

CHRISTOPHER HADNAGY
MICHELE FINCHER
FOREWORD BY ROBIN DREEKE

PHISHING DARK WATERS

The Offensive and Defensive
Sides of Malicious E-mails



WILEY

Phishing Dark Waters



Phishing Dark Waters

The Offensive and Defensive Sides of
Malicious E-mails

Christopher Hadnagy
Michele Fincher

WILEY

Phishing Dark Waters: The Offensive and Defensive Sides of Malicious E-mails

Published by
John Wiley & Sons, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

Copyright © 2015 by John Wiley & Sons, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-1-118-95847-6
ISBN: 978-1-118-95849-0 (ebk)
ISBN: 978-1-118-95848-3 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Web site may provide or recommendations it may make. Further, readers should be aware that Internet Web sites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services please contact our Customer Care Department within the United States at (877) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at <http://booksupport.wiley.com>. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2015933609

Trademarks: Wiley and the Wiley logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. Wiley Publishing, Inc., is not associated with any product or vendor mentioned in this book.

I dedicate this book to a few people who made it possible. My amazing wife, Areesa, you are one of the most patient, kind, and wise people I have ever met. I hold on to the dream of an eternal future.

Michele, thankfully Ping made that referral a few years ago. Without you this is not possible.

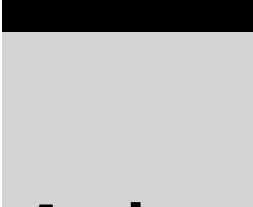
Dave, as I write these words, I can't believe how far we have come. Thank you for your support.

—Christopher Hadnagy

This is for my husband, the most beautiful soul in the universe and ruler of all my domains.

And to Chris; thank you for giving me a job and believing in me.

—Michele Fincher



About the Authors

Christopher Hadnagy is the founder and CEO of Social-Engineer, Inc. Chris possesses more than 16 years' experience as a practitioner and researcher in the security field. His efforts in training, education, and awareness have helped to expose social engineering as the top threat to the security of organizations today.

Chris established the world's first social-engineering framework at www.social-engineer.org, providing an invaluable repository of information for security professionals and enthusiasts. That site grew into a dynamic web resource, including a podcast and newsletter, which have become staples in the security industry and are referenced by large organizations around the world. Chris also created the first hands-on social-engineering training course and certification, *Advanced Practical Social Engineering*, which is attended by law enforcement, military, and private sector professionals.

A sought-after writer and speaker, Chris has spoken and trained at events such as RSA, Black Hat, and various presentations for corporate and government clients. Chris is also the best-selling author of two books: *Social Engineering: The Art of Human Hacking* (Wiley, 2010) and *Unmasking the Social Engineer: The Human Element of Security* (Wiley, 2014).

Chris specializes in understanding how malicious attackers exploit human communication and trust to obtain access to information and resources through manipulation and deceit. His goal is to secure companies by educating them on the methods used by attackers, identifying vulnerabilities, and mitigating issues through appropriate levels of awareness and security.

Chris is a certified Expert Level graduate of Dr. Paul Ekman's Micro Expressions courses, having made the study of nonverbal behaviors one of his specialties. In addition, he holds certifications as an Offensive Security Certified Professional (OSCP) and an Offensive Security Wireless Professional (OSWP).

Michele Fincher is the Chief Influencing Agent of Social-Engineer, Inc. She has more than 20 years' experience as a behavioral scientist, researcher, and information security professional. Michele's diverse background has helped solidify Social-Engineer, Inc.'s place as the premier social-engineering consulting firm.

As a U.S. Air Force officer, Michele's assignments included the USAF Academy, where she was a National Board Certified Counselor and Assistant Professor in the Department of Behavioral Sciences and Leadership. Upon separating from the Air Force, Michele went on to hold positions with a research and software development firm in support of the U.S. Air Force Research Laboratory, as well as with an information security firm, where she conducted National Security Agency appraisals and Certification and Accreditation for federal government information systems.

