Computer Security Literacy

Staying Safe in a Digital World

Douglas Jacobson and Joseph Idziorek

CRC Press
Taylor & Francis Group
A CHAPMAN & HALL BOOK

Computer Security Literacy
Staying Safe in a Digital World

Douglas Jacobson · Joseph Idziorek

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

A CHAPMAN & HALL BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed in the United States of America on acid-free paper
Version Date: 20120831

International Standard Book Number: 978-1-4398-5618-5 (Paperback)

Library of Congress Cataloging-in-Publication Data

Jacobson, Douglas.
Computer security literacy : staying safe in a digital world / Douglas Jacobson, Joseph Idziorek.
pages cm
Includes bibliographical references.
ISBN 978-1-4398-5618-5 (pbk.)
1. Computer security. I. Idziorek, Joseph. II. Title.

QA76.9.A25J224 2013
005.8--dc23 2012028121

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Computer Security Literacy
Staying Safe in a Digital World

Preface

APPROACH

Traditional computer security books educate readers about a multitude of topics, ranging from secure programming practices, protocols, and algorithm designs to cryptography and ethics. These books typically focus on the implementation or theory of security controls and mechanisms at the application, operating system, network, and physical layers. Breaking this traditional model, *Computer Security Literacy: Staying Safe in a Digital World* instead seeks to educate the reader at the user layer and focuses on practical topics that one is likely to encounter on a regular basis. It has long been recognized that the user is in fact the weakest link in the security chain. So, why not effect change by providing practical and relevant education for the normal user of information technology? As it turns out, we, the users, often have the greatest impact on the security of our computer and information as a result of the actions that we do or do not perform. This text provides practical security education to give the context to make sound security decisions. The outcomes of this book will enable readers to

- Define computer security terms and mechanisms
- Describe fundamental security concepts
- State computer security best practices
- Describe the strengths, weaknesses, and limitations of security mechanisms and concepts
- Give examples of common security threats, threat sources, and threat motivations
- Explain their role in protecting their own computing environment and personal and confidential information

- Discuss current event topics and read security articles in the popular press
- Assess computing actions in the context of security

The approach of this book is to provide context to everyday computing tasks to better understand how security relates to these actions. One of the most common ways that security professionals attempt to bestow knowledge is through awareness campaigns and the creation of websites that contain security tips and advice. If you have discovered this book, then you are likely aware computer security is a real and ever-present problem. Whether seen or unseen, everyday users of information technology encounter a number of security threats whether it be in the form of suspect emails, social networking posts, hyperlinks, or the downloading of files or programs from the Internet. While awareness is key, it does not provide the context for one actually to go forth and make sound security decisions. Security tip and advice websites, on the other hand, attempt to supplement learning by the offering of a handful of security best practices. A popular tip found on such a website is "make passwords long and strong." While this statement makes logical sense, it does nothing to inform the user of the threats that this security tip protects against. Furthermore, and more important, it does not discuss the limitations of this suggestion and if simply creating a long-and-strong password is sufficient to protect against all the threats that seek to learn, steal, or observe passwords. As discussed in Chapter 3, creating a long-and-strong password is important, but it is only a small part of the equation necessary to create and maintain secure passwords.

Because there is a common perception that computer security is a topic of concern only for the technological elite, there exists a significant gap between the types of books currently offered in computer security and the demographic of people who stand to benefit from learning more about the practical aspects of computer security. Many of the previously written texts on computer security are too technical for a broad audience and furthermore do not contain practical computer knowledge about common security threats, best practices, and useful content on how security mechanisms such as antivirus software and firewalls protect against hackers and malware. One of the unique qualities that differentiates this book from past security texts is that it was written specifically for a diverse and nontechnical audience. To do this, the key concepts of the book are balanced by commonly held analogies. In addition, relevant and recent

current events are used to provide tangible evidence regarding the function and impact of security in everyday life.

