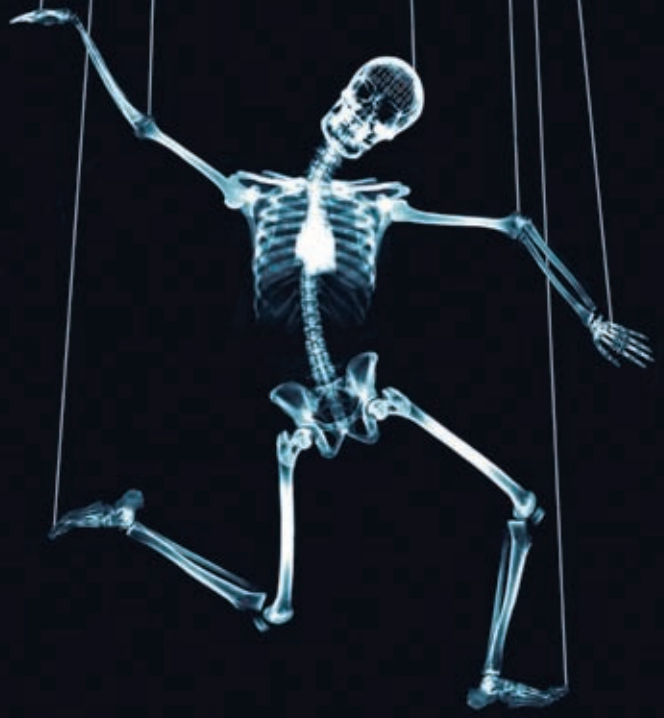
SOCIAL ENGINEERING

The Art of Human Hacking



CHRISTOPHER HADNAGY

Social Engineering

Social Engineering

The Art of Human Hacking

Christopher Hadnagy

Wiley Publishing, Inc.

Social Engineering: The Art of Human Hacking

Published by
Wiley Publishing, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

Published by Wiley Publishing, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-0-470-63953-5
ISBN: 978-1-118-02801-8 (ebk)
ISBN: 978-1-118-02971-8 (ebk)
ISBN: 978-1-118-02974-9 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Library of Congress Control Number: 2010937817

To my beautiful wife and my wonderful family; without you this would not have been possible. Mati, there are no words to describe the gratitude I feel for what you have done.

ABOUT THE AUTHOR

CHRISTOPHER HADNAGY is the lead developer of `www.social-engineer.org`, the world's first social engineering framework. In more than 14 years of security and IT activity, he has partnered with the team at `www.backtrack-linux.org` and worked on a wide variety of security projects. He also serves as trainer and lead social engineer for Offensive Security's penetration testing team.

ABOUT THE TECHNICAL EDITOR

JIM O'GORMAN is a professional penetration tester and social engineering auditor with more than 14 years of experience working for companies ranging from small ISPs to Fortune 100 corporations. Jim is co-trainer of the Offensive Security Advanced Windows Exploitation class, one of the most difficult exploit development classes available. A founding member of `www.social-engineer.org`, Jim is an authority on educating the public about social engineering threats.

CREDITS

Executive Editor
Carol Long

Project Editor
Brian Herrmann

Technical Editor
Jim O'Gorman

Production Editor
Kathleen Wisor

Copy Editor
Paula Lowell

Editorial Director
Robyn B. Siesky

Editorial Manager
Mary Beth Wakefield

Freelancer Editorial Manager
Rosemarie Graham

Marketing Manager
Ashley Zurcher

Production Manager
Tim Tate

Vice President and Executive Group Publisher
Richard Swadley

Vice President and Executive Publisher
Barry Pruett

Associate Publisher
Jim Minatel

Project Coordinator, Cover
Lynsey Stanford

Compositor
Maureen Forys,
Happenstance Type-O-Rama

Proofreader
Jen Larsen, Word One New York

Indexer
Johnna VanHoose Dinse

Cover Image
© Digital Vision/Getty Images

Cover Designer
Ryan Sneed

CONTENTS

FOREWORD

Security is a puzzle with two sides. From the inside, we look for a sense of comfort and assurance. From the outside, thieves, hackers, and vandals are looking for gaps. Most of us believe our homes are safe until one day, we find ourselves locked out. Suddenly, our perspective shifts and weaknesses are easily found.

To completely understand any kind of security it is essential to step outside of the fence, in essence locking ourselves out, and start looking for other ways in. The problem is that most of us are blinded to potential problems by our own confidence or our belief that strong locks, thick doors, a high-end security system, and a guard dog are more than enough to keep most people at bay.

I'm not most people. In the last ten years I have pulled more cons and scams than anyone in history. I've beaten casinos, faked sports events, fixed auctions, talked people out of their dearest possessions, and walked right past seemingly unbeatable levels of security.

