accounts" as Best You Can	162
G. Consider Encryption to Secure Data on Your Local Device	165
1. To Encrypt or Not to Encrypt? That Is the Question	166
2. Encryption by the Application	167
3. File and Folder Encryption by the Operating System	169
4. Full Disk Encryption	170
5. Encryption Summary	173
H. Organize Your Data—Your Files and Folders	174
1. Basic File Organization Concepts	176
2. Storage Location	179
I. Conclusion	186

<b>CHAPTER 10</b>	
<b>Secure Your Network and Internet Use</b>	<b>189</b>
A. Introduction	189
B. Mentally Assess Your Home Network	190
C. Identify Parts of Your Home Network	190
D. Internet Connection	191
E. Modem	192
F. Router and Wi-Fi	193
1. Learn About Basic Wi-Fi Routing	193
2. Log In to Your Router Administration Portal	195
3. Secure Your Router Administration Username and Password	198
4. Update Router Firmware	199
5. Secure the Wi-Fi Network Password and Ensure the Network Is Encrypted	200
6. Evaluate Your Wi-Fi Network Name	201
7. Disable Wi-Fi Protected Setup	203
8. Disable Remote Access Features You Don't Need	203
9. Enable Your Router's Firewall (If Available)	203
10. Disable Universal Plug and Play If You Don't Need It	203
11. Run Your Router's Security Self-Assessment Function (If Available)	204
12. Enable a Guest Network on Your Router (If Available)	204
13. Check Your Router's Physical Security	204
14. Learn About Additional Router and Wi-Fi Security Features	205
15. Wi-Fi Router Conclusion	207
G. Software Firewalls (Encore for Your Laptops and Desktops)	208
H. Review Device Software That Accesses the Internet (Encore for What Is Phoning Home)	209
I. How Your Data Is Transmitted	209
J. Equipment on the Network	210
1. Printers, Scanners, Fax Machines, All-in-Ones, and More	210
2. Network Attached Storage	211
K. The "Internet of Things" and Smart Homes	211
L. Reduce Your Attack Surface: Disconnect When Not Needed	217

M. More About Networks for the Very Curious	218
1. Windows Task Manager	219
2. Windows Resource Monitor	219
3. Windows Firewall	219
4. Windows Firewall with Advanced Security	219
5. Windows Commands Regarding Network Activity	219
6. Mac Applications and Commands Regarding Network Activity	220
7. Install a Free Software Firewall	220
N. Conclusion	221

## **CHAPTER 11**

### **Secure Your Family, Children, and Seniors 223**

A. Introduction	223
B. Children	223
1. Assessment	225
2. Your Parental “Privacy Policy”	225
3. Educating Your Child to Make Good Decisions	227
4. Reviewing Your Child’s Devices and Computer Usage	228
5. Sample Guidelines or Rules of Conduct	232
6. Reviewing the Data That Is Posted About Your Children	234
C. Seniors	237
D. Conclusion	240

## **CHAPTER 12**

### **Secure Yourself When You Travel 241**

A. Introduction	241
B. Devices and Travel	242
1. Preventing Loss or Theft	243
2. Using Someone Else’s Device	248
C. Internet Access and Travel	250
D. Data and Travel	253
1. Data You Bring (Data at Rest)	253
2. Data You Access (Data in Transit)	254



E. Miscellaneous Anti-Fraud When You Travel	256
F. Special Considerations When Traveling to Certain Countries	257
G. Conclusion	258

**CHAPTER 13**

**Secure the Work Office 259**

A. Introduction	259
B. The Workplace Mental Assessment	262
C. Physically Secure Your Office	263
1. Visitor Entry	263
2. Locks and Doors	266
3. Alarm Systems and Video Surveillance	269
4. The “Plain View” Doctrine in Your Office	270
D. Securing Your Employees and Coworkers	270
1. Screening and the Insider Threat	271
2. Training	271
3. Shadow IT in the Office	273
4. Acceptable Use of Workplace Computers	276
E. Secure the Devices in Your Office	276
F. Secure the Data in Your Office	277
1. Network Storage Devices in Your Office	278
2. Documents and Data in the Cloud	278
3. E-mail	279
4. Data at Rest	279
5. Data in Transit	279
6. Business Contacts and Social Media	279
G. Secure the Workplace Network and Internet Use	280
H. Secure the Workplace from Fraud	283
1. Protecting Your E-mail Accounts	283
2. Confirming the Authenticity of Payment Instructions Sent to You	285
3. Escrow Operators (“Money Mules”) and Money Laundering	286
4. Cybersecurity and Anti-Fraud Policies and Procedures	289
I. Business Continuity and Disaster Recovery Planning	290