Computer security education need not be made exclusive to technical audiences. If abstracted correctly, it is our belief that practical security education can be made accessible to readers of all technological backgrounds. As it turns out, we all perform the same basic routines on our computers and the Internet each day. During an average day, people use passwords, connect to the Internet on an unsecure wireless connection, share media via external devices, receive suspicious emails, surf the web, share information via social networking, and much, much more. Each of these actions involves a potential risk and can result in consequences with malicious intent. However, the understanding of these risks and corresponding defensive strategies is not as complicated as you would think and does not require an engineering degree as a prerequisite to gain working knowledge. While defensive security measures like antivirus software, firewalls, and software patches have been around for quite sometime, we truly believe that practical security education—the content found in this book—is the future of innovation in computer security.

ORGANIZATION

The content of this text is presented in a logical progression of topics that allows for a foundation to be constructed and context to be built on as the reader progresses through the chapters. The organization of the book is as follows:

- **Chapter 1** presents an introduction to the topic of computer security, defines key terms and security truisms, as well as discusses commonly held, but inaccurate, conceptions about the topic of computer security.
- **Chapter 2** provides the technological foundation for the remainder of the book by developing a working model for how a computer operates and how the Internet moves data from one computer to another.
- **Chapter 3** discusses the many threats that seek to steal, observe, and learn passwords. Once the threats are understood, this chapter provides password security best practices and defines a secure password as not only a strong password but also a unique and secret password.
- **Chapter 4** focuses on the topic of email and broadly presents how email is sent and received on the Internet. With this context in hand,

the many threats that plague the common uses of email are discussed, and mitigation strategies are presented.

- **Chapter 5** focuses on all the different ways that malware infects a computer and what malware does once it infects a computer.
- **Chapter 6** supplements Chapter 5 by providing a defense-in-depth strategy to mitigate against the many malware threats that one is likely to encounter. The defense-in-depth strategy consists of data backup, software patches, firewalls, antivirus software, and last but not least, user education.
- **Chapter 7** deals primarily with the operation of the web browser and how functions that afford convenience also are at odds with security and privacy. This chapter also discusses the popular and applicable topics of HTTPS and cookies, among other types of information stored by web browsers.
- **Chapter 8** presents the topic of online shopping by discussing common security threats and online shopping best practices, such as the motivation why using a credit card is more secure than a debit card when making online purchases.
- **Chapter 9** explains the security vulnerabilities that wireless networks present. Included in this discussion is an explanation of the differences between a secure and unsecure wireless network and the security threats and best practices for both a user of a wireless network (as typically found in a coffee shop) and as an administrator of a home wireless network.
- **Chapter 10** takes a different approach to social networking security and privacy by focusing on the higher-level concepts as they relate to public information sharing. A key discussion includes how information that is found on social networking sites affects one's job or career prospects.
- **Chapter 11** unravels the many different ways that cyber criminals use social engineering tactics to trick their victims into revealing personal information or installing malware on their computers. Included in this chapter are the steps one can take to dissect a URL (Uniform Reference Locator) and how to consider each part of the

URL in the context of security—a key skill to detect phishing emails and messages.

- **Chapter 12** examines the human threat of practical security by discussing a number of concepts and scenarios of how actions in the virtual world can have negative repercussions in the physical world.
- **Chapter 13** provides context to many of the security best practices discussed throughout the chapters by way of case studies or scenarios that one will typically encounter in the everyday use of information technology.
- **Chapter 14** summarizes the text and presents the steps to continue learning about computer security as well as daily, weekly, and monthly tasks individuals should perform to keep their defense-in-depth strategy current.
- **Appendix A** suggests a number of books and websites for readers to continue their exploration of computer security and to stay current on the latest security trends.
- **Appendix B** delivers supplemental context and a brief background into the topic of cryptography. Included are the terms and concepts that form the basic building blocks of cryptography as well as the function of cryptography in everyday computing.
- **Appendix C** introduces a number of web and Internet-based technologies that can be used to further increase one's defense-in-depth strategy when surfing the web. Technologies such as link scanners, virtual private networks (VPNs), and private browsing are presented to help prevent against common Internet-based threats or privacy concerns.
- A **Glossary** is provided as a quick-access resource for common security terminology.

