1 A Look into the World of Social Engineering

If you know the enemy and know yourself you need not fear the results of a hundred battles.

—Sun Tzu

Social engineering (SE) has been largely misunderstood, leading to many differing opinions on what social engineering is and how it works. This has led to a situation where some may view SE as simply lying to scam trivial free items such as pizza or obtaining sexual gratification; others think SE just refers to the tools used by criminals or con men, or perhaps that it is a science whose theories can be broken down into parts or equations and studied. Or perhaps it's a long-lost mystical art giving practitioners the ability to use powerful mind tricks like a magician or illusionist.

In whatever camp your flag flies, this book is for you. Social engineering is used every day by everyday people in everyday situations. A child trying to get her way in the candy aisle or an employee looking for a raise is using social engineering. Social engineering happens in government or small business marketing. Unfortunately, it is also present when criminals, con men, and the like trick people into giving away information that makes them vulnerable to crimes. Like any tool, social engineering is not good or evil, but simply a tool that has many different uses.

Consider some of these questions to drive that point home:

- Have you been tasked to make sure your company is as secure as possible?
- Are you a security enthusiast who reads every bit of the latest information out there?
- Are you a professional penetration tester who is hired to test the security of your clients?
- Are you a college student taking some form of IT specialization as your major?

- Are you presently a social engineer looking for new and improved ideas to utilize in your practice?
- Are you a consumer who fears the dangers of fraud and identity theft?

Regardless of which one of those situations fits you, the information contained within this book will open your eyes to how you can use social engineering skills. You will also peer into the dark world of social engineering and learn how the "bad guys" use these skills to gain an upper hand. From there, you learn how to become less vulnerable to social engineering attacks.

One warning up front: This book is not for the weak. It takes you into those dark corners of society where the "black hats," the malicious hackers, live. It uncovers and delves into areas of social engineering that are employed by spies and con men. It reviews tactics and tools that seem like they are stolen from a James Bond movie. In addition, it covers common, everyday situations and then shows how they are complex social engineering scenarios. In the end, the book uncovers the "insider" tips and tricks of professional social engineers and yes, even professional criminals.

Some have asked why I would be willing to reveal this information. The answer is simple: The "bad guys" don't stop because of a contractual limitation or their own morals. They don't cease after one failed attempt. Malicious hackers don't go away because companies don't like their servers to be infiltrated. Instead, social engineering, employee deception, and Internet fraud are used more and more each day. While software companies are learning how to strengthen their programs, hackers and malicious social engineers are turning to the weakest part of the infrastructure—the people. Their motivation is all about return on investment (ROI); no self-respecting hacker is going to spend 100 hours to get the same results from a simple attack that takes one hour, or less.

The sad result in the end is that no way exists to be 100% secure—unless you unplug all electronic devices and move to the mountains. Because that isn't too practical, nor is it a lot of fun, this book discusses ways to become more aware and educated about the attacks out there and then outlines methods that you can use to protect against them. My motto is "security through education." Being educated is one of the only surefire ways to remain secure against the increasing threats of social engineering and identity theft. Kaspersky Labs, a leading provider of antivirus and protection software, estimated that more than 100,000 malware samples were spread through social networks in 2009. In a recent report, Kaspersky estimated that "attacks against social networks are 10 times more successful" than other types of attacks.

The old hacker adage, "knowledge is power" does apply here. The more knowledge and understanding one has of the dangers and threats of social engineering

each consumer and business can have and the more each attack scenario is dissected, the easier it will be to protect from, mitigate, and stop these attacks. That is where the power of all this knowledge will come in.

Why This Book Is So Valuable

Many books are available on the market on security, hacking, penetration testing, and even social engineering. Many of these books have very valuable information and tips to help their readers. Even with all that the information available, a book was needed that takes social engineering information to the next level and describes these attacks in detail, explaining them from the malicious side of the fence. This book is not merely a collection of cool stories, neat hacks, or wild ideas. This book covers the world's first framework for social engineering. It analyzes and dissects the very foundation of what makes a good social engineer and gives practical advice on how to use these skills to enhance the readers' abilities to test the biggest weakness—the *human infrastructure*.

The Layout

This book offers a unique approach to social engineering. It is structured closely to the in-depth social engineering framework found at `www.social-engineer.org/framework`. This framework outlines the skills and the tools (physical, mental, and personality) a person should strive to possess to be an excellent social engineer.

This book takes a "tell and show approach" by first presenting a principle behind a topic then defining, explaining, and dissecting, then showing its application using collections of real stories or case studies. This is not merely a book about stories or neat tricks, but a handbook, a guide through the dark world of social engineering.

