

SECURITY AWARENESS

APPLYING PRACTICAL SECURITY IN YOUR WORLD



Fifth Edition

Mark Ciampa



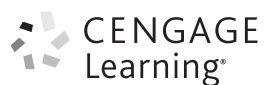
Security Awareness: Applying Practical Security In Your World



Security Awareness: Applying Practical Security In Your World

Fifth Edition

Mark Ciampa, Ph.D.



Australia • Brazil • Mexico • Singapore • United Kingdom • United States

This is an electronic version of the print textbook. Due to electronic rights restrictions, some third party content may be suppressed. Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. The publisher reserves the right to remove content from this title at any time if subsequent rights restrictions require it. For valuable information on pricing, previous editions, changes to current editions, and alternate formats, please visit www.cengage.com/highered to search by ISBN#, author, title, or keyword for materials in your areas of interest.

Important Notice: Media content referenced within the product description or the product text may not be available in the eBook version.

Security Awareness: Applying Practical Security In Your World, Fifth Edition**Mark Ciampa**SVP, GM Skills & Global Product
Management: Dawn Gerrain

Product Director: Kathleen McMahon

Product Team Manager: Kristin McNary

Senior Director, Development:
Marah BellegardeProduct Development Manager: Leigh
HefferonSenior Content Developer: Michelle Ruelos
Cannistraci

Product Assistant: Abigail Pufpaff

Vice President, Marketing Services: Jennifer
Ann Baker

Marketing Director: Michele McTighe

Senior Production Director: Wendy Troeger

Production Director: Patty Stephan

Senior Content Project Manager: Brooke
Greenhouse

Managing Art Director: Jack Pendleton

Cover Image(s): © Alex Mit/Shutterstock.com

© 2017, 2014 Cengage Learning

WCN: 02-200-203

ALL RIGHTS RESERVED. No part of this work covered by the copyright herein may be reproduced or distributed in any form or by any means, except as permitted by U.S. copyright law, without the prior written permission of the copyright owner.

All screenshots, unless otherwise noted, are used with permission from Microsoft Corporation. Microsoft® is a registered trademark of the Microsoft Corporation.

For product information and technology assistance, contact us at
Cengage Learning Customer & Sales Support, 1-800-354-9706

For permission to use material from this text or product,
submit all requests online at www.cengage.com/permissions.

Further permissions questions can be e-mailed to
permissionrequest@cengage.com

Library of Congress Control Number: 2015957517

ISBN: 978-1-3055-0037-2

Cengage Learning20 Channel Center Street
Boston, MA 02210
USA

Cengage Learning is a leading provider of customized learning solutions with employees residing in nearly 40 different countries and sales in more than 125 countries around the world. Find your local representative at www.cengage.com

Cengage Learning products are represented in Canada by
Nelson Education, Ltd.

To learn more about Cengage Learning, visit www.cengage.com.

Purchase any of our products at your local college store or at our preferred online store www.cengagebrain.com.

Notice to the Reader

Publisher does not warrant or guarantee any of the products described herein or perform any independent analysis in connection with any of the product information contained herein. Publisher does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instructions contained herein, the reader willingly assumes all risks in connection with such instructions. The publisher makes no representations or warranties of any kind, including but not limited to, the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and the publisher takes no responsibility with respect to such material. The publisher shall not be liable for any special, consequential, or exemplary damages resulting, in whole or part, from the readers' use of, or reliance upon, this material.

Printed in the United States of America
Print Number: 01 Print Year: 2015



Brief Contents

PREFACE	xi
CHAPTER 1	
Introduction to Security	1
CHAPTER 2	
Personal Security	37
CHAPTER 3	
Computer Security	75
CHAPTER 4	
Internet Security	115
CHAPTER 5	
Mobile Security	149
CHAPTER 6	
Privacy	183
GLOSSARY	217
INDEX	223

Table of Contents

PREFACE	xi
CHAPTER 1	
Introduction to Security	1
Challenges of Securing Information	3
Today's Attacks	4
Difficulties in Defending against Attacks	7
What Is Information Security?	10
Understanding Security	10
Defining Information Security	11
Information Security Terminology	14
Understanding the Importance of Information Security	15
Who Are the Attackers?	19
Cybercriminals	20
Script Kiddies	21
Brokers	21
Insiders	22
Cyberterrorists	22
Hactivists	22
State-Sponsored Attackers	23
Building a Comprehensive Security Strategy	23
Block Attacks	24
Update Defenses	24
Minimize Losses	25
Stay Alert	25
Chapter Summary	25
Key Terms	26
Review Questions	26
Hands-On Projects	30
Case Projects	34
References	35
CHAPTER 2	
Personal Security	37
Personal Security Attacks	39
Password Attacks	40
Attacks Using Social Engineering	44
Identity Theft	50
Social-Networking Risks	51
Personal Security Defenses	53
Password Defenses	53
Recognizing Phishing Attacks	57
Avoiding Identity Theft	57
Setting Social-Networking Defenses	58
Chapter Summary	60
Key Terms	62

