

"Chris Hadnagy's new book *Social Engineering: The Science of Human Hacking* is a great read for any audience interested in the subject of social engineering, detailing the exact steps from OSINT to execution in order to infiltrate any target."

—Kevin Mitnick, author, speaker, and consultant

Second Edition

SOCIAL ENGINEERING

The Science of Human Hacking

CHRISTOPHER HADNAGY
FOREWORD BY STEVE "WOZ" WOZNAK

WILEY

Social Engineering

Social Engineering

The Science of Human
Hacking

Christopher Hadnagy

WILEY

Social Engineering: The Science of Human Hacking

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

Copyright © 2018 by John Wiley & Sons, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-1-119-43338-5
ISBN: 978-1-119-43373-6 (ebk)
ISBN: 978-1-119-43375-0 (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 website may provide or recommendations it may make. Further, readers should be aware that Internet websites 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: 2018943781

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. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

*My whole life that I live as a social engineer, a father, husband,
boss, friend, and more doesn't happen without my amazing wife, Areesa.*

I love you more than words can say.

*My son, Colin, watching you grow up in this world and become a
security-minded young man, as well as working with me, makes all the
work worthwhile. I love you.*

*Amaya, you have been the light of my life, my reason for smiles on dark days,
and the cause of joy in my heart. I cannot put into words how much I love you
and how truly proud I am of who you are as a person.*



ABOUT THE AUTHOR



CHRISTOPHER HADNAGY is the CEO and Chief Human Hacker of Social-Engineer, LLC as well as the lead developer and creator of the world's first social engineering framework found at www.social-engineer.org. He is the founder and creator of the Social Engineering Village (SEVillage) at DEF CON and DerbyCon, as well as the creator of the popular Social Engineering Capture The Flag (SECTF). He is a sought-after speaker and trainer and has traveled the globe to deliver at many events including RSA, Black Hat, DEF CON, and even has debriefed the Pentagon on these topics. He can be found tweeting at @humanhacker.

ABOUT THE TECHNICAL EDITOR

MICHELE FINCHER is the Information Security Awareness Lead at a specialty chemical company. She possesses more than 20 years' experience as a behavioral scientist, researcher, and information security professional. Her specialty is understanding the psychology behind secure decision-making, particularly with respect to the area of social engineering.

Michele has been a 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, SourceCon, SC Congress, Interop, and Techno Security.

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



CREDITS

PROJECT EDITOR
Charlotte Kughen

TECHNICAL EDITOR
Michele Fincher

PRODUCTION EDITOR
Athiyappan Lalith Kumar

COPY EDITOR
Kathryn Duggan

PRODUCTION MANAGER
Katie Wisor

MANAGER OF CONTENT ENABLEMENT AND
OPERATIONS
Pete Gaughan

MARKETING MANAGER
Christie Hilbrich

EXECUTIVE EDITOR
Jim Minatel

PROJECT COORDINATOR, COVER
Brent Savage

PROOFREADER
Nancy Bell

INDEXER
Johnna VanHoose

COVER DESIGNER
Wiley

COVER IMAGE
Background © Floriana /iStockphoto;
Author Photo © Amaya Hadnagy
Photography, 2018



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.”

Those are the opening words of *Social Engineering: The Art of Human Hacking*. As I sit here and read them now, it’s almost like a dream; the hazy memory makes me feel like I will wake up any minute. I reflect on the journey that has taken me through the past decade, and especially the last eight years, and it has all come to life in this book.

Over the last eight years I have worked with people like Dr. Paul Ekman, Robin Dreeke, Neil Fallon, and others. I have had the honor of interviewing people like Dr. Robert Cialdini, Dr. Amy Cuddy, Dov Baron, Dr. Ellen Langer, Dr. Dan Airely, and so many others. I have had the privilege of giving a speech with Apollo Robins and meeting Will Smith. I have been flown to the UK to train members of MI-5 and MI-6. And I have been invited to the Pentagon to debrief 35 generals, heads of state, and other officials on social engineering.

