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 yIlo' ghogh HablI' HIv* (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-Engineer 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-with-out-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.

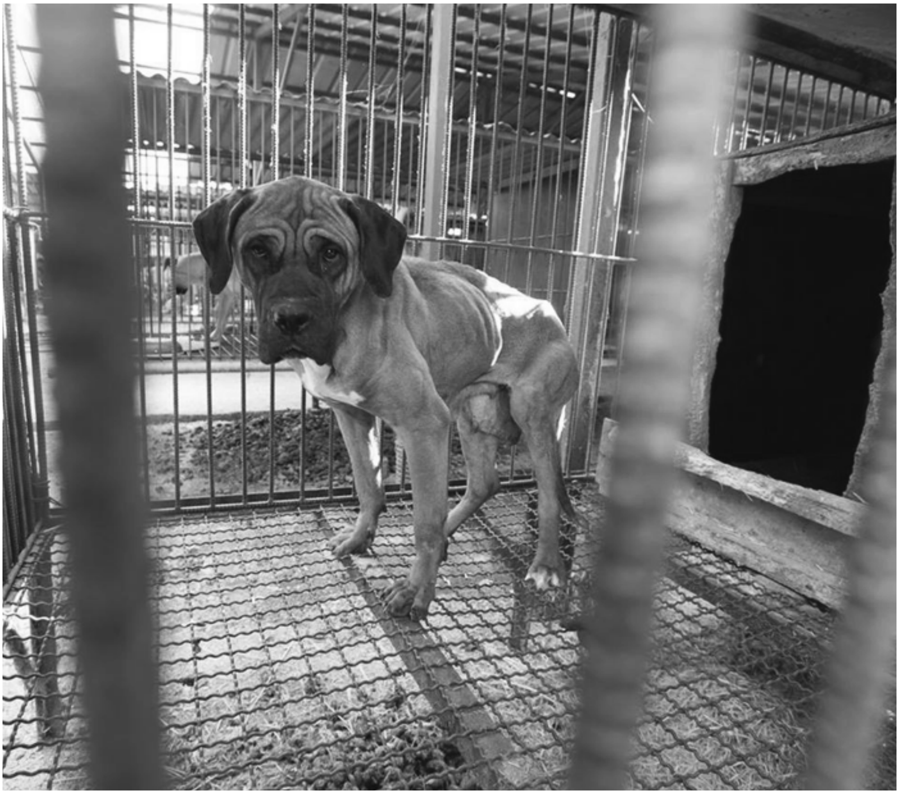


Figure 1-1 How does this make you feel?

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 up of a few different types of folks. If you determine that the best pretext for the job is janitorial staff, which of the following team members would be the best fit?

- 40-year-old white, blonde male
- 43-year-old Asian female
- 27-year-old Latino female

If you determine that your best pretext is intercompany kitchen work, which of the following team members would be the best fit?

- 40-year-old white, blonde male
- 43-year-old Asian female
- 27-year-old Latino female

The fact is, a skilled social engineer in any of the categories can make a go of it and succeed. But which one will lead to the least amount of thinking? Remember, thinking is the enemy of the social engineer.

With that in mind, let's get back to how I define social engineering:

> *Social engineering is* any *act that influences a person to take an action that may or may not be in his or her best interests.*

Why is my definition so broad and general? It's because I believe that social engineering isn't *always* negative.

There was a time when you could say, "I'm a hacker," without causing normal people to run for cover, unplugging every electronic device in their path. Being a hacker used to mean someone who *needed* to know how something worked. A hacker wasn't satisfied with just base knowledge; that person wanted to dig deep into the inner workings of anything. Then, once it was understood, a hacker would see if there was any way to bypass, enhance, exploit, or alter its original purpose.

When I started my first book, I wanted to try to make sure that I could define social engineering in a way that didn't always imply that it involved a terrible scam artist or conman or grifter. The very same principles that I see the bad guys use can be applied for good purposes, and I want people to know that.