TARGET AUDIENCE

This book is truly meant for anyone interested in information technology who wants to understand better the practical aspects of computer security. The only prerequisites that a reader needs are prior use of a computer, web browser, and the Internet. Depending on your motivation for wanting to learn more about practical computer security knowledge, this book serves many different audiences. Although originally written to provide a

much-needed textbook for a course on introduction to computer security literacy at the university, college, community college, or high school levels, by no means is this an exclusive audience. The content presented in this book would also be a great resource for corporate training as many of the same activities that one performs when using a computer and the Internet for personal reasons overlap with many common business functions (i.e., email, surfing the web, social networking). Furthermore, the layout and presentation of the content of this book are tailored toward a normal user of information technology and would serve as an excellent read for anyone desiring a self-guided introduction to practical computer security.

Perhaps you have had your identity stolen, had your email account hacked, or have experienced a number of malware infections in the past. On the other hand, maybe you are interested in learning how antivirus software works, the weaknesses of firewalls, or how malware spreads and its function once it infects a computer. Or, maybe you want to acquire a working knowledge of computer security terminology, security mechanisms, and threats to give you an edge at work. Each of these reasons, and many more, are the exact motivations that the content found in this book seeks to address. Information technology has become ingrained into almost every aspect of our daily lives, from browsing the web and social networking to email and surfing the Internet at a coffee shop. However, it has been our experience that as technically savvy as our society has become, the same savviness has not extended into the realm of practical computer security knowledge. Whatever your motivation, this text serves as a practical guide to navigating the many dangers that unfortunately accompany the numerous conveniences that technology affords.

SCREENSHOT DISCLAIMER

It should be noted that technology is constantly evolving, and as this evolution takes place, the provided screen shots will likely become outdated. Despite this challenge, we have strived to provide underlying context so that even if the appearance of a particular screenshot changes, the explanation of the core technology will remain relevant.

Website: www.dougj.net/literacy

ACKNOWLEDGMENTS

Doug Jacobson: I want to thank my wife, Gwenna, and our children, Sarah, Jordan, and Jessica, for their support, patience, and love. And a special thank you to Sarah for designing the art for the book cover.

Joseph Idziorek: Thank you to my fiancé, Arlowyn, the love of my life, to my parents and my sister Katie for all their support, and to my amazing friends.

Both authors would like to thank Dr. Terry Smay for his input and editing help.

About the Authors

Douglas Jacobson is a university professor in the Department of Electrical and Computer Engineering at Iowa State University. He is currently the director the Iowa State University Information Assurance Center, which has been recognized by the National Security Agency as a charter Center of Academic Excellence for Information Assurance Education. Dr. Jacobson teaches network security and information warfare and has written a textbook on network security. Dr. Jacobson's current funded research is targeted at developing robust countermeasures for network-based security exploits and large-scale attack simulation environments; he is the director of the Internet-Scale Event and Attack Generation Environment (ISEAGE) test bed project. Dr. Jacobson has received two R&D 100 awards for his security technology, has two patents in the area of computer security, and is an IEEE Fellow.

Joseph Idziorek received his PhD in computer engineering from the Department of Electrical and Computer Engineering at Iowa State University. As a graduate student, he developed an introductory course, Introduction to Computer Security Literacy, and taught the course 10 times to over 250 students. Dr. Jacobson and Dr. Idziorek have also authored two publications regarding this course. Apart from practical security education, Dr. Idziorek's research interests include cloud computing security and the detection and attribution of fraudulent resource consumption attacks on the cloud utility pricing model. He has authored a number of conference and journal publications on this research topic. Dr. Idziorek now works as program manager at Microsoft.

Contents