viii Table of Contents

Review Questions	62
Hands-On Projects	65
Case Projects	72
References	73
CHAPTER 3	
Computer Security	75
Attacks Using Malware	77
Circulation/Infection	77
Concealment	82
Payload Capabilities	83
Computer Defenses	91
Managing Patches	91
Examining Firewalls	94
Installing Antimalware Software	96
Monitoring User Account Control (UAC)	97
Creating Data Backups	99
Recovering from Attacks	101
Chapter Summary	102
Key Terms	104
Review Questions	104
Hands-On Projects	108
Case Projects	113
References	113
CHAPTER 4	
Internet Security	115
How the Internet Works	117
The World Wide Web	117
Email	119
Internet Security Risks	120
Browser Vulnerabilities	120
Malvertising	123
Drive-By Downloads	125
Cookies	126
Email Risks	127
Internet Defenses	130
Securing the Web Browser	130
Email Defenses	133
Internet Security Best Practices	135
Chapter Summary	137
Key Terms	138
Review Questions	139
Hands-On Projects	142
Case Projects	146
References	147

CHAPTER 5	
Mobile Security	149
Mobile Attacks	151
Attacks through Wireless Networks	151
Attacks on Mobile Devices	156
Mobile Defenses	163
Wireless Network Security	163
Mobile Device Security	167
Chapter Summary	171
Key Terms	172
Review Questions	173
Hands-On Projects	176
Case Projects	181
References	182
CHAPTER 6	
Privacy	183
Privacy Primer	185
What Is Privacy?	186
Risks Associated with Private Data	186
Privacy Protections	189
Cryptography	189
Privacy Best Practices	203
Responsibilities of Organizations	204
Chapter Summary	206
Key Terms	206
Review Questions	207
Hands-On Projects	210
Case Projects	215
References	216
GLOSSARY	217
INDEX	223



Preface

Security continues to be a major concern of virtually all computer users today. Consider the reasons why: attacks directed at point-of-sale (PoS) systems in retail stores resulted in over one billion records of consumers' payment card information being stolen in a single year, or an average of 2.8 million records stolen each day or 32 records every second.ⁱ

Almost one of three users in a survey said that either they or another household member had information from a payment card used at a store stolen by computer attackers during the last year, making this the most frequently experienced crime on a list of nine crimes.ⁱⁱ In a two-year period 91 percent of healthcare organizations reported at least one data breach, 39 percent reported two to five data breaches, and 40 percent had more than five data breaches. The total cost for healthcare data breaches is about \$6 billion per year, with the average loss to each organization of \$2,134,800.ⁱⁱⁱ Security researchers recently demonstrated how easy it was for a car to be remotely controlled from a remote location 10 miles away, manipulating not only the car's air conditioning, radio, and windshield wipers, which the driver could not change, but also the acceleration and braking.^{iv} This incident prompted the National Highway Traffic Safety Administration (NHTSA) to recall 1.4 million vehicles to patch this vulnerability, making it the first time that cars had been recalled due to security vulnerability.^v It is no surprise that in a recent survey 69 percent of Americans report they frequently or occasionally worry about having their payment card information stolen by cyberattackers. This compares with 45 percent who worry about their home being burglarized and 7 percent who are concerned about being assaulted by a coworker.^{vi}

Yet knowing how to make computer and mobile devices secure and keep them safe is still a puzzle to most users. What steps should you take to protect your computer, and which are the most important? How do you install software patches? Should you have antivirus software on your mobile device? What does a firewall do? What is a Trojan horse? How can you test your computer to be sure that it cannot be attacked through the Internet? Knowing how to keep a computer and mobile devices secure can be a daunting task.

This book provides you with the knowledge and tools you need to make your computer and related technology equipment—tablets, laptops, smartphones, and wireless networks—secure. *Security Awareness: Applying Practical Security in Your World, Fifth Edition*, presents a basic introduction to practical computer security for all users, from students to home users to business professionals. Security topics are introduced through a series of real-life user experiences, showing why computer security is necessary and providing the essential elements for making and keeping computers secure. Going beyond the concepts of computer security, you will gain practical skills on how to protect your computers and devices from increasingly sophisticated attacks.

Each chapter in the book contains Hands-On Projects that cover making computers secure, as well as how to use and configure security hardware and software. These projects are designed to make what you learn come alive through actually performing the tasks. Besides the Hands-On Projects, each chapter provides realistic security Case Projects that allow you to interact with other learners from around the world using the Information Security Community website that accompanies the textbook. Every chapter also includes review questions to reinforce your knowledge while helping you to apply practical security in your world.

Intended Audience

This book is intended to meet the needs of students and professionals who want to be able to protect their computers and technology devices from attacks. A basic working knowledge of computers is all that is required to use this book. The book's pedagogical features are designed to provide a truly interactive learning experience to help prepare you for the challenges of securing your technology. In addition to the information presented in the text, each chapter includes Hands-On Projects that guide you through implementing practical hardware, software, and network security step by step. Each chapter also contains case studies, requiring you to apply concepts presented in the chapter to achieve a successful solution.