I often use this illustration: If you came up to me and said, "Hey, Chris. I want to have a princess tea party with you—you sit here, and I will paint your nails while you wear a pink scarf and we talk about Disney princesses," I would not only laugh at you, but I would slowly back away while looking for the nearest exit. Yet, I must admit that there may be some pictures floating around of this type of event.

How so? My daughter asked me to have a princess tea party with her. Now, before you say, “Hey, that’s an unfair comparison—you love her!” I’ll admit, that had a lot to do with my decision to join her, but think about the psychological principles that were at play for me to make that decision. To agree to a decision that I would literally refuse in a nanosecond had anyone else asked me, I had to bypass my normal decision-making in order to say “Yes.”

USELESS FACT

Considering a nanosecond is one billionth of a second, and the average person speaks at a rate of 145 words per minute, I literally could not “say” the word *no* in a nanosecond. On the other hand, light, which travels at 186,000 miles per second, can travel 1 foot in a nanosecond.

When you understand how decisions are made, you can start to understand how a malicious attacker can use emotional triggers, psychological principles, and application of the art and science of social engineering to get you to “take an action that is not in your best interests.”

Dr. Paul Zak appeared in *The Social-Engineer Podcast* episode 44. He wrote the book *The Moral Molecule* (Dutton, 2012). In that book and in our podcast, Dr. Zak spoke about his research into a hormone called oxytocin. His research helped us to see how closely it is linked with trust because he made one very important comment about how oxytocin is released into our blood when we feel that someone trusts us. Please understand this very vital point: your brain releases oxytocin not just when you trust someone, but also when *you feel* that someone else has given you trust. According to Dr. Zak’s research, this phenomenon has been demonstrated in person, over the phone, over the Internet, and even when you can’t see the person who is doing the “trusting.”

SEPODCAST REFERENCE

Episode 44 of *The Social-Engineer Podcast* includes the fascinating conversation with Dr. Zak about his life’s work. You can find it at `www.social-engineer.org/podcast/ep-044-do-you-trust-me/`

Another chemical that our brains produce is dopamine. Dopamine is a neurotransmitter produced by the brain and released during moments of pleasure, happiness, and stimulation. Blend oxytocin with dopamine, and you have a social engineering brain cocktail that can open any door you want.

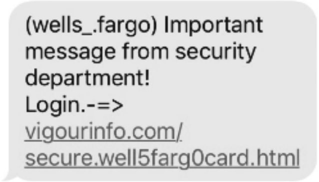
Dopamine and oxytocin are released in our brains during intimate moments, but they also can be released during normal conversations. Those conversations are at the core of social engineering.

I believe we use these same principles daily—many times, unknowingly—with our spouses, bosses, fellow workers, clergy, therapists, service people, and everyone else we meet. Consequently, understanding social engineering and how to communicate with your fellow human is imperative for all people today.

In a world where technology has made it easy to communicate using emoticons or fewer than 280 characters, it has become more difficult to learn how to use conversational skills, let alone see when those skills are being used against us. Taking it one step further, social media has created a society where telling everyone everything about ourselves is acceptable, and even promoted.

When I talk about social engineering from a malicious perspective, I break it down into the following four vectors:

» **SMiShing:** Yes, this is a real thing, and it stands for SMS phishing, or phishing through text messages. When Wells Fargo was breached in 2016, I received the SMiShing attack shown in Figure 1-2.



(wells_.fargo) Important
message from security
department!
Login.-=>
vigourinfo.com/
secure.well5farg0card.html

Figure 1-2 This SMiShing attack trapped a lot of people.

What's crazy is that I don't even use Wells Fargo, but I still received this attack. (And no, I am not telling you what bank I use—nice try.)

With a simple click, these attacks were geared either to steal credentials or to load malware on the mobile device and sometimes both.

