Advanced Persistent Training

Take Your Security Awareness Program to the Next Level

Jordan Schroeder, CISSP, CISM

Apress®

Advanced Persistent Training

Jordan Schroeder
Edinburgh, United Kingdom

ISBN-13 (pbk): 978-1-4842-2834-0 ISBN-13 (electronic): 978-1-4842-2835-7
DOI 10.1007/978-1-4842-2835-7

Library of Congress Control Number: 2017943503

Cover image designed by Freepik

Managing Director: Welmoed Spahr
Editorial Director: Todd Green
Acquisitions Editor: Nikhil Karkal
Development Editor: James Markham
Technical Reviewer: Gandhi Aryavalli
Coordinating Editor: Prachi Mehta
Copy Editor: Kim Wimpsett
Compositor: SPi Global
Indexer: SPi Global
Artist: SPi Global

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail rights@apress.com, or visit www.apress.com/rights-permissions.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/9781484228340. For more detailed information, please visit www.apress.com/source-code.

Printed on acid-free paper

To my wife and daughter:
Contentment is knowing River …

Contents at a Glance

Contents

About the Author

Jordan Schroeder is a former department head at a technical school and corporate trainer. As an information security expert and a moderator of the Security.StackExchange.com site, he is dedicated to researching and delivering effective and innovative methods to teach professionals and laypeople alike how to digitally secure their organizations and the assets they control.

Jordan developed and runs SelfPhish, a phishing education and research platform aimed at discovering an individual's vulnerability to different types of social engineering attacks and then tailoring security awareness training to that individual. His experience and research through SelfPhish forms the basis for many of his opinions and recommendations in this book.

About the Technical Reviewer

Aryavalli Sriranga Narasimha Gandhi is a seasoned information security expert. He has been fighting as a soldier for the past 18 years, defending families from cyber-attacks, malware, and APTs (bots) by providing integrated security solutions on-premises and in the cloud and by reviewing security effectiveness at the compute, hyper, network, and app layers. He has represented OWASP as a global leader, driving security awareness across the globe. In addition, he has been a seasoned speaker about information security at NIT, Trichy, step-up conferences, and several nonprofit security conferences.

Acknowledgments

I wish to extend my gratitude to the following people who showed their support throughout this project:

Mark Chapman (PhishLine)
Winn Schwartau (The Security Awareness Company)
Joe Ferrara (Wombat Security Technologies)
Todd Lefkowitz (Rapid7)
Nick Santora (Curricula)
Rohyt Belani (PhishMe)
Chris Hadnagy (Social-Engineer.com)
Geordie Stewart (Risk Intelligence, Ltd.)
Alison Truelove
Richard Evans
Dan Buhler
Secure the Human Community

In addition to the companies that have provided their insights on the topics in this book, the following companies have been wonderful in their support for this project:

www.PhishMe.com

www.Social-Engineer.com

www.TheSecurityAwarenessCompany.com

Foreword

I cannot believe I fell for it!

About a month ago, a semi-authentic-sounding stranger asked me to review a book he was writing on phishing. His unsolicited e-mail was very polite and personalized. It promised to mention my company alongside my competitors, who were already included in the alleged book. It had a link to a somewhat offensive-sounding web site, GoPhishYourself. A few words were consistently misspelled from my U.S.-centric perspective. Of course, there was urgency to "act now before the publication date." If I agreed, he promised to send me a draft of the book as a PDF attachment.

As a "visionary leader" in the field of automated social engineering and security awareness training, it was not possible to ignore such an epic phish! With proper technical controls and a keen sense of irony, I carefully clicked the link, replied to the e-mail, and opened the PDF.

Unbelievably, not only did the draft of the book seem legitimate, it was actually good!

On our first phone call, I had to get to the bottom of what this author, or seriously committed phisher, wanted from me. Surprisingly, he did not want sponsorship money, credit card numbers, or bitcoins. He was an educator, information security professional, trainer, software developer, and blogger who felt that there was a book that needed to be written. To complement his extensive hands-on experience, he had spent a lot of time researching and talking to other educators, security professionals, and leaders in the security awareness industry. He was open to feedback and was committed to sharing his best work with the information security community.

Fast-forward through many in-depth phone calls and several major revisions, and the book is now a reality. The book was written for the growing number of information security professionals and trainers who need to take an established information security awareness program to the next level. After spending many years working with the best people in this profession, I am happy to be invited to make a small contribution to Jordan's work.

For the first part of the book, the style is to provide a full explanation of some fundamental security awareness concepts, with a wealth of specific references for further research and support. About halfway through the book, Jordan's style really shines, with thought-provoking insights and references that are not typically found in this context. Jordan has a way of filling in the gaps for theories or articles that were on the fringes of visibility and taking them front and center. All you need to do is kick back and read a few succinct paragraphs to gain a better understanding of some pretty sophisticated concepts. He then goes a step further to share the voice of other information security awareness leaders. Believe me, it is not easy to get a hold of these people, much less get them to take the time to contribute to a project. I wonder if he phished them too?

The book starts out with an introduction to the challenges faced by information security awareness teams. It is a good warm-up to get us on the same page as Jordan describes many of the common challenges faced by information security professionals charged with running a security awareness program, without the benefit of also being trained educators. Jordan provides some great insights into how to change habits and affect behaviors. As security professionals, we have all experienced the struggle to overcome the challenges to motivate adoption without necessarily being armed with formal concepts such as overcoming "inconvenience without benefit."

The book also talks about building active feedback into a mature program using gamification and habit coaching techniques to improve the effectiveness of the program. I like how Jordan is not afraid to share his perspective with objective references to support the position. The quality bibliographic references will be useful to help growing programs get to the next level.

At this point, Jordan really steps up to provide interesting insights on how to create a partnership with the learner. His real-world experience shines when sharing thoughts on incident response. I looked good in a meeting just the other day because I shared his concept of "report and then get trained" as a possible method to increase the effectiveness of an incident response program.

The coverage of persistent training provides a nice background for training concepts such as graduated learning and spaced repetition. He also shares some useful advice about not getting carried away with your mock phishing tests, which is a common problem because it is just so much fun!

Jordan wraps up his dedicated work by sharing some professional tips that quickly go beyond the obvious. All of us are vaguely aware of generational differences in the workforce, the importance of relating to real attacks, and the value of "train the trainer." Jordan's tips will help you take your program to the next level with confidence.

As a whole, the book provides solid insights into improving your enterprise information security program. It arms the reader with thoughtful views and supporting references to help all organizations improve. The concepts in the book have already helped me sound more educated while igniting or reigniting some lively debates, rants, and discussions with my friend Chris Hadnagy, social engineering guru and author of *Phishing Dark Waters* and other titles.

While part of me is still wondering whether this whole project is the world's most epic phishing scam, we all will undoubtedly learn from the insights and research embedded in the following pages. Jordan's book is a clear benefit to our industry and, indeed, is a book that needed to be written. Enjoy!

Mark T. Chapman, CFE CISM CISSP CRISC
President and founder, PhishLine LLC
Milwaukee, Wisconsin