Chapter Descriptions

Here is a summary of the topics covered in each chapter of this book:

- **Chapter 1, “Introduction to Security,”** begins by explaining the challenge of information security and why it is important. This chapter also introduces information security terminology, defines who the attackers are, and gives an overview of attacks and defenses.
- **Chapter 2, “Personal Security,”** examines attacks on passwords and the dangers of social engineering. It also covers identity theft and social networking risks, and provides information on personal security defenses to protect users from attacks.
- **Chapter 3, “Computer Security,”** explores attacks on computers that use different types of malware, such as viruses, worms, Trojans, and botnets. Chapter 3 also includes information on how to protect a computer by managing patches, examining firewalls, installing anti-malware software, and configuring personal firewalls. It also gives guidance on how to recover from an attack.

- **Chapter 4, “Internet Security,”** gives an overview of how the Internet works and the security risks that go along with using it. The chapter closes by exploring how to use the Internet securely.
- **Chapter 5, “Mobile Security,”** examines attacks that come through wireless networks, such as Wi-Fi and Bluetooth, along with attacks on mobile devices such as tablets, laptops, and smartphones. It also explores how networks and devices can be secured.
- **Chapter 6, “Privacy,”** explores the risks to private data along with privacy best practices. In addition, this chapter outlines the responsibilities of a business or organization to protect users’ data.

Features

To aid you in fully understanding computer and network security, this book includes many features designed to enhance your learning experience.

- **Chapter Objectives.** Each chapter begins with a detailed list of the concepts to be mastered within that chapter. This list provides you with both a quick reference to the chapter’s contents and a useful study aid.
- **Security in Your World.** Each chapter opens with a security-related vignette that introduces the chapter content and helps the reader to understand why these topics are important. These stories are continued throughout the chapter, providing additional information about real-life computer security.
- **Illustrations and Tables.** Numerous illustrations of security vulnerabilities, attacks, and defenses help you visualize security elements, theories, and concepts. In addition, the tables provide details and comparisons of practical and theoretical information.
- **Exceptional Security.** For those users who want to set the highest level of protection against cyberattacks, a series of practical suggestions is provided for going “above and beyond” a basic level of security.
- **Chapter Summaries.** Each chapter’s text is followed by a summary of the concepts introduced in that chapter. These summaries provide a helpful way to review the ideas covered in each chapter.
- **Key Terms.** All of the terms in each chapter that were introduced with bold text are gathered in a Key Terms list at the end of the chapter, providing additional review and highlighting key concepts. Key term definitions are included in a Glossary at the end of the text.
- **Review Questions.** The end-of-chapter assessment begins with a set of review questions that reinforce the ideas introduced in each chapter. These questions help you evaluate and apply the material you have learned. Answering these questions will ensure that you have mastered the important concepts.
- **Hands-On Projects.** Although it is important to understand the concepts behind security, nothing can improve upon real-world experience. To this end, each chapter provides several Hands-On Projects aimed at providing you with practical security software and hardware implementation experience. These projects use the Windows 10 operating system, as well as software downloaded from the Internet.
- **Case Projects.** Located at the end of each chapter are two Case Projects. In these exercises, you implement the skills and knowledge gained in the chapter through real design and

implementation scenarios. Additional Case Projects, including a running case study that places you in the role of a problem solver, requiring you to apply concepts presented in the chapter, are available in the MindTap online learning environment.

New to This Edition

- Updated information on the latest security attacks and defenses
- Entirely new chapter on privacy
- New section in each chapter on exceptional security
- New Security in Your World vignettes in each chapter
- The latest information on and best practices for securing wireless networks and mobile devices (laptops, smartphones, and tablets)
- New material on cryptography and attacks using social engineering, and other topics
- New Hands-On Projects in each chapter covering some of the latest security software
- Updated Case Projects in each chapter
- Information Security Community Site activity in each chapter allows learners to interact with other learners and security professionals from around the world

Text and Graphic Conventions

Wherever appropriate, additional information and exercises have been added to this book to help you better understand the topic at hand. Icons throughout the text alert you to additional materials. The icons used in this textbook are described below.



The Note icon draws your attention to additional helpful material related to the subject being described.



Tips based on the author's experience provide extra information about how to attack a problem or what to do in real-world situations.



Each Hands-On activity in this book is preceded by the Hands-On icon and a description of the exercise that follows.



Case Project icons mark Case Projects, which are scenario-based assignments. In these case examples, you are asked to implement independently what you have learned.

Information Security Community Site

Stay secure with the Information Security Community Site! Connect with students, professors, and professionals from around the world, and stay on top of this ever-changing field.

Visit www.community.cengage.com/infosec2 to:

- **Download** resources such as instructional videos and labs.
- **Ask** authors, professors, and students the questions that are on your mind in our Discussion Forums.
- **See** up-to-date news, videos, and articles.
- **Read** weekly blogs from author Mark Ciampa.
- **Listen** to podcasts on the latest Information Security topics.

Each chapter includes information on a current security topic and asks the learner to post their reactions and comments to the Information Security Community Site. This allows users from around the world to interact and learn from other users as well as with security professionals and researchers.