The last eight years have been an amazing roller-coaster ride. But like any project, nothing is made on an island of one. These experiences, my life, and the people I have had the honor of getting to know and work with are because of so many people that have helped me along the way.

My wife, Areesa, is one of the most patient and beautiful women I have ever met. Although she does not live in this world that I exist in, she truly supports me, loves me, and gives me a happy life that is full of laughs, adventure, and everlasting memories.

When my son, Colin, was little, he was going to be a doctor, then a writer, then a volunteer. Funny enough, he tried his hand at caregiving and writing, and he still volunteers. His positive attitude and kind spirit is an example to me.

I remember swearing that I would never let my daughter, Amaya, in this world of social engineering; I would keep her safe. She has taught me that keeping her safe means teaching her, including her, and making her a part of my life. She has given me so much more than I have given her.

Although Dr. Ekman wasn’t directly related to this book, his kindness, motivation and generosity are an inspiration to me. Thank you.

I want to thank and acknowledge others who have been a continuing part of my journey:

- » Ping Look is an endless and selfless supply of advice and help.
- » Dave Kennedy's friendship and support mean so much.
- » The Innocent Lives Foundation has become an integral part of this process, so I want to thank the following people from that organization:
 - » I never would have thought I could say that Neil Fallon and I would become friends (pinch me). But now he helps guide me, direct me, and encourage me. He truly reminds me to be human.
 - » Tim Maloney's support and protection have been such a big part of putting together the ILF. His friendship, faith, and support in this process is something I cannot sufficiently thank him for.
 - » Casie Hall's excitement and enthusiasm to be a part of the solution is contagious.
 - » I thank AJ Cook for her support with ILF and being so easy to work with in our efforts to save kids. Her dedication is exemplary.
 - » Aisha Tyler's (ha! Even typing that name seems a little surreal.) work ethic, kindness, and ability to focus is a model that we should all emulate.
- » My team at Social-Engineer, LLC has been great. Colin, Mike, Cat, Ryan, Amanda, Kaz, Jenn, and Karen—each has helped me improve and supported me through this process.
- » I swear my editor Charlotte should be my ghost writer for a book. She captured thoughts and helped me sound more intelligent. (That is a hard job!)
- » And the readers and fans of the Social-Engineer *Podcast*, SEVillages at the conferences, my other books, and SE-Events—you have held me to a high standard, haven't been afraid to call me out on stupid mistakes, and have made me constantly strive to do better. Thank you!



CONTENTS AT A GLANCE

<i>Acknowledgments</i>	<i>xi</i>
<i>Foreword</i>	<i>xix</i>
<i>Preface</i>	<i>xxi</i>
I A Look into the New World of Professional Social Engineering	1
2 Do You See What I See?	17
3 Profiling People Through Communication	63
4 Becoming Anyone You Want to Be	83
5 I Know How to Make You Like Me	101
6 Under the Influence	123
7 Building Your Artwork	157
8 I Can See What You Didn't Say	183
9 Hacking the Humans	223
10 Do You Have a M.A.P.P.?	257
11 Now What?	277
<i>Index</i>	287



CONTENTS

<i>Acknowledgments</i>	<i>xi</i>
<i>Foreword</i>	<i>xix</i>
<i>Preface</i>	<i>xxi</i>
1 A Look into the New World of Professional Social Engineering	1
What Has Changed?	2
Why Should You Read This Book?	4
An Overview of Social Engineering	6
The SE Pyramid	11
What's in This Book?	14
Summary	15
2 Do You See What I See?	17
A Real-World Example of Collecting OSINT	17
Nontechnical OSINT	22
Tools of the Trade	59
Summary	61
3 Profiling People Through Communication	63
The Approach	66
Enter the DISC	68
Summary	80
4 Becoming Anyone You Want to Be	83
The Principles of Pretexting	84
Summary	98
5 I Know How to Make You Like Me	101
The Tribe Mentality	103
Building Rapport as a Social Engineer	105
The Rapport Machine	120
Summary	121
6 Under the Influence	123
Principle One: Reciprocity	125
Principle Two: Obligation	128