At Social-Engineer, Inc., Michele is a senior penetration tester with professional expertise in all facets of social-engineering vectors, assessments, and research. A remarkable writer, she is also the talent behind many of the written products of Social-Engineer, Inc., including numerous reports and assessments, blog posts, and the *Social-Engineer Newsletter*.

Michele is an often-requested trainer and speaker on various technical and behavioral subjects for law enforcement, the intelligence community, and the private sector in venues including the Black Hat Briefings, RSA, Techno Security, and the *Advanced Practical Social Engineering* training course.

Michele has her Bachelor of Science in Human Factors Engineering from the U.S. Air Force Academy and her Master of Science in Counseling from Auburn University. She is a Certified Information Systems Security Professional (CISSP).

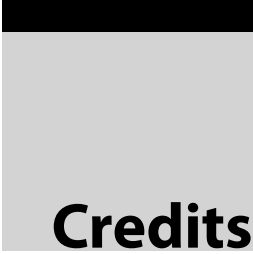


About the Technical Editor

David Kennedy is founder of Trusted Sec and Binary Defense Systems. Both organizations focus on the betterment of the security industry from an offense and a defense perspective. David was the former Chief Security Officer (CSO) for a Fortune 1000 company where he ran the entire information security program. David is a co-author of the book *Metasploit: The Penetration Testers Guide* (No Starch Press, 2011) and the creator of the Social-Engineer Toolkit (SET) and Artillery. David has been interviewed by several news organizations including CNN, Fox News, MSNBC, CNBC, Katie Couric, and BBC World News.

David is the co-host of the Social-Engineer Podcast and has appeared on a number of additional podcasts. David has testified in front of Congress on two occasions regarding the security around government websites. David is one of the co-authors of the Penetration Testing Execution Standard (PTES), a framework designed to fix the penetration testing industry. David is the co-founder of DerbyCon, a large-scale conference in Louisville, Kentucky.

Prior to working at Diebold, David was a VP of Consulting and Partner of a mid-size information security consulting company running the security consulting practice. And before working in the private sector, David worked for the United States Marine Corps and deployed to Iraq twice for intelligence-related missions.



Credits

Executive Editor

Carol Long

Project Editor

Charlotte Kughen

Technical Editor

David Kennedy

Production Editor

Christine O'Connor

Copy Editor

Charlotte Kughen

Manager of Content**Development and Assembly**

Mary Beth Wakefield

Marketing Director

David Mayhew

Marketing Manager

Carrie Sherrill

Professional Technology &**Strategy Director**

Barry Pruett

Business Manager

Amy Knies

Associate Publisher

Jim Minatel

Project Coordinator, Cover

Brent Savage

Proofreader

Nicole Hirschman

Indexer

Johnna Van Hoose Dinse

Cover Designer

Wiley

Cover Image

iStock.com/Evgeny Sergeev
and Fishhook iStock.com/Aslan
Alphan



Acknowledgments

In 2014 some life-altering changes occurred for me, and one of the many good ones was my team growing. As Michele and I started to teach my new team members my methodology for phishing awareness, it dawned on me that I had to write another book.

Phishing was being used in a large portion of the attacks we saw in the news, and people are still largely unaware of what phishing is and how to defend against it.

Yet, the clients I was working with were seeing drastic changes in behavior with regard to phishing e-mails—from 80+ percent click ratios and only a fraction of people reporting to less than 10 percent click ratios and more than 60 percent reporting. As the year progressed, those statistics kept climbing and falling in the right directions.

I had just recently finished *Unmasking the Social Engineer*, and I told my wife I would take a hiatus from writing. When I write, I become somewhat of a recluse; my amazing wife describes me as “difficult.” I can still see the scene; we were driving down the road, and I thought I would set up my desire to write a new book by talking about some of the recent news stories about security breaches. I started to talk about how phishing was such a huge problem, and I said that I only wished there were a book out there to help people do what we do.