Throughout the book you can find many Internet links to stories or accounts as well as links to tools and other aspects of the topics discussed. Practical exercises appear throughout the book that are designed to help you master not only the social engineering framework but also the skills to enhance your daily communications.

These statements are especially true if you are a security specialist. As you read this book, I hope to impress upon you that security is not a "part-time" job and is not something to take lightly. As criminals and malicious social engineers seem to go from bad to worse in this world, attacks on businesses and personal lives seem to get more intense. Naturally, everyone wants to be protected, as evidenced by

the increase in sales for personal protection software and devices. Although these items are important, the best protection is knowledge: security through education. The only true way to reduce the effect of these attacks is to know that they exist, to know how they are done, and to understand the thinking process and mentality of the people who would do such things.

When you possess this knowledge and you understand how malicious hackers think, a light bulb goes off. That proverbial light will shine upon the once-darkened corners and enable you to clearly see the "bad guys" lurking there. When you can see the way these attacks are used ahead of time, you can prepare your company's and your personal affairs to ward them off.

Of course, I am not contradicting what I said earlier; I believe there is no way to truly be 100% secure. Even top-secret, highly guarded secrets can be and have been hacked in the simplest of manners.

Look at the archived story at `www.social-engineer.org/resources/book/TopSecretStolen.htm`, from a newspaper in Ottawa, Canada. This story is very interesting, because some documents ended up in the wrong hands. These weren't just any documents, but top-secret *defense* documents that outlined things such as locations of security fences at the Canadian Forces Base (CFB) in Trenton, the floor plan of the Canadian Joint Incident Response Unit, and more. How did the breach occur? The plans were thrown away, in the trashcan, and someone found them in the dumpster. A simple dumpster dive could have led to one of that country's largest security breaches.

Simple-yet-deadly attacks are launched every day and point to the fact that people need education; need to change the way they adhere to password policies and the way they handle remote access to servers; and need to change the way they handle interviews, deliveries, and employees who are hired or fired. Yet without education the motivation for change just isn't there.

In 2003 the Computer Security Institute did a survey along with the FBI and found that 77% of the companies interviewed stated a disgruntled employee as the source of a major security breach. Vontu, the data loss prevention section of Symantec (`http://go.symantec.com/vontu/`), says that 1 out of every 500 emails contains confidential data. Some of the highlights of that report, quoted from `http://financialservices.house.gov/media/pdf/062403ja.pdf`, are as follows:

- 62% reported incidents at work that could put customer data at risk for identity theft.
- 66% say their co-workers, not hackers, pose the greatest risk to consumer privacy. Only 10% said hackers were the greatest threat.

- 46% say it would be "easy" to "extremely easy" for workers to remove sensitive data from the corporate database.
- 32%, about one in three, are unaware of internal company policies to protect customer data.

These are staggering and stomach-wrenching statistics.

Later chapters discuss these numbers in more detail. The numbers show a serious flaw in the way security itself is handled. When there is education, hopefully *before* a breach, then people can make changes that can prevent unwanted loss, pain, and monetary damage.

Sun Tzu said, "If you know the enemy and know yourself you need not fear the results of a hundred battles." How true those words are, but knowing is just half the battle. Action on knowledge is what defines wisdom, not just knowledge alone.

This book is most effective used as a handbook or guide through the world of social attacks, social manipulation, and social engineering.

What's Coming Up

This is book is designed to cover all aspects, tools, and skills used by professional and malicious social engineers. Each chapter delves deep into the science and art of a specific social engineering skill to show you how it can be used, enhanced, and perfected.

The next section of this chapter, "Overview of Social Engineering," defines social engineering and what roles it plays in society today, as well as the different types of social engineering attacks, including other areas of life where social engineering is used in a non-malicious way. I will also discuss how a social engineer can use the social engineering framework in planning an audit or enhancing his own skills.

Chapter 2 is where the real meat of the lessons begins. Information gathering is the foundation of every social engineering audit. The social engineer's mantra is, "I am only as good as the information I gather." A social engineer can possess all the skills in the world, but if he or she doesn't know about the target, if the social engineer hasn't outlined every intimate detail, then the chance of failure is more likely to occur. Information gathering is the crux of every social engineering engagement, although people skills and the ability to think on your feet can help you get out of a sticky situation. More often than not, the more information you gather, the better your chances of success.