- **Vishing:** As I already mentioned, this is voice phishing. This has increased as a vector drastically since 2016. It is easy, cheap, and very profitable for the attacker. It is also nearly impossible to locate and then catch the attacker with spoofed numbers calling from outside the country.
- **Phishing:** The most talked about topic in the world of social engineering is phishing. In fact, the technical editor on this book, Michele, and I wrote about it in a book titled *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails* (Wiley, 2016). (Yes, I did just shamelessly plug one of my other books.) Phishing has been used to shut down manufacturing plants, hack the DNC, breach the White House as well as dozens of major corporations, and steal countless millions of dollars in different scams. Phishing is by far the most dangerous of the four main vectors.
- **Impersonation:** I know, we should put some form of 'ishing on this one too, but the best I could do is list it last because it's different. However, its placement in this list by no means indicates that we don't have to worry about it as much as the others. In the past 12 months, we have collected hundreds of stories of people impersonating police, federal agents, and fellow employees committing some truly horrific crimes. In April 2017, there was a story of a man who was impersonating the police and was caught. He was dealing in child pornography and using his impersonation to profit.

MORE INFO

At the time of writing, that sickening story can be found on this site: `www.sun-sentinel.com/local/broward/pembroke-pines/fl-sb-pines-man-child-porn-20170418-story.html`.

Every social engineering attack you read about can be broken down into one of these four categories. More recently, we are seeing what we call the combo attack, where malicious social engineers are using a combination of these in one attack to achieve their means.

When I analyze these attacks, I start to see patterns that not only identify what kinds of tools and processes are used, but that can also help a security expert define more clearly how to perform these attacks and then use the results to educate and protect. I called this the *SE pyramid*.

The SE Pyramid

Let me just jump straight into the pyramid before I define why I came up with this and what each section means. The pyramid is illustrated in Figure 1-3.

As you can see, the pyramid is broken into a few sections, and approaches social engineering from the perspective of an SE professional—that is, not one using SE for nefarious purposes but to help clients and customers.

I'm going to define each section of the pyramid, and I'll get into the layers in more detail later in this book.

OSINT

OSINT, or Open Source Intelligence, is the life blood of every social engineering engagement. It is also the piece that should have the most time spent on it. Due to that, it occupies the first and largest piece of the pyramid. One piece of this part of the pyramid is rarely addressed: documentation. How will you document, save, and catalog all the information you find? I discuss this key factor a bit more in the next chapter.

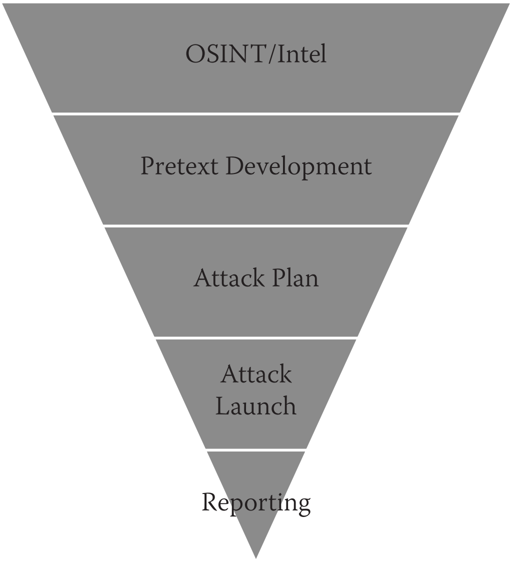


Figure 1-3 The SE Pyramid

Pretext Development

Based on all the findings from the OSINT period, the next logical step is to start to develop your pretexts. This is a crucial piece that's best done with OSINT in mind. During this phase, you see what changes or additions need to be made to ensure success. This is also when it becomes clear what props and/or tools are needed.

Attack Plan

Having a pretext in hand does not mean you are ready. The next stage is to plan out the three W's: what, when, and who.

- What is the plan? What is it we are going for and trying to achieve? What does the client want? These questions will help develop the next piece.
- When is the best time to launch the attack?
- Who needs to be available at a moment's notice for support or assistance?