As I paused, my wise and amazingly insightful wife said, “No; not another book right now.” I did what every good man would do in this situation and blamed my right hand, Michele.

“Well, Michele and I think it would be a good idea, and plus she will do a lot of the writing.”

And here we are at the end result—a documented precision journal on how to master the art of corporate phishing awareness programs. This book will not be covering the phishing often done in penetration testing, where an auditor uses phish to gain remote access. Instead this book focuses on getting your population aware and ready for the phishing attacks that will hit your organization.

There are many people that I want to thank and acknowledge, as this book would not have happened without them.

Again, I acknowledge my wife, Areesa. Thank you for your patience and support and for always letting me blab on about this stuff when you would rather talk about other things. I love you.

Michele, okay, so I didn't make you write most of the book . . . but still without your support this book would not have gotten finished. Thank you.

Carol, you fought for us on this book. I want you to know your effort didn't go unnoticed. Thank you for your support.

Charlotte, working with you was fun, rewarding, and very smooth. Thank you!

Dave K, you know, when you aren't pranking me, icing me, hugging me, making fun of me, embarrassing me, or annoying me with annoying music on the podcast, you really are a great guy. Thanks for your help with this book.

Nick Fureaux, thanks for letting me run ideas by you. Your constant support and advice are why I can continue.

Ping Look, well, if you hadn't spent those three hours talking me down about seven or eight Black Hats ago, referred Michele to me, and kept me grounded, well, this book wouldn't be happening.

My team—Amanda, Mike, Colin, Jessica, and Tamara—thank you for your support and stepping up when M and I needed to catch up on writing.

Robin, heck, who would have thought that after working together for a few years we would be where we are? Thank you for your continued support, friendship, and help. And a big thank-you for writing the foreword for this book.

My loyal clients, customers, and friends that let me run my ideas by them, thank you.

I know from my previous two books that there is no way to please everyone. Some of you will read this book and love it; some will hate it. All I ask is that if you find something wrong, or you see something you don't like or agree with, reach out to Michele and me. Talk to us and give us a chance to explain or correct if needed.

My hope is that you will see the hard work and effort that went into this book, that you will find it not only interesting but also useful on your journey to understand, educate on, and combat phishing attacks.

Thank you for once again letting me in your mind for a little while.

— Christopher Hadnagy, CEO and founder of Social-Engineer, Inc.

No one reads a phishing book just for fun, but my fondest wish is that you find this book both entertaining and useful. A major motivator for me was not only our client base but also the people in my life that I hope to make safer. My nieces and nephews have grown up on the Internet, and it terrifies me just a little that they could already be victims of identity theft before their lives really even begin. So this isn't just a book for security professionals. It's for anyone who ventures online to connect to the world.

As Chris mentioned, it takes a lot of support to write a book. I'm going to apologize ahead of time to the people I miss, because otherwise I'd be at this all day.

Being married to my husband was a major win when it came to writing this book. It turns out he has the ability to patiently endure cold and/or burned dinners while simultaneously doing research and editing my writing. I don't know how many times we had the "Do you really want to write that?" discussion over pizza (as a result of cold and/or burned dinners). Thank you, my love.

Chris, you could have picked anyone to help you write this book. I appreciate that I got that opportunity.

Amanda, Mike, Colin, Jess, and T, you know how hard you work. I do, too. Thank you.

To Carol and Charlotte at Wiley, thank you for making my first book experience wonderful.

— Michele Fincher, Chief Influencing Agent, Social-Engineer, Inc.