Principle Three: Concession.	131
Principle Four: Scarcity.	134
Principle Five: Authority.	137
Principle Six: Consistency and Commitment.	142
Principle Seven: Liking.	146
Principle Eight: Social Proof.	148
Influence vs. Manipulation.	151
Summary.	156
7 Building Your Artwork.	157
The Dynamic Rules of Framing.	159
Elicitation.	168
Summary.	182
8 I Can See What You Didn't Say	183
Nonverbals Are Essential.	184
All Your Baselines Belong to Us.	187
Understand the Basics of Nonverbals.	196
Comfort vs. Discomfort.	198
Summary.	220
9 Hacking the Humans.	223
An Equal Opportunity Victimizer.	224
The Principles of the Pentest.	225
Phishing.	229
Vishing.	233
SMiShing.	240
Impersonation.	241
Reporting.	246
Top Questions for the SE Pentester.	250
Summary.	254
10 Do You Have a M.A.P.P.?	257
Step 1: Learn to Identify Social Engineering Attacks.	259
Step 2: Develop Actionable and Realistic Policies.	261
Step 3: Perform Regular Real-World Checkups.	264
Step 4: Implement Applicable Security-Awareness Programs.	266
Tie It All Together.	267
Gotta Keep 'Em Updated.	268

Let the Mistakes of Your Peers Be Your Teacher	270
Create a Security Awareness Culture	271
Summary	274
II Now What?	277
Soft Skills for Becoming an Social Engineer	277
Technical Skills	280
Education	281
Job Prospects	283
The Future of Social Engineering	284
<i>Index</i>	287



FOREWORD

When I started Apple Computers in 1976 with Steve Jobs, I did not imagine where that invention would take the world. I wanted to do something that was unheard of: create a personal computer. One that any person could use, enjoy, and benefit from. Jump forward only a short 40 or so years and that vision is a reality.

With billions of personal computers around the globe, smartphones, smart devices, and technology being embedded into every aspect of our lives, it is important to take a step back and look at how we maintain safety and security while still innovating and growing and working with the next generation.

I love getting to work with youth today, inspiring them to innovate and grow. I love seeing the ideas flow from them as they figure out new and creative ways to use technology. And I truly love being able to see how this technology can enhance people's lives.

With that said, we need to take a serious look at how we secure this future. In 2004 when I gave the keynote speech at HOPE Conference, I said that a lot of hacking is playing with other people and getting them to do strange things. My friend, Kevin Mitnick, has mastered this over the years in one area of security called social engineering.

Chris's book captures the very essence of social engineering, defining and shaping it for all of us to understand. He has rewritten the book on it again, defining the core principles of how we as humans make decisions and how those very same processes can be manipulated.

Hacking has been around for a while, and human hacking has been around for as long as humans have. This book can prepare you, protect you, and educate you how to recognize, defend, and mitigate the risks that come from social engineering.

—Steve “Woz” Wozniak



PREFACE

Social engineering—I can remember when searching for that term led you to videos on getting free burgers or dates with girls. Now it seems like it's almost a household term. Just the other day I heard a friend of the family, who's not in this industry at all, talking about an email scam. She said, "Well, that's just a great example of social engineering!"

It threw me for a loop for a second, but here we are, eight years after my decision to start a company solely focused on social engineering, and now it's a full-blown industry and household term.

If you were to just start reading this book it would be easy to mistake my intentions. You might think I am fully okay with arming the bad guys or preparing them for nefarious acts. That cannot be further from the truth.

When I wrote my first book, there were many folks who, during interviews, got very upset with me and said I was arming the malicious social engineers. I felt the same then as I do now: you cannot really defend against social engineering until you know all sides of its use. Social engineering is a tool like a hammer, shovel, knife, or even a gun. Each has a purpose that can be used to build, save, feed, or survive; each tool also can be used to maim, kill, destroy, and ruin. For you to understand how to use social engineering to build, feed, survive, or save, you need to understand both uses. This is especially true if your goal is to defend. Defending yourself and others from malicious uses of social engineering requires that you step over into the dark side of it to get a clear picture of how it is used.