I have made a living exposing the methods of thieves, liars, crooks, and con men on a hit TV show called *The Real Hustle*. If I'd been a real criminal I would probably be rich, famous, or dead—probably all three. I have used a lifetime of research into all forms of deception to teach the public just how vulnerable they really are.

Each week, along with Alexis Conran, I pull real scams on real people who have no idea they are being ripped off. Using hidden cameras, we show the audience at home what is possible so they can recognize the same scam.

This unusual career has resulted in a unique understanding of how criminals think. I've become a sheep in wolves' clothing. I've learned that, no matter how impossible something might seem, there's almost always a clever, unexpected way to solve the problem.

An example of this is when I offered to show how easy it would be to not only steal a woman's purse, but also to get her to tell me the PIN to her ATM or credit cards. The BBC didn't think it was possible to accomplish this. When we presented this as an item for *The Real Hustle*, the BBC commissioner wrote "will never happen" beside it and sent it back. We knew it was entirely possible because different versions of the same scam had been reported, where victims of theft were talked into revealing their PINs in several clever scams around the UK. We took elements from different scams to illustrate exactly how someone might be duped into giving someone else complete access to their bank account.

To prove our point we set up the scam at a local cafe. The cafe was on the top floor of a mall on Oxford Street in London. It was relatively quiet as I sat at an empty table wearing a business suit. I placed my briefcase on the table and waited for a suitable victim. In a few moments, just such a victim arrived with a friend and sat at the table next to mine, placing her bag on the seat beside her. As was probably her habit, she pulled the seat close and kept her hand on the bag at all times.

I needed to steal the entire bag, but, with her hand resting on it and her friend sitting opposite, she was beginning to look like bad news. But, after a few minutes, her friend left to find a restroom. The mark was alone so I gave Alex and Jess the signal.

Playing the part of a couple, Alex and Jess asked the mark if she would take a picture of them both. She was happy to do so. She removed her hand from her bag to take the camera and snap a picture of the "happy couple" and, while distracted, I casually reached over, took her bag, and calmly locked it inside my briefcase. My victim was yet to notice the empty chair as Alex and Jess left the cafe. Once out of sight, Alex headed quickly for the parking garage.

It didn't take long for her to realize her bag was gone. Instantly, she began to panic. She stood up and looked around, frantically. This was exactly what we were hoping for so, I asked her if she needed help.

She started to ask me if I had seen anything. I told her I hadn't but convinced her to sit down and think about what was in the bag. A phone. Make-up. A little cash. And her credit cards. Bingo!

I asked who she banked with and then told her that I worked for that bank. What a stroke of luck! I reassured her that everything would be fine but she would need to cancel her credit card right away. I called the "help-desk" number, which was actually Alex, and handed my phone to her. She was hooked and it was now up to Alex to reel her in.

Alex was downstairs in the van. On the dashboard, a CD player was playing office noises we had downloaded from the Internet. He kept the mark calm, strung her along, and then assured her that her card could easily be canceled but, to verify her identity, she needed to enter her PIN on the keypad of the phone she was using.

My phone and my keypad.

You can guess the rest. Once we had her PIN, I left her with her friend and headed for the door. If we were real thieves, we would have had access to her account via ATM withdrawals and chip and PIN purchases. Fortunately for her, it was just a TV show and she was so happy when I came back to return her bag and tell her it was all a fake scam. She even thanked me for giving her bag back to which I replied, "Don't thank me. I'm the one who stole it."

No matter how secure a system is, there's always a way to break through. Often, the human elements of the system are the easiest to manipulate and deceive. Creating a state of panic, using influence, manipulation tactics, or causing feelings of trust are all methods used to put a victim at ease.

The scenario outlined here is an extreme example, but it shows that, with a little creativity, seemingly impossible scams can be pulled off.

The first step in becoming more secure is simply conceding that a system is vulnerable and can be compromised. On the contrary, by believing a breach is impossible, a blindfold is placed over your eyes as you run full speed ahead. *Social Engineering* is designed to provide you with invaluable insight into the methods used to break seemingly secure systems and expose the threats that exist in the largest vulnerability, the people. This book is not a guide for hackers—they already know how to break in and are finding new ways every day. Instead, Chris Hadnagy offers those inside the fence an opportunity to take a look from the other side, the dark side, as he exposes the thinking and methods of the world's most malicious hackers, con men, and social engineers.

Remember: those who build walls think differently than those who seek to go over, under, around, or through them. As I often tell my audiences, if you think you can't be conned, you're just the person I'd like to meet.