Instructor's Materials

Everything you need for your course is in one place! The following supplemental materials are available for use in a classroom setting. All the supplements available with this book are provided to the instructor online. Please visit login.cengage.com and log in to access instructor-specific resources on the Instructor's Companion Site.

Instructor's Manual. The Instructor's Manual that accompanies this textbook includes the following items: additional instructional material to assist in class preparation, including suggestions for lecture topics, tips on setting up a lab for the Hands-On Projects, and solutions to all end-of-chapter materials.

Cengage Learning Testing Powered by Cognero. This flexible, online system allows you to do the following:

- Author, edit, and manage test bank content from multiple Cengage Learning solutions.
- Create multiple test versions in an instant.
- Deliver tests from your LMS, your classroom, or wherever you want.

PowerPoint Presentations. This book comes with a set of Microsoft PowerPoint slides for each chapter. These slides are meant to be used as a teaching aid for classroom presentations, to be made available to students on the network for chapter review, or to be printed for classroom distribution. Instructors are also at liberty to add their own slides for other topics introduced.

Figure Files. All of the figures and tables in the book are reproduced. Similar to PowerPoint presentations, these are included as a teaching aid for classroom presentation, to make available to students for review, or to be printed for classroom distribution.

MindTap

MindTap for *Security Awareness: Applying Practical Security in Your World, Fifth Edition* is a fully online, highly personalized learning experience built upon Cengage Learning content. MindTap combines student learning tools—readings, multimedia, activities, and assessments—into a singular Learning Path that guides students through their course. Instructors personalize the experience by customizing authoritative Cengage Learning content and learning tools into the Learning Path that integrates into the MindTap framework seamlessly with Learning Management Systems.

Instant Access Code: (ISBN: 9781305946682)

Printed Access Code: (ISBN: 9781305946699)

To access additional course materials, go to www.cengagebrain.com and search for this book title periodically for more details.

About the Author

Mark Ciampa, Ph.D., Security+, is Associate Professor of Information Systems at Western Kentucky University in Bowling Green, Kentucky. Previously, he served as Associate Professor and Director of Academic Computing for 20 years at Volunteer State Community College in Gallatin, Tennessee. Dr. Ciampa has worked in the IT industry as a computer consultant for the U.S. Postal Service, the Tennessee Municipal Technical Advisory Service, and the University of Tennessee. He is also the author of many Cengage textbooks, including *Security+ Guide to Network Security Fundamentals, Fifth Edition*; *CWNA Guide to Wireless LANs, Third Edition*; *Guide to Wireless Communications*; and *Networking BASICS*. He holds a Ph.D. in technology management with a specialization in digital communication systems from Indiana State University.

Acknowledgments

A large team of dedicated professionals contributed to the creation of this book. I am honored to be part of such an outstanding group of professionals, and to everyone on the team I extend my sincere thanks. A special thanks goes to Product Manager Kristin McNary for her support and providing me the opportunity to work on this project. Thanks also to Associate Product Manager Amy Savino, Senior Content Developer Michelle Ruelos Cannistraci, Senior Content Project Manager Brooke Greenhouse, and to Serge Palladino, Technical Editor, as well as the excellent production and permissions teams at Cengage Learning.

Special recognition again goes to the very best developmental editor, Deb Kaufmann. As always, Deb was there to find all of my errors, watch every tiny detail of this project, answer my never-ending list of questions, and make very helpful suggestions. Without question, Deb is the developmental editor every author wishes for, and I was extremely grateful to have her on this project.

And finally, I want to thank my wonderful wife, Susan. What can I say? Once again her patience, support, and love gave me what I needed to finish this project. I could not have written the first word without her.

Dedication

To Braden, Mia, Abby, Gabe, Cora, and Will.

To the User

This book should be read in sequence, from beginning to end. However, each chapter is a self-contained unit, so after completing Chapter 1 the reader may elect to move to any subsequent chapter.

Hardware and Software Requirements

Following are the hardware and software requirements needed to perform the end-of-chapter Hands-On Projects.

- Microsoft Windows 10 (Projects may also be completed using Windows 8.1, 8, or 7 although the steps may slightly differ.)
- An Internet connection and web browser

Specialized Requirements

Whenever possible, the needs for specialized requirements were kept to a minimum. The following chapter features specialized hardware:

- Chapter 1: A USB flash drive

Free Downloadable Software Requirements

Free, downloadable software is required for the Hands-On Projects in the following chapters.