I was recently chatting with AJ Cook about her work on *Criminal Minds*, and she mentioned that she often has to meet with real federal agents who work serial-killer cases to prepare herself for playing the role of JJ on the show. The same idea applies directly to this book.

As you read this book, do it with an open mind. I tried my hardest to put the knowledge, experience, and practical wisdom I have learned over the last decade onto these pages. There will always be some mistakes or something you don't like or something you might feel was not 100% clear. Let's discuss it; reach out to me and let's talk. You can find me on Twitter: @humanhacker. Or you can email me from one of the websites: www.social-engineer.org or www.social-engineer.com.

When I teach my five-day courses, I always ask the students to not treat me like some infallible instructor. If they have knowledge, thoughts, or even feelings that contradict something I say, I want to discuss it with them. I love learning and expanding my understanding on these topics. I extend the same request to you.

Finally, I want to thank you. Thank you for spending some of your valuable time with me in the pages of this book. Thank you for helping me improve over the years. Thank you for all your feedback, ideas, critiques, and advice.

I truly hope you enjoy this book.

—Christopher Hadnagy



1

A Look into the New World of Professional Social Engineering

*I suppose your security is your success, and your key
to success is your fine palate.*

—GORDON RAMSAY

I still vividly remember sitting in front of my computer screen as I started to pen the first paragraph of *Social Engineering: The Art of Human Hacking*. It was way back in 2010. I am half tempted to tell you we had to write books uphill both ways back then, using a typewriter, but I don't want to get too dramatic.

In that time, when you searched the Internet for “social engineering,” you got a few pages on social engineering legend Kevin Mitnick and some videos on how to pick up girls or get free burgers from McDonald's. Fast-forward eight years, and now the term *social engineering* is used almost as a household term. In the past three or four years, I have seen social engineering in security, government, education, psychology, military, and every other application you can imagine.

This transition begs the question of why. One colleague told me, “It's your fault, Chris.” I think he meant it as an insult, although I felt a tinge of pride at that statement. However, I don't feel that I'm solely responsible for the near ubiquity of the term *social engineering* (SE). I believe that we see it being used by everyone and their brother now because it is not only the easiest attack vector—as it was seven years ago—but because it's now also meriting the largest payloads for attackers.

The cost to set up an SE attack is low. The risk is even lower. And the potential payout is *huge*. My team has been collecting stories in the news about SE attacks and scouring the web for statistics. I feel comfortable stating that in 2017, more than 80% of all breaches had a social engineering element to them.

The IBM “2017 Cost of Data Breach Study” states that the average cost of a breach was 3.62 million US\$. When the potential for a payout is that large, it's certainly not hard to see why an attacker would want to use social engineering.

PRO TIP As of 2017, the IBM “Cost of Data Breach Study” had been produced for 12 years. You can find it at <https://www-03.ibm.com/security/data-breach/>. Or you can simply enter “Cost of Data Breach Study” in any search engine to find and download a full and current report.

I also remember one of my first interviews after my *Social Engineering: The Art of Human Hacking* book was published in 2010, when I was asked, “Aren’t you worried that you are arming the bad guys?” But to me, SE is like any new type of warfare.

To help me more clearly explain this, I think about the story of Bruce Lee arriving in America in the 1960s. Racial prejudice was high, and he was doing something that no one else was doing: teaching Jeet Kune Do (an ancient Chinese martial art) to people of any race, color, or nation. He was battling in the university he went to with fellow students who felt they knew a lot about fighting. But he laid out flat opponent after opponent. Eventually, some of those opponents even became Bruce’s friends or students.