Attack Launch

Now comes the fun part: launching the attacks. With the preparation done on the attack plan, you are prepared to go full steam ahead. It is important to be prepared but not to be so scripted that you can't be dynamic. I am all for having a written plan, and I think it can save you a ton of headaches down the road. The caution I have is that if you script out every word or action you feel needs to be taken, you can run into problems when the unexpected happens. Your brain realizes there is nothing on the script to help, and you begin to stutter, get nervous, and show signs of fear. This can really ruin your ability to succeed. Instead of scripting, I suggest using an outline, which gives you a path to follow but allows for artistic freedom.

Reporting

Wait—don't skip over this section. Come back and read it. Yes, reporting is not fun, but you can think of it this way: Your customer just paid you *x* dollars to perform some services, and most likely, you were pretty darn successful in those attacks.

But the customer didn't pay you just because they wanted to look cool. They paid you to understand what they can do to fix the problem. For that reason, the reporting phase is at the very tip of the pyramid, is the very pinnacle that the rest of the pyramid rests on.

The five phases of this pyramid, if followed, will lead to your success not only as a social engineer, but as a professional who is offering social engineering services to your customers. The fact is that, with the exception of reporting, these steps are followed by the malicious social engineers in the world.

In 2015, Dark Reading reported on an attack that involved this very pyramid. (You can read the article "CareerBuilder Attack Sends Malware-Rigged Resumes to Businesses" at `www.darkreading.com/vulnerabilities---threats/careerbuilder-attack-sends-malware-rigged-resumes-to-businesses/d/d-id/1320236?`.)

1. The attackers investigated attacking a few targets and while working through their OSINT phase, they found out that their targets used a popular site called CareerBuilder.
2. After completing the OSINT phase, the attackers started on pretext development. This led them to plan a pretext as a job seeker, who was looking to get hired at whatever role their targets were offering. They realized the tools they needed would be some maliciously encoded files and some realistic-looking resumes.
3. They started to plan the attacks, by answering some of those W questions.
4. They then launched the attacks by uploading their malicious documents *not* to the target but to the CareerBuilder website. The companies that posted the jobs would be notified by email that there was a new applicant, and that email would contain the attacker's uploaded attachments.
5. They did not follow through with any actionable reporting phase, but there is some actionable reporting on this attack thanks to some researchers at Proofpoint.

This attack was successful because the target would get an email with an attachment from a trusted and reputable source (CareerBuilder). Consequently, the target would open the attachment without thinking. And that is exactly the goal of the malicious social engineer: to get the target to take an action that is *not* in their best interest without thinking through the potential dangers involved.

What's in This Book?

When I started to plan this book, I wanted to make sure that I kept to the outline of the first edition of *Social Engineering* so those who benefited from its pages would benefit from this book too. At the same time, I wanted to change the book and update it to cover some of new attacks and things I never discussed in the previous book.

I wanted to make sure I took all the advice from fans, researchers, readers, and reviewers in the hopes that I could make this book much better than the first. Let me outline how this book is formatted so you know what to look forward to.

Following the path of the pyramid, Chapter 2, "Do You See What I See?," discusses OSINT and covers some of the timeless techniques used. I refrain from delving into actual tools too much, although I mention a few that have stayed in my tool chest for the last decade.

In Chapter 3, "Profiling People Through Communication," I examine a topic that I barely touched in the first edition. I delve deep into advanced communication modeling and profiling tools.

Chapter 4, Becoming Anyone You Want," is where I start to dive into pretexting. This is a topic that not many people talk about outside of social engineering. I cover tips, tricks, and many of the experiences (both successes and failures) that I have had over the years.

In Chapter 5, "I Know How to Make You Like Me," I compile information from the many podcasts, newsletters, and conversations with some of the world's greats—like Robin Dreeke—and apply the principles of rapport-building to social engineering. Robin Dreeke is the head of the FBI's Behavioral Analysis Unit and a good friend of mine. He is a master at building rapport and trust and has defined the steps to do both.

Chapter 6, "Under the Influence," applies the work of one of the leaders in the study of influence, Robert Cialdini, to the field of social engineering. The chapter takes the principles that he developed over his years of research and shows how they can and are being used by social engineers.