Chapter 1:

- Microsoft Safety Scanner
- Irongeek Thumbscrew

Chapter 2:

- KeePass Password Safe
- LastPass
- SuperGenPass

Chapter 3:

- EICAR AntiVirus Test File
- Macrium Reflect

Chapter 4:

- Qualys Browser Check
- Browzar Private Web Browser

Chapter 5:

- Xirrus Wi-Fi Monitor Inspector
- Prey Project

Chapter 6:

- OpenPuff Steganography
- Hashtab
- Criptext


References

- i. “2014 Year of Mega Breaches & Identity Theft,” *Breach Level Index*, accessed June 4, 2015. <http://breachlevelindex.com/pdf/Breach-Level-Index-Annual-Report-2014.pdf>.
- ii. “Hacking Tops List of Crimes Americans Worry about Most,” *Gallup*, accessed June 5, 2015. http://www.gallup.com/poll/178856/hacking-tops-list-crimes-americans-worry.aspx?utm_source=alert&utm_medium=email&utm_content=heading&utm_campaign=syndication.
- iii. “Criminal Attacks: The New Leading Cause of Data Breach in Healthcare,” Ponemon Institute, accessed June 4, 2015. <http://www.ponemon.org/blog/criminal-attacks-the-new-leading-cause-of-data-breach-in-healthcare>.
- iv. Greenberg Andy, “Hackers Remotely Kill a Jeep on the Highway—With Me in It,” *Wired*, July 21, 2015, accessed Aug. 6, 2015. <http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>.
- v. “Recalls and Defects,” *NHTSA*, accessed Aug. 6, 2015. <http://www.nhtsa.gov/Vehicle+Safety/Recalls+%26+Defects>.
- vi. “Hacking Tops List of Crimes Americans Worry about Most,” *Gallup*, accessed June 5, 2015. http://www.gallup.com/poll/178856/hacking-tops-list-crimes-americans-worry.aspx?utm_source=alert&utm_medium=email&utm_content=heading&utm_campaign=syndication.

Introduction to Security

After completing this chapter you should be able to do the following:

- Describe the challenges of securing information
- Define information security and explain why it is important
- Identify the types of attackers that are common today
- Describe attacks and defenses



Security in Your World

"Here's your latte," said Cora, as she set the two cups down on the table. Mia looked up from her phone. "Thanks. I promise I'll pay you back," she said. Mia and Cora had stopped at the coffee house between classes at the college they attended. "That's OK," said Cora. "But as I was paying for our drinks I noticed that the man in front of me pulled cash out of his billfold to pay for his coffee. Now when was the last time you saw someone here pay cash?"

Mia took a sip of her latte. "Well, it's not very often. How did you pay?" she asked. Cora sat down at the table. "I just tapped my phone on that black thing on the counter." Mia smiled. "So you used a contactless payment system by launching a mobile payment app on your smartphone and touching the reader." Cora laughed and said, "OK, if you say so." Mia was majoring in Computer Information Systems and wanted to go into the field of computer security, and she often tried to help Cora use the correct technical terminology. Mia set down her phone and said, "Well, maybe that man in front of you paid with cash because he was worried about security. In my Introduction to Computers class last week we read an article about how vulnerable these payment systems can be."

"Oh, there you go with security again," Cora said. "I think that is really overblown. I saw something online last week that said, 'Millions of Internet Users Could Be at Risk' but I never heard of anyone who had a problem. And I've never been attacked, and you know how much time I spend online!" Mia grinned. "Oh, did you expect those millions of users to send you an email when they were attacked? Actually, you've already had some attacks targeted at you today." Cora looked puzzled. "Like what?"

Mia took another sip of her latte and then said to Cora, "Look at your school email account." As Cora took out her phone and looked at her emails Mia said, "Do you have a weird email from Tommaso?" Cora scrolled through her inbox and then stopped. "Yes, here it is. The only thing the email has is a link to a website I've never heard of. That's strange. Why did he send that to me? And how did you know about it?" Cora asked. Mia said, "I received the same one. Tommaso's email account has probably been compromised and it's sending out these spam emails to everyone in his address book, including you and me." "Well, he needs to have that antivirus software stuff on his computer," Cora said.

Mia picked up her phone again. "No, antivirus software doesn't stop everything. And look at this next email message: 'You have exceeded your email limit. All student email accounts need to be revalidated by clicking on the link below.' Of course, if you click on the links, you're bound to get infected, probably just like Tommaso. And did you see the email last week from the college that a database of personal records of over 100,000 students and alumni going back 5 years was stolen by attackers? Whoever did it may already have our names, addresses, Social Security numbers,

and even the financial data we used for our student loans. No antivirus software on your computer is going to stop that from happening.”

Cora pushed her chair back in frustration. “Well, now I’m mad. Why can’t they just stop these attacks? And how am I supposed to know what to do?”

1

Our world today is one in which everyone has been forced to continually protect themselves, their families, and their property from attacks by invisible foes. Bombings, random shootings, airplane hijackings, and other types of physical violence occur around the world with increasing frequency. To counteract this violence, new types of security defenses have been implemented. Passengers using public transportation are routinely screened before boarding. Fences are erected across borders. Telephone calls are monitored. These attacks and the security defenses against them have impacted virtually every element of our lives and they significantly affect how all of us live each and every day.

And these attacks are not just physical. Our computers and technology devices are also frequent targets of attacks. An endless stream of malicious attacks is directed at individuals, schools, businesses, and governments through desktop computers, laptops, smartphones, and tablets. Internet web servers must repel thousands of attacks every day. Identity theft using stolen electronic data has skyrocketed. An unprotected computer connected to the Internet can be infected within minutes. Terms like *phishing*, *rootkits*, *worms*, *zombies*, and *botnets*—virtually unheard of just a few years ago—are now part of our everyday security technology vocabulary.

