1.

Record Nr.	UNINA9910796734103321
Autore	Bandler John
Titolo	Cybersecurity for the home and office : the lawyer's guide to taking charge of your own information security / / John Bandler
Pubbl/distr/stampa	Chicago, Illinois : , : ABA, Section of Science & Technology Law, , [2017] ©2017
ISBN	1-63425-908-4
Descrizione fisica	1 online resource (xxiv, 392 pages) : illustrations
Disciplina	005.8024/34
Soggetti	Computer security - Law and legislation - United States Computer networks - Security measures - United States Law offices - United States Data protection - Law and legislation - United States
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Intro -- Title Page -- Copyright -- Dedication -- Contents -- About the Author -- Acknowledgments -- Foreword -- CHAPTER 1 The Need for Cybersecurity -- Why This Book? -- What You Should Do Right Now -- How This Book Is Organized -- You Can Improve Your Own Cybersecurity -- CHAPTER 2 The Black Market for Your Data: The Cybercrime Economy -- A. Introduction -- B. It Is a Big Business -- C. It Is International -- D. Digital Currency -- E. Payment Card Fraud: An Example of the Cybercrime Economy -- F. Other Cybercrime and Identity Theft Schemes -- 1. Financial Account Takeover -- 2. New Financial Account Opening -- 3. Infected Computers -- 4. Phishing, Spam, and Internet Account Takeover -- 5. Other Ways to Obtain Passwords -- 6. E-mail Account Compromise (Hack) -- 7. Ransomware -- 8. Scareware and Technical Support Scams -- G. Government and Law Enforcement Response -- CHAPTER 3 Advertising: Another Market for Your Data -- A. Introduction -- B. Corporate Collection and Use of Your Information and Data -- C. What (or Who) Is the Product? -- D. Privacy Policies and the Consumer -- E. Corporate Data Storage -- F. Conclusion -- CHAPTER 4 Basic Information Security Principles -- A. Introduction -- B. Physical Security -- 1. Theft and Damage -- 2.

Controlling Access to Your Devices at Home -- C. Confidentiality -- 1. Authentication -- 2. Encryption -- D. Availability -- 1. "If It Ain't Broke, Don't Fix It." But Maybe It Is Broken After All? -- 2. Availability, Authentication, and Confidentiality -- 3. Availability and Ransomware and Other Malicious Destruction -- 4. Availability and Backup -- 5. Business Continuity and Disaster Recovery Planning -- E. Integrity -- F. The Principle of "Least Privilege" and "Need to Know" -- 1. Data Access -- 2. Administrator Rights and Accounts -- G. Information Classification -- H. Conclusion.

CHAPTER 5 Basic Computer Principles -- A. Introduction -- B. The Evolution of Computing -- 1. Storing Information -- 2. Processing Information -- C. Computer Hardware -- 1. Case -- 2. Power Supply -- 3. Display -- 4. Ports: USB, Parallel, Serial, VGA, DVI, HDMI, DP -- 5. Input Devices (Keyboard, Mouse, Microphone, Camera, and More) -- 6. Network Interface Controller -- 7. Processor (Central Processing Unit, Microprocessor) -- 8. Random Access Memory -- 9. Motherboard (System Board) -- 10. Internal Data Storage -- 11. External Data Storage -- 12. External Devices Such as Scanners and Printers -- D. Programs That Run on Your Computer: BIOS, Operating System, Applications -- 1. BIOS -- 2. Operating System -- 3. File System -- 4. Applications (Software) -- 5. Virtual Ports -- E. From Desktop to Miniature: Laptop, Notebook, Tablet, Smartphone, Smartwatch, IoT -- F. Computers on Steroids: The Cloud and Data Centers -- G. Encryption of Data at Rest -- H. Conclusion -- CHAPTER 6 Basic Networking and the Internet -- A. Introduction -- B. Network Interface Controller -- C. Internet -- 1. Dial-up -- 2. Cable Internet (Broadband) -- 3. Phone Company Internet (DSL, FiOS) -- 4. Cellular Company Internet -- 5. Satellite Internet -- D. Modem -- E. Router -- F. Internet Communication 101 -- 1. IP Addresses on the Internet -- 2. IP Addresses on Your Local Network: Network Address Translation -- 3. Ports: Virtual Router Ports and Computer Ports -- 4. TCP/UDP Internet Protocols (Language) -- 5. Network Layers -- G. Wired Networking -- H. Wireless Networking -- I. Encryption in Transit -- J. Conclusion -- CHAPTER 7 Start Securing Yourself -- A. Introduction -- B. Set Your Cybersecurity Dial -- C. Turning Up Your Security Dial Is an Investment -- D. There Is No Perfect Product or Solution -- E. Let's Get Started (If You Haven't Already).