J. Incident Response Planning	290
K. Cyber Insurance	292
L. Conclusion	293

## **CHAPTER 14**

### **The Law, and the Role and Responsibilities of Lawyers 295**

A. Introduction	295
B. Attorney Professional Responsibility Rules on Cybersecurity	299
1. The American Bar Association and the ABA Model Rules of Professional Conduct	300
2. A Survey of Cybersecurity-Related Opinions and Issues	303
C. Cybersecurity Laws, Data Breach Laws, and Litigation	312
1. Cybersecurity Laws and Data Disposal Laws	312
2. Data Breach Notification Laws	313
3. Data Breach Litigation	314
D. Privacy Laws and Regulations	315
E. Rules for Financial Institutions	316
F. HIPAA and HITECH	318
G. Electronic Communications Privacy Act	319
H. Cybersecurity Information Sharing Act	319
I. Cybercrime-Related Criminal Statutes	320
J. Cybersecurity Standards	323
1. Critical Security Controls	323
2. National Institute of Standards and Technology	325
3. The International Organization for Standardization	326
4. Other Standards (COBIT, ISA, PCI DSS)	326
K. Conclusion	326

## **CHAPTER 15**

### **Troubleshooting and Responding to Your Own Incidents 329**

A. Introduction	329
B. Finding Specific Troubleshooting Help	329

C. Diagnosis 101	330
1. Troubleshooting	330
2. Is It a Tech Issue or Has a Crime Occurred?	331
3. Device vs. Cloud vs. Other Issue	331
D. Preserving Evidence of a Potential Crime or Tort	332
E. Device-Related Issues	333
1. Device Not Working Properly—Can’t Tell Why	333
2. Device Won’t Turn Off, Won’t Boot Up, or Won’t Start	333
3. Malware Infection (Including Ransomware)	334
4. Lost or Stolen Device	335
5. Someone Untrustworthy Had Temporary Access to Your Device	335
6. Lack of Connectivity	336
7. Repurposing a Device	337
F. Data-Related Issues	338
1. Can’t Find or Access the Data	338
2. Data Is Not Readable	338
3. Lost/Forgotten Password to Data in the Cloud	338
4. Lost/Forgotten Password to Data That Is Stored Locally	339
5. Cloud Account Was Hacked	339
6. Accidental Dissemination of Confidential Material	339
G. Network- or Internet-Related Issues	340
H. Suspicious Requests or Suspicious Potential Clients	340
I. Victim of Cybercrime	341
1. Stop the Attacker and Regain Access, Control, and Security	341
2. Follow-Up Actions	342
J. Victim of Identity Theft	342
K. Victim of Cyberbullying, Harassment, or Threats	342
L. Traveling to a High-Risk Country	343
M. Conclusion	343

**Conclusion**

<b>APPENDIX 1</b>	
<b>Your Cybersecurity Posture and Awareness</b>	<b>347</b>
<b>APPENDIX 2</b>	
<b>Cybersecurity Threats and Risks You Face</b>	<b>351</b>
<b>APPENDIX 3</b>	
<b>Your Cybersecurity Dial</b>	<b>355</b>
<b>APPENDIX 4</b>	
<b>Cybersecurity Myths</b>	<b>357</b>
<b>APPENDIX 5</b>	
<b>How Computers Count and Why You Might Care</b>	<b>359</b>
<b>APPENDIX 6</b>	
<b>Smartphone and Tablet Decommissioning Checklist</b>	<b>361</b>
<b>APPENDIX 7</b>	
<b>Laptop and Desktop Decommissioning Checklist</b>	<b>363</b>
<b>APPENDIX 8</b>	
<b>View Data Flowing Across Your Network</b>	<b>367</b>
<b>APPENDIX 9</b>	
<b>Additional Resources and Bibliography</b>	<b>369</b>

<b>APPENDIX 10</b>	
<b>Home Device Inventory</b>	<b>377</b>
<b>APPENDIX 11</b>	
<b>Personal Device and Data Summary</b>	<b>379</b>
<b>APPENDIX 12</b>	
<b>Data Summary</b>	<b>381</b>
<b>APPENDIX 13</b>	
<b>Home Network and Internet Summary</b>	<b>383</b>
<b>Index</b>	<b>385</b>