Although all computer users have heard about attacks that can threaten the security of their devices—and many have already been victims of attacks—the overwhelming majority of users are unsure about how to actually make their devices secure. Ask yourself this question: If you were warned that a particularly nasty Internet attack was to be released within the next few hours, what would you do to protect your computer and the information on it? Install antivirus software? Download a patch? Turn on a firewall? Unplug your Internet connection? Or do nothing and hope for the best?

It is important for all computer users today to be knowledgeable about computer security and to know what steps to take to defend against attacks. Applying practical security in your world has never been more important than it is right now.

This chapter introduces you to computer security. It begins by examining the current challenges in computer security and why it is so difficult to achieve. It then describes information security in more detail and explores why it is important. Finally, the chapter looks at who is responsible for these attacks and outlines the steps to build a comprehensive security strategy.

Challenges of Securing Information

“Why can’t we stop all these attacks?” is a question that is often heard. Although it may seem that there should be a straightforward and easy solution to preventing attacks and securing our computers, in reality there is no single simple solution. This can be seen through the different types of attacks that computer users face today as well as the difficulties in defending against these attacks.

Today's Attacks

Despite the fact that information security continues to rank as a high concern and tens of billions of dollars are spent annually on computer security, the number of successful attacks continues to increase. Information regarding recent attacks includes the following:

- Attacks directed at point-of-sale (PoS) systems in retail stores resulted in over 1.02 billion records of consumers' payment card information being stolen in a single year. This averages to 2.8 million records stolen each day or 32 records every second.¹ These malicious programs, called "memory-scrapers," steal a user's payment card numbers as soon as the card is swiped at the PoS. Because today's PoS terminals are specialized desktop or tablet computers, attackers are infecting these devices by sending emails to retailers that pretend to be from someone looking for a job, with the subject line as "Any Jobs?" or "My Resume." Attached to the email is a Microsoft Word file that pretends to be a resume and even says "Protected Document: This file is protected by Microsoft Office." Yet the file contains a malicious program that when opened will infect the PoS system.
- One of the main targets of attackers today is the healthcare industry. That is because healthcare records contain much more than just a patient's payment card number. These records contain medical information and financial information about the patient and family, which can then be used to steal their identities. In addition, stolen medical records can be used for billing fraud (charging medical treatments to the victim), for medical identity theft (pretending to be the victim to receive medical care), and even for purchasing drugs for resale. And because federal laws prohibit health plans from having annual or even lifetime dollar limits on most medical benefits, attackers can use stolen healthcare information to perform frauds that result in huge sums. An industry report revealed that in one year healthcare providers and payers reported a 60 percent increase in detected attacks, with financial losses from these attacks increasing 282 percent over the previous year.² Another report indicated that in a 24-month period 91 percent of healthcare organizations reported at least one breach, 39 percent reported two to five data breaches, and 40 percent had more than five data breaches. The total cost for healthcare data breaches is about \$6 billion per year, with the average loss to each organization of \$2,134,800.³
- Vulnerability in home wireless networking equipment was found in 90 products from 25 major manufacturers, which could allow attackers to launch their malicious software against any device connected to the home network. The vulnerable service that runs on the equipment cannot be disabled nor can the attacks coming from the Internet be blocked. While some manufacturers issued immediate fixes for their equipment, other manufacturers said that fixes would take several months to create and distribute to consumers. And some manufacturers said that their products have reached "end-of-life" and would not be patched.⁴
- A magazine reporter agreed to let two security researchers demonstrate how easy it was for a car to be remotely controlled. From a location ten miles away, the researchers manipulated the car's air conditioning, radio, and windshield wipers, which the driver could not change. As the driver pressed the accelerator while merging onto a crowded Interstate highway the car started slowing down with an 18-wheeler barreling down on him as the researchers continued to manipulate the car. The researchers even disabled the brakes so that the car ended up in a ditch.⁵ This incident prompted the National Highway

Traffic Safety Administration (NHTSA) to recall 1.4 million vehicles to patch this vulnerability, making it the first time that cars had been recalled due to a security vulnerability.⁶