Paul Wilson
October 2010

PREFACE AND ACKNOWLEDGMENTS

It was just a few years ago that I was sitting with my friend and mentor, Mati Aharoni, deciding to launch `www.social-engineer.org`. The idea grew and grew until it became an amazing website supported by some truly brilliant people. It didn't take long to come up with the idea to put those years of research and experience down into the pages of a book. When I had the idea, I was met with overwhelming support. That said, some specific acknowledgements are very important to how this book became what it is today.

From a very young age I was always interested in manipulating people. Not in a bad way, but I found it interesting how many times I was able to obtain things or be in situations that would be unreal. One time I was with a good friend and business associate at a tech conference at the Javits Center in New York City. A large corporation had rented FAO Schwarz for a private party. Of course, the party was by invitation only, and my friend and I were two small fish in a large pond: the party was for the CEOs and upper management of companies like HP, Microsoft, and the like. My friend said to me, "It would be really cool to get into that party."

I simply responded, "Why can't we?" At that point I thought to myself, "I know we can get in there if we just ask the right way." So I approached the women in charge of the ticket booth and the guest list and I spoke to them for a few minutes. As I was speaking to them, Linus Torvalds, the creator of the Linux kernel, walked by. I had picked up a Microsoft plush toy at one of the booths and as I joke I turned to Linus and said, "Hey, you want to autograph my Microsoft toy?"

He got a good laugh out of it and as he grabbed his tickets he said, "Nice job, young man. I will see you at the party."

I turned back to the women in charge of the ticket booth and was handed two tickets to an exclusive party inside FAO Schwartz.

It wasn't until later in life that I began to analyze stories like this, after some started calling it "the Hadnagy Effect." As funny as that sounds, I began to see that much of what occurred to me wasn't luck or fate, but rather knowing how to be where I needed to be at the right time.

That doesn't mean it didn't take hard work and a lot of help along the way. My muse in life is my wonderful wife. For almost two decades you have supported me in all my ideas and efforts and you are my best friend, my confidant, and my support pillar. Without you I would not be where I am today. In addition, you have produced

two of the most beautiful children on this planet. My son and my daughter are the motivation to keep doing all of this. If anything I do can make this place just a little more secure for them, or teach them how to keep themselves safe, it is all worthwhile.

To my son and daughter, I cannot express enough gratitude for your support, love, and motivation. My hope is that my son and my little princess will not have to deal with the malicious, bad people out in this world, but I know just how unlikely that is. May this information keep you both just a little more secure.

Paul, aka rAWjAW, thanks for all your support on the website. The thousands of hours you spent as the "wiki-master" paid off and now we have a beautiful resource for the world to use. I know I don't say it enough, but "you're fired!" Combined with the beautiful creation of Tom, aka DigIp, the website is a work of art.

Carol, my editor at Wiley, worked her butt off to get this organized and following some semblance of a timeline. She did an amazing job putting together a great team of people and making this idea a reality. Thank you.

Brian, I meant what I said. I am going to miss you when this is over. As I worked with you over the last few months I began to look forward to my editing sessions and the knowledge you would lay on me. Your honest and frank counsel and advice made this book better than it was.

My gratitude goes out to Jim, aka Elwood, as well. Without you a lot of what has happened on `social-engineer.org` as well as inside this book, heck in my life in the last couple years, would not be a reality. Thank you for keeping me humble and in check. Your constant reality checks helped me stay focused and balance the many different roles I had to play. Thank you.

Liz, about twelve years ago you told me I should write a book. I am sure you had something different in mind, but here it is. You have helped me through some pretty dark times. Thank you and I love you.

Mati, my mentor, and my *achoti*, where would I be without you? Mati, you truly are my mentor and my brother. Thank you from the bottom of my heart for having the faith in me that I could write this book and launch `www.social-engineer.org` and that both would be good. More than that, your constant counsel and direction have been translated on the pages of this book to make me more than I thought I could be.

Your support with the BackTrack team along with the support of the team at `www.offensive-security.com` have transcended all I could have expected. Thank you for helping me balance and prioritize. My *achoti*, a special thanks to you for being the voice of reason and the light at the end of some frustrating days. With all my love I thank you.

Each person I mentioned here contributed to this book in some fashion. With their help, support and love this book has become a work that I am proud to have my name on. For the rest of you who have supported the site, the channel, and our research, thank you.

As you read this book, I hope it affects you the way writing it has affected me.

Albert Einstein once said, "Information is not knowledge." That is a powerful thought. Just reading this book will not somehow implant this knowledge into your being. Apply the principles, practice what is taught in these pages, and make the information a part of your daily life. When you do, you will then see this knowledge take effect.

Christopher Hadnagy
October 2010

Social Engineering