What is the lesson? People had to adapt to a new type of fighting, or they would just constantly get beat. Was there a risk that a student of Bruce Lee could use his newfound skills to hurt other people and do evil? Yes, but Bruce felt it was necessary to educate people, so they could remain protected.

So, my answer to the question, “Aren’t you worried that you are arming the bad guys?” is the same as it was eight years ago: I cannot control how you use this information. You can read this book and go out and attack people and steal their money. Or you can read this book and learn to be a defender for what is right. The choice is yours, but the good guys need someone to help teach them.

Learning to defend against this new style of attack takes more than just learning how to take a beating. Like Jeet Kune Do, it requires a balance of learning how to attack, learning how to defend, and knowing when to do each. As you learn how to be a social engineer, you need to be able to think like the bad guys while remembering you are the good guy. To steal another analogy, you need to be strong with the force but not walk over to the dark side.

Now you might be asking, “If not much has changed in your response, then why do we need a second edition of your book?” Well, let me tell you.

What Has Changed?

This is a fundamental question when it comes to social engineering. On the surface, the answer is, “Not much.” You can go back a long way and find anecdotes about social engineering. For example, one of the first documented stories I can

find is in the Bible, in the book of Genesis, and it reportedly happened around 1800 BCE. Jacob wanted the blessing that was to be given to his older brother Esau. Knowing his father, Isaac, had failing eyesight and relied on other senses to know who he was speaking to, Jacob dressed in Esau's clothing and prepared food like Esau would have prepared. Here's the best part: Esau was known to be extraordinarily hairy, but Jacob wasn't, so he fastened the skins of two young goats to his arms and the back of his neck. When Isaac reached out to touch Jacob, Isaac relied on his senses of smell, touch, and taste to tell him that he was with Esau rather than Jacob. According to the account in Genesis, Jacob's social engineering attack worked!

From the dawn of recorded history, we see one account after another of humans tricking, duping, conning, or scamming one another. On the surface, there might not be much that's brand new when it comes to social engineering, but that doesn't mean that nothing ever changes.

One example is vishing. I honestly remember using the word *vishing* for the first time. People looked at me like I was speaking Klingon. Seriously, I might as well have said *laH yIllo' ghogh Habll' Hlv* (you Trekkies will appreciate that). As of 2015, though, *vishing* was added to *Oxford English Dictionary*.

PRO TIP Klingon is a fictional language, but there is an actual institute (www.kli.org) devoted to teaching, translating, and speaking Klingon. You also can find numerous translators online. To date, I have not heard a story of anyone “social engineering” any other person in Klingon.

Why is it important that *vishing* is now in the dictionary? It goes to show how much social engineering vectors have affected the world. Words that once appeared to be part of a “made up” language now are part of our everyday vocabulary.

It's not just the vocabulary that's become commonplace. Now there are services that specialize in helping the bad guys be better at being bad. For example, while I was doing work for a client, I stumbled upon a service that specialized in proofreading and spellchecking malicious phishing emails. That company provided 24/7 English-speaking support. Blend stuff like that with our BYOD (bring your own device) culture and the fact that most mobile devices are mini supercomputers, and then stir in some new-world social media addiction. What you're left with is a recipe for a whole new attack landscape—social engineer style.

In addition to the landscape changing, I have changed. When I wrote the first edition of this book, the title was *Social Engineering: The Art of Human Hacking*. I chose that name because I felt that what I was describing in that book was much

like art. Art is subjective; it means different things to different people. It can be applied differently and can be used, viewed, liked, and hated for completely different reasons.

This second edition is called *Social Engineering: The Science of Human Hacking*. The Merriam-Webster dictionary gives one definition of *science* as, “The state of knowing: knowledge as distinguished from ignorance or misunderstanding.” Eight years ago, much of what I did was new to the security realm, and I was learning as I went. Now I am in a “state of knowing” due to the additional years of experience on my resume.