Chapter 7, "I Didn't Even Ask You for That," defines framing and elicitation and outlines how anyone can master both.

In Chapter 8, "I Can See What You Didn't Say," we return to one of my favorite topics: nonverbals. I dig super-deep into this topic in my book *Unmasking the Social Engineer: The Human Element of Security* (Wiley, 2014), but this chapter is a beginner's guide to get you started in the world of nonverbals.

In Chapter 9, "Hacking the Humans," I take the previous eight chapters and apply them to five different types of social engineering attacks. This chapter shows how important it is for you, as a professional social engineer, to apply the principles of this book.

As we near the end, Chapter 10, "Do You Have a M.A.P.P.?," covers prevention and mitigation. In a book about professional social engineering, it is fitting to have this chapter cover the four steps in learning to fight all social engineering attacks.

Then, like all good things, this book must conclude. So, Chapter 11, "Now What?," brings this book to an end.

Here are a few promises I have for you:

- I promise to not quote Wikipedia as a valued source, especially when mentioning research. (I learned from my mistakes.)
- I promise to tell you many stories from my experiences during the last seven or more years. Sometimes, I tell one story from many angles to help really get a few points solidly fixed for you. But I try and mix up those stories so you don't get bored.
- When I am using the research or work of some of the greatest minds in their fields, I will make sure you have references to their work, so you can look deeper into any topic you may want.
- Just as I did with the first book I ever wrote, I openly welcome all contacts, comments, suggestions, and criticism.

All I ask in return is that you read this book in the light it was intended. If you are a novice, this book can help you learn what is needed to be a professional social engineer. If you are experienced, then I hope my sharing a few stories, tips, and tricks will give you some new tools for your arsenal. If you are an enthusiast, then I want you to read this with the same excitement as I had while writing it. And if you are a skeptic, then read this with the thought that I am not claiming to be the one and only messiah of SE. I'm just a passionate social engineer with many years of experience that I want to share to try and make this world a little bit safer.

Summary

No book that I write would be complete without a cooking analogy, so here it goes. Like any great meal, there is a lot of planning, a great recipe that calls for fresh ingredients, and then artistic and scientific execution. Social engineering, although simplistic in nature, is not a recipe for a novice. It involves understanding how humans make decisions, what motivates them, and how to control your own emotions while exploiting those same processes in others.

The topic of this book is still as relevant today as it was eight years ago—maybe even more so now. In the past eight years, I have watched many people rise as professional social engineers. I have seen many malicious social engineers rise and fall too.

With the nature of attacks leaning so heavily toward the human element, it is imperative that all security professionals understand social engineering. But there is so much more to this topic. I remember when I started working as a chef (in a former life a long time ago), my mentor would take ingredients and tell me to taste little bits of each. But why?

He told me that I couldn't possibly know what it means "to taste" if I didn't really understand what each item tasted like. If I know that the recipe calls for some horseradish, and I want it to be a little spicier, then I understand that I could add a little bit more. Understanding that a certain ingredient also has a salty quality might make me adjust my salt for the recipe, so items are not overly seasoned. You get the point.

Even if you are not in the security industry, it is important to understand how each of these ingredients "tastes" so you can be protected. What does it mean to build rapport with someone, and how can that be used to get you to part with your money? (This is covered in Chapter 5.) How does influence, when sprinkled in an elicitation conversation, make someone give up a password over the phone? (This is covered in Chapters 6 and 7.)

Each of these ingredients can help you to learn the "taste." When you know them, you can recognize when someone tries them out on you, and you are more secure. You can sense something isn't right, and you can take defensive actions.

Have you ever watched any cooking competition with Gordon Ramsay? When he tastes a dish that he hates, he identifies the specific problem: "This dish has way too much pepper and they used too much oil." A novice, on the other hand, might say, "It's too spicy and greasy." Are those two descriptions the same thing? I think not. My goal is to help you become a Gordon Ramsay of the SE world—but maybe with less foul language.

With that said, let's jump into the first meaty chapter and discuss OSINT.