1. Put a Password on All of Your Computing Devices -- 2. Enable the "Auto Lock" Feature -- 3. Run an Anti-Malware Scan on Your Laptop and Desktop -- 4. Disconnect from the Internet When You Don't Need It -- 5. Use Complex and Unique Passwords -- 6. Enable "Two-Step" Login -- 7. Ensure That Your Home Wi-Fi Network Is Password Protected -- F. Conclusion -- CHAPTER 8 Secure Your Devices -- A. Introduction -- B. Mentally Assess Your Devices -- C. Getting Started -- D. Device Inventory (Scavenger Hunt) -- 1. Device Description -- 2. Ownership and Expectation of Privacy -- E. Access: Physical Control -- F. Access: Electronic (Technical) -- 1. Device Password Complexity -- 2. Auto Lock Feature and Affirmatively Locking Your Device -- G. User Accounts: Usage by Whom and for What Purposes? -- 1. Administrator Accounts vs. User Accounts -- 2. Segregation of User Accounts -- H. Operating System -- I. Applications (Software) -- J. Data Stored on Device -- K. Data the Device Can Access (Cloud Data) -- L. Anti-Malware -- M. Internet Access -- N. Firewall -- O. Decommissioning Your Device -- 1. Basic Decommissioning Steps -- P. Conclusion -- CHAPTER 9 Secure Your Data -- A. Introduction -- B. Mentally Assess Your Data and What It Means to You -- 1. Assess Your Own Skills and Memory -- 2. Assess by Data Type -- 3. Assess by Data Importance and Risk -- 4. Assess by Data Storage Location and Provider -- 5.

Assessment Wrap-Up -- C. Getting Started -- D. Secure Your Devices (Encore) -- E. Back Up Your Data -- 1. Manually Back Up Data to an External Hard Drive -- 2. Make Incremental Backups of Your Most Important Documents -- 3. Manually Back Up Data from Your Cloud Accounts to a Local Device or External Hard Drive -- 4. Backup Using Your Operating System's Native Backup Application -- 5. Automatic Backup vs. Manual Backup.

F. Secure Your Cloud Data and Internet Accounts (and Back Them Up) -- 1. Secure Your Important Online Accounts -- 2. Secure Your "Unimportant Accounts" as Best You Can -- G. Consider Encryption to Secure Data on Your Local Device -- 1. To Encrypt or Not to Encrypt? That Is the Question -- 2. Encryption by the Application -- 3. File and Folder Encryption by the Operating System -- 4. Full Disk Encryption -- 5. Encryption Summary -- H. Organize Your Data-Your Files and Folders -- 1. Basic File Organization Concepts -- 2. Storage Location -- I. Conclusion -- CHAPTER 10 Secure Your Network and Internet Use -- A. Introduction -- B. Mentally Assess Your Home Network -- C. Identify Parts of Your Home Network -- D. Internet Connection -- E. Modem -- F. Router and Wi-Fi -- 1. Learn About Basic Wi-Fi Routing -- 2. Log In to Your Router Administration Portal -- 3. Secure Your Router Administration Username and Password -- 4. Update Router Firmware -- 5. Secure the Wi-Fi Network Password and Ensure the Network Is Encrypted -- 6. Evaluate Your Wi-Fi Network Name -- 7. Disable Wi-Fi Protected Setup -- 8. Disable Remote Access Features You Don't Need -- 9. Enable Your Router's Firewall (If Available) -- 10. Disable Universal Plug and Play If You Don't Need It -- 11. Run Your Router's Security Self-Assessment Function (If Available) -- 12. Enable a Guest Network on Your Router (If Available) -- 13. Check Your Router's Physical Security -- 14. Learn About Additional Router and Wi-Fi Security Features -- 15. Wi-Fi Router Conclusion -- G. Software Firewalls (Encore for Your Laptops and Desktops) -- H. Review Device Software That Accesses the Internet (Encore for What Is Phoning Home) -- I. How Your Data Is Transmitted -- J. Equipment on the Network -- 1. Printers, Scanners, Fax Machines, All-in-Ones, and More -- 2. Network Attached Storage.

K. The "Internet of Things" and Smart Homes -- L. Reduce Your Attack Surface: Disconnect When Not Needed -- M. More About Networks for the Very Curious -- 1. Windows Task Manager -- 2. Windows Resource Monitor -- 3. Windows Firewall -- 4. Windows Firewall with Advanced Security -- 5. Windows Commands Regarding Network Activity -- 6. Mac Applications and Commands Regarding Network Activity -- 7. Install a Free Software Firewall -- N. Conclusion -- CHAPTER 11 Secure Your Family, Children, and Seniors -- A. Introduction -- B. Children -- 1. Assessment -- 2. Your Parental "Privacy Policy" -- 3. Educating Your Child to Make Good Decisions -- 4. Reviewing Your Child's Devices and Computer Usage -- 5. Sample Guidelines or Rules of Conduct -- 6. Reviewing the Data That Is Posted About Your Children -- C. Seniors -- D. Conclusion -- CHAPTER 12 Secure Yourself When You Travel -- A. Introduction -- B. Devices and Travel -- 1. Preventing Loss or Theft -- 2. Using Someone Elses Device -- C. Internet Access and Travel -- D. Data and Travel -- 1. Data You Bring (Data at Rest) -- 2. Data You Access (Data in Transit) -- E. Miscellaneous Anti-Fraud When You Travel -- F. Special Considerations When Traveling to Certain Countries -- G. Conclusion -- CHAPTER 13 Secure the Work Office -- A. Introduction -- B. The Workplace Mental Assessment -- C. Physically Secure Your Office -- 1. Visitor Entry -- 2. Locks and Doors -- 3. Alarm Systems and Video Surveillance -- 4. The "Plain View" Doctrine in Your Office -- D. Securing Your Employees and Coworkers -- 1.

Screening and the Insider Threat -- 2. Training -- 3. Shadow IT in the Office -- 4. Acceptable Use of Workplace Computers -- E. Secure the Devices in Your Office -- F. Secure the Data in Your Office -- 1. Network Storage Devices in Your Office -- 2. Documents and Data in the Cloud -- 3. E-mail -- 4. Data at Rest.

5. Data in Transit.