That experience, I hope, will make this book much more meaningful to you, whether you’re a security expert who’s looking to understand social engineering, an enthusiast who’s looking to broaden your horizons, or an educator who’s looking to understand problems to include in your lessons. No matter why you are reading this book, my hope is that by thinking of these topics on a more scientific level, I can relay this information in a much more useful and complete manner.

Why Should You Read This Book?

I feel that this first chapter needs to follow the same pattern I took in my first book, so I want to spend a little time discussing why I feel that anyone should read this book. Yes, I realize I might be biased here, but humor me for a moment.

Are you a human? I am going to guess that if you are sitting in front of this book, reading this paragraph, you are either some advanced form of AI or you’re human. I’ll even go so far as to say that 99.9999999% of this book’s audience is human. Social engineering takes the way humans are wired to make decisions and exploits the vulnerabilities in those processes.

The goal of the social engineer is to get you to make a decision without thinking. The more you think, the more likely you are to realize you are being manipulated, which of course is bad for the attacker. In episodes 7 and 70 of *The Social-Engineering Podcast*, I had the privilege of interviewing Dr. Ellen Langer. She spoke to me about something she called alpha and beta mode.

Alpha mode is when one’s brain is running at 8 to 13 cps (cycles per second). It is generally characterized by “daydreaming,” or what Dr. Langer called “relaxed, focused concentration.”

Beta mode is when one’s brain runs anywhere from 14 to 100 cps. This is when our brains are alert, observant, and aware of the things going on around us.

SEPODCAST REFERENCE

Following are the URLs where you can find the episodes of *The Social-Engineer Podcast* during which I interviewed Dr. Langer:

- » Episode 7 includes my first interview with Dr. Langer, in which we discuss her research and her books: www.social-engineer.org/podcast/episode-007-using-persuasion-on-the-mindless-masses/
- » Episode 70 takes place five years after my first interview with Dr. Langer. She came back on the show to tell us what she had learned over the years, what had changed, and how we have advanced: www.social-engineer.org/podcast/ep-070-thinking-without-a-box/

Which state benefits a social engineer more? Obviously, the answer is alpha mode because thinking and awareness are lessened. This is not just the case when it comes to malicious intentions. Manipulation and some types of influence are geared toward getting you to act without thought.

For example, you most likely have seen a commercial like this: A famous female musical artist comes on the screen, and a very sad song is playing in the background. The image changes to scenes of kittens and puppies that have been beaten, hurt, and underfed. The animals are filthy and dirty, and they look like they're at death's door. Now the artist comes back on screen; she's surrounded by healthy animals, and she's showering them with love. What's the message? For only a few dollars, those malnourished, near-dead animals can be transformed into loving pets—healthy, happy, and all yours. The images in the commercial are like what you see in Figure 1-1.

Are the producers of the commercial manipulating you for selfish means? Not entirely. What they have learned is that if they trigger your emotions, there is a greater likelihood that you will donate or take the desired action. The success rate is much greater than if they just appeal to knowledge or logic. The more emotions are triggered, the less you think rationally. The less you think rationally, the quicker you will decide based solely on the emotions triggered.

So, back to my earlier point: If you are human, then this book can help you understand what types of attacks exist. You can learn how the bad guys are using your humanity against you, and you can learn how to defend against these attacks to protect your loved ones from being victims.

Let me start by giving you an overview of social engineering.



Figure 1-1 How does this make you feel?

IMAGE CREDIT TO AMAZON COMMUNITY ANIMAL RESCUE, WWW.FLICKR.COM/PHOTOS/AMAZON-CARES/2345707195

An Overview of Social Engineering

Whenever I discuss social engineering, I usually start with a definition that I have been using for the last 10 years. I've modified it only slightly over time.

But before I give you that definition of social engineering, I need to state one very important point: social engineering (SE) is not politically correct. This truth can be hard for many people to swallow, but it's real: SE takes advantage of the fact that gender bias, racial bias, age bias, and status bias (as well as combinations of those biases) exist.

For instance, imagine you have to infiltrate a client's building. To do so, you need to develop a pretext that allows you to gain entry easily. Your team is made