Contents at a Glance

Foreword		xxiii
Introduction		xxvii
Chapter 1	An Introduction to the Wild World of Phishing	1
Chapter 2	The Psychological Principles of Decision-Making	33
Chapter 3	Influence and Manipulation	53
Chapter 4	Lessons in Protection	75
Chapter 5	Plan Your Phishing Trip: Creating the Enterprise Phishing Program	97
Chapter 6	The Good, the Bad, and the Ugly: Policies and More	131
Chapter 7	The Professional Phisher’s Tackle Bag	147
Chapter 8	Phish Like a Boss	179
Index		189



Contents

Foreword	xxiii
Introduction	xxvii
Chapter 1 An Introduction to the Wild World of Phishing	1
Phishing 101	2
How People Phish	4
Examples	7
High-Profile Breaches	7
Phish in Their Natural Habitat	10
Phish with Bigger Teeth	22
Spear Phishing	27
Summary	29
Chapter 2 The Psychological Principles of Decision-Making	33
Decision-Making: Small Bits	34
Cognitive Bias	35
Physiological States	37
External Factors	38
The Bottom Line About Decision-Making	39
It Seemed Like a Good Idea at the Time	40
How Phishers Bait the Hook	41
Introducing the Amygdala	44
The Guild of Hijacked Amygdalas	45
Putting a Leash on the Amygdala	48
Wash, Rinse, Repeat	49
Summary	50

Chapter 3	Influence and Manipulation	53
	Why the Difference Matters to Us	55
	How Do I Tell the Difference?	56
	How Will We Build Rapport with Our Targets?	56
	How Will Our Targets Feel After They Discover They've Been Tested?	56
	What Is Our Intent?	57
	But the Bad Guys <i>Will</i> Use Manipulation . . .	57
	Lies, All Lies	58
	P Is for Punishment	59
	Principles of Influence	61
	Reciprocity	61
	Obligation	62
	Concession	63
	Scarcity	63
	Authority	64
	Consistency and Commitment	65
	Liking	66
	Social Proof	67
	More Fun with Influence	67
	Our Social Nature	67
	Physiological Response	68
	Psychological Response	69
	Things to Know About Manipulation	70
	Summary	71
Chapter 4	Lessons in Protection	75
	Lesson One: Critical Thinking	76
	How Can Attackers Bypass This Method?	77
	Lesson Two: Learn to Hover	77
	What If I Already Clicked the Link and I Think It's Dangerous?	80
	How Can Attackers Bypass This Method?	81
	Lesson Three: URL Deciphering	82
	How Can Attackers Bypass This Method?	85
	Lesson Four: Analyzing E-mail Headers	85
	How Can Attackers Bypass This Method?	90
	Lesson Five: Sandboxing	90
	How Can Attackers Bypass This Method?	91
	The "Wall of Sheep," or a Net of Bad Ideas	92
	Copy and Paste Your Troubles Away	92
	Sharing Is Caring	93
	My Mobile Is Secure	94
	A Good Antivirus Program Will Save You	94
	Summary	95

Chapter 5	Plan Your Phishing Trip: Creating the Enterprise Phishing Program	97
	The Basic Recipe	99
	Why?	99
	What's the Theme?	102
	The Big, Fat, Not-So-Legal Section	105
	Developing the Program	107
	Setting a Baseline	108
	Setting the Difficulty Level	109
	Writing the Phish	121
	Tracking and Statistics	122
	Reporting	125
	Phish, Educate, Repeat	127
	Summary	128
Chapter 6	The Good, the Bad, and the Ugly: Policies and More	131
	Oh, the Feels: Emotion and Policies	132
	The Definition	132
	The Bad	133
	Making It "Good"	133
	The Boss Is Exempt	133
	The Definition	134
	The Bad	134
	Making It "Good"	134
	I'll Just Patch One of the Holes	135
	The Definition	135
	The Bad	136
	Making It "Good"	136
	Phish Just Enough to Hate It	136
	The Definition	137
	The Bad	137
	Making It "Good"	138
	If You Spot a Phish, Call This Number	138
	The Definition	139
	The Bad	139
	Making It "Good"	140
	The Bad Guys Take Mondays Off	140
	The Definition	141
	The Bad	141
	Making It "Good"	141
	If You Can't See It, You Are Safe	142
	The Definition	142
	The Bad	143
	Making It "Good"	143
	The Lesson for Us All	143
	Summary	144