- It has been speculated for several years that someone could manipulate aircraft while in flight because the systems that control the aircraft are not properly protected. According to the FBI, a security researcher may have actually done that. On a flight between Chicago and Syracuse a researcher tweeted that he was probing the aircraft systems of his flight. The airlines' Cyber Security Intelligence Department, which monitors social media, saw the tweet and alerted the FBI. According to the FBI, a special agent later examined the first-class cabin seat where the researcher was seated and found that he had tampered with the Seat Electronic Box (SEB), which is located under some passenger seats. This allowed him to connect his laptop to the in-flight entertainment (IFE) system via the SEB. Once the researcher accessed the IFE he could then access other systems on the plane. The researcher claims that he was able to cause the airplane to climb after manipulating its software. The airline has now banned him from all of its flights.⁷
- Many cars today offer a Passive Keyless Entry and Start (PKES) system, which allows the driver to unlock the doors and start the car without having to take the key out of her pocket or purse. All a driver has to do is get close enough to the car for the wireless signal from their key fob to be detected by the car, and once detected the doors automatically unlock and the engine can be started by pushing a button on the dashboard. Recently a neighborhood in Los Angeles was experiencing a series of mysterious break-ins on cars that had PKES systems. One person, who happened to be a newspaper reporter, had his car entered three times but there was no evidence of forced entry. One day as the reporter watched his car from inside his house he saw a young girl ride up on her bicycle and then take out of her backpack a small black device. She then walked over and unlocked the car and climbed in. The owner ran outside and the girl quickly left. Evidently the girl used an inexpensive power amplifier: when she turned the amplifier on it increased to over 50 feet (15 meters) the distance that the car could search for the key fob. Although the key fob was sitting on the kitchen counter inside the reporter's house, the car was still able to detect it and was fooled into thinking that the driver was approaching the car.⁸ The cost of the amplifier is as little as \$17. Car owners who want to protect themselves from this attack are being told to put their keys in their freezer, which will stop an amplified signal from reaching the key.
- A sample set of tens of thousands of malicious files were scanned by the four most commonly deployed antivirus products. Within the first hour the antivirus products only identified 30 percent of the malicious software. It took 24 hours before these products correctly identified 66 percent of the infected files as malicious, and after seven days the accumulated total was 72 percent. However, it took more than six months for the four antivirus products to correctly identify and protect all of the malicious files. Based on the average number of infections being distributed by attackers this means that these antivirus products would have missed 796 malicious files each day.⁹
- The iconic entertainer Madonna was forced to quickly move up for immediate purchase the release of six tracks from one of her upcoming albums, although the album was not scheduled to appear for another three months. This emergency release was due to the fact that 13 prerelease recordings, which was probably the entire album, were stolen and leaked onto the Internet. In addition, previously unpublished photos were also taken and posted without permission. Madonna stated that in order to combat future leaks her content will no longer be placed on any devices that are connected to a



network or the Internet. Instead, hard drives containing music will be hand-carried to recipients. Madonna went on to say that at any future photo or video recordings everyone involved will be required to leave their cell phones checked at the door.¹⁰

- In a recent survey 69 percent of Americans report they frequently or occasionally worry about having their payment card information stolen by cyberattackers. This compares with 45 percent who worry about their home being burglarized and 7 percent who are concerned about being assaulted by a coworker. Americans between the ages of 30 and 64 worry about this more than younger and older Americans do. And almost one out of three said that either they or another household member had information from a payment card used at a store stolen by computer attackers during the last year, making this the most frequently experienced crime on a list of nine crimes.¹¹
- Despite the fact that some Apple computer users may feel that their devices are more secure than those from other manufacturers, vulnerabilities in Apple devices continue to be exposed and manipulated by attackers. Recently a critical vulnerability on Apple computers was found based on a flawed energy conservation implementation that left protections unlocked on the affected Macs after they woke up from sleep mode. This vulnerability was rated as critical since it can provide an attacker with persistent access to a computer even if a user completely wiped her hard drive clean and reinstalled the operating system. All but the latest models of Apple Mac computers are affected by this vulnerability.¹²
- The number of security breaches that expose users' digital data to attackers continues to rise. From January 2005 through July 2015, over 853 million electronic data records in the United States were breached, exposing to attackers a range of personal electronic data, such as address, Social Security numbers, health records, and credit card numbers.¹³ Table 1-1 lists some of the security breaches that occurred during only a one-month period, according to the Privacy Rights Clearinghouse.¹⁴

Organization	Description of security breach	Number of identities exposed
Office of Personnel Management	Current and former federal employees exposed employees' job assignments, performance, and training, and may have exposed Social Security information and/or financial information.	4,000,000
CareFirst BlueCross BlueShield	The breach of a single database exposed names, birth dates, email addresses, and insurance identification numbers.	1,100,000
Penn State's College of Engineering	In two different intrusions attackers accessed "sensitive data" of all College of Engineering students, faculty, and staff.	18,000
Salley Beauty	"Unusual activity of payment cards at some stores" followed a similar attack 60 days before in which information on over 25,000 customer payment cards was stolen.	Unknown
AT&T	In three separate incidents employees accessed customer names and Social Security numbers, which were then sold to outsiders who used that information to unlock stolen cell phones.	280,000
Anthem BlueCross BlueShield	Names, birthdays, medical IDs, Social Security numbers, street addresses, email addresses, employment and income information were stolen in an attack that may have gone undetected for ten months.	80,000,000

Table 1-1 Selected security breaches involving personal information in a one-month period

Difficulties in Defending against Attacks

The challenge of keeping computers secure has never been greater, not only because of the number of attacks but also because of the difficulties faced in defending against these attacks. These difficulties include the following:



- *Universally connected devices.* It is unthinkable today for any technology device—desktop computer, tablet, laptop, or smartphone—not to be connected to the Internet. Although this provides enormous benefits, it also makes it easy for an attacker halfway around the world to silently launch an attack against a connected device.
- *Increased speed of attacks.* With modern technology attackers can quickly scan millions of devices to find weaknesses and launch attacks with unprecedented speed. Today's attack tools initiate new attacks without any human participation, thus increasing the speed at which systems are attacked.
- *Greater sophistication of attacks.* Attacks are becoming more complex, making it more difficult to detect and defend against them. Attackers today use common Internet protocols and applications to perform attacks, making it more difficult to distinguish an attack from legitimate network traffic. Other attack tools vary their behavior so the same attack appears differently each time, further complicating detection.
- *Availability and simplicity of attack tools.* Whereas in the past an attacker needed to have an extensive technical knowledge of networks and computers as well as the ability to write a program to generate the attack, that is no longer the case. Today's software attack tools do not require any sophisticated knowledge on the part of the attacker. In fact, many of the tools, such as the Kali Linux interface shown in Figure 1-1, have a graphical user interface (GUI) that allows the user to easily select options from a menu. These tools are freely available or can be purchased from other attackers at a surprisingly low cost.
- *Faster detection of vulnerabilities.* Weakness in hardware and software can be more quickly uncovered and exploited with new software tools and techniques.
- *Delays in security updating.* Hardware and software vendors are overwhelmed trying to keep pace with updating their products against attacks. One antivirus software security institute receives more than 390,000 submissions of potential malware *each day*.¹⁵ At this rate the antivirus vendors would have to create and distribute updates *every few seconds* to keep users fully protected. This delay in distributing security updates adds to the difficulties in defending against attacks.
- *Weak security updates distribution.* While vendors of mainstream products, such as Microsoft, Apple, and Adobe, have a system for notifying users of security updates for many of their products and distributing them on a regular basis, few other software vendors have invested in these costly distribution systems. Users are generally unaware that a security update even exists for a product because there is no reliable means for the vendor to alert the user. Also, these vendors often do not create small security updates that “patch” the existing software, but instead they fix the problem in an entirely new version of the software—and then require the user to pay for the updated version that contains the patch.



Figure 1-1 Menu of attack tools

Source: Kali Linux



Vendors of smartphone operating systems are particularly well known for not providing security updates on a timely basis, if at all. Most vendors and wireless carriers do not attempt to provide users with significant updates (such as from version 5.6 to 5.7), instead hoping that users will purchase an entirely new smartphone—and service contract—to have the latest and most secure device.

- *Distributed attacks.* Attackers can use hundreds of thousands of computers under their control in an attack against a single server or network. This “many against one” approach makes it virtually impossible to stop an attack by identifying and blocking a single source.
- *User confusion.* Increasingly, users are called upon to make difficult security decisions regarding their computer systems, sometimes with little or no information to guide them. It is not uncommon for a user to be asked security questions such as *Do you want to view only the content that was delivered securely?* or *Is it safe to quarantine this attachment?* or *Do you want to install this extension?* With little or no direction, users are inclined to provide answers to questions without understanding the security risks. In addition, popular information that is circulated about security through consumer news outlets or websites is often inaccurate or misleading, resulting in even more user confusion.

Table 1-2 summarizes the reasons why it is difficult to defend against today’s attacks.



Reason	Description
Universally connected devices	Attackers from anywhere in the world can attack.
Increased speed of attacks	Attackers can launch attacks against millions of computers within minutes.
Greater sophistication of attacks	Attack tools vary their behavior so the same attack appears differently each time.
Availability and simplicity of attack tools	Attacks are no longer limited to highly skilled attackers.
Faster detection of vulnerabilities	Attackers can discover security holes in hardware or software more quickly.
Delays in security updating	Vendors are overwhelmed trying to keep pace updating their products against the latest attacks.
Weak security update distribution	Many software products lack a means to distribute security updates in a timely fashion.
Distributed attacks	Attackers use thousands of computers in an attack against a single computer or network.
User confusion	Users are required to make difficult security decisions with little or no instruction.

Table 1-2 Difficulties in defending against attacks

Security in Your World

As she waited for her class to start, Cora turned around to talk with her friend Abby about the conversation she had earlier with Mia. Cora said, “You read about this security stuff all the time, but I don’t have a clue what they’re talking about. It’s like they’re talking over my head about ‘vulnerabilities’ and ‘threats.’ ” Abby nodded her head. “I know what you mean.” Then she continued, “But who would want to break into our computers or cell phones? And so what if they did? What’s the worst thing that can happen? They would read our email and texts? Let them! Really, what do we have that somebody would want?”

Cora opened her book as her instructor walked into the room. “But Mia said that there are all sorts of bad things that can happen if you’re attacked.” “Like what?” asked Abby skeptically. “Remember yesterday when you said that you went online and bought that birthday present for your brother and used your credit card number?” Cora asked. “Mia said that an attacker online could steal your credit card number and then use it to charge things to your account.” Abby paused. She remembered that her Uncle Greg had his credit card number stolen earlier this year and had thousands of dollars charged on it. “And what if an attacker got into your computer and just erased everything? Think of all those photos you have stored on your computer. You wouldn’t want to lose them.” “Well, OK,” said Abby.

(continues)