The questions that I will answer in that chapter include the following:

- What sources can a social engineer use?
- What information is useful?
- How can a social engineer collect, gather, and organize this information?
- How technical should a social engineer get?
- How much information is enough?

After the analyzation of information gathering, the next topic addressed in Chapter 2 is communication modeling. This topic closely ties in with information gathering. First I will discuss what communication modeling is and how it began as a practice. Then the chapter walks through the steps needed to develop and then use a proper communication model. It outlines how a social engineer uses this model against a target and the benefits in outlining it for every engagement.

Chapter 3 covers elicitation, the next logical step in the framework. It offers a very in-depth look into how questions are used to gain information, passwords, in-depth knowledge of the target, and his or her company. You will learn what is good and proper elicitation and learn how important it is to have your elicitations planned out.

Chapter 3 also covers the important topic of preloading the target's mind with information to make your questions more readily accepted. As you unravel this section you will clearly see how important it is to become an excellent elicitor. You will also clearly see how you can use that skill not just in your security practices but in daily life.

Chapter 4, which covers pretexting, is powerful. This heavy topic is one of the critical points for many social engineers. Pretexting involves developing the role the social engineer will play for the attack on the company. Will the social engineer be a customer, vendor, tech support, new hire, or something equally realistic and believable? Pretexting involves not just coming up with the storyline but also developing the way your persona would look, act, talk, walk; deciding what tools and knowledge they would have; and then mastering the entire package so when you approach the target, you *are* that person, and not simply playing a character. The questions covered include the following:

- What is pretexting?
- How do you develop a pretext?
- What are the principles of a successful pretext?
- How can a social engineer plan and then execute a perfect pretext?

The next step in the framework is one that can fill volumes. Yet it must be discussed from the viewpoint of a social engineer. Chapter 5 is a no-holds-barred discussion on some very confrontational topics, including that of *eye cues*. For example, what are the varying opinions of some professionals about eye cues, and how can a social engineer use them? The chapter also delves into the fascinating science of microexpressions and its implications on social engineering.

Chapter 5 goes on analyzing the research, yielding answers to these questions:

- Is it possible to use microexpressions in the field of security?
- How would you do so?
- What benefit are microexpressions?
- Can people train themselves to learn how to pick up on microexpressions automatically?
- After we do the training, what information is obtained through microexpressions?

Probably one of the most debated-on topics in Chapter 5 is *neurolinguistic programming* (NLP). The debate has many people undecided on what it is and how it can be used. Chapter 5 presents a brief history of NLP as well as what makes NLP such a controversy. You can decide for yourself whether NLP is usable in social engineering.

Chapter 5 also discusses one of the most important aspects of social engineering in person or on the phone: knowing how to ask good questions, listen to responses, and then ask more questions. Interrogation and interviewing are two methods that law enforcement has used for years to manipulate criminals to confess as well as to solve the hardest cases. This part of Chapter 5 puts to practical use the knowledge you gained in Chapter 3.

In addition, Chapter 5 discusses how to build instant rapport—a skill you can use in everyday life. The chapter ends by covering my own personal research into "the human buffer overflow": the notion that the human mind is much like the software that hackers exploit every day. By applying certain principles, a skilled social engineer can overflow the human mind and inject any command they want.

Just like hackers write overflows to manipulate software to execute code, the human mind can be given certain instructions to, in essence, "overflow" the target and insert custom instructions. Chapter 5 is a mind-blowing lesson in how to use some simple techniques to master how people think.

Many people have spent their lives researching and proving what can and does influence people. Influence is a powerful tool with many facets to it. To this end, Chapter 6 discusses the fundamentals of persuasion. The principles engaged in Chapter 6 will start you on the road toward becoming a master of persuasion.

The chapter presents a brief discussion of the different types of persuasion that exist and provides examples to help solidify how you can use these facets in social engineering.

The discussion doesn't stop there—framing is also a hot topic nowadays. Many different opinions exist on how one can use framing, and this book shows some real-life examples of it. Then dissecting each, I take you through the lessons learned and things you can do to practice reframing yourself as well as use framing in everyday life as a social engineer.

Another overwhelming theme in social engineering is *manipulation*:

- What is its purpose?
- What kinds of incentives drive manipulators?
- How can a person use it in social engineering?

Chapter 6 presents all a social engineer needs to know on the topic of manipulation, and how to successfully apply such skills.

Chapter 7 covers the tools that can make a social engineering audit more successful. From physical tools such as hidden cameras to software-driven information gathering tools, each section covers tested-and-tried tools for social engineers.

Once you understand the social engineering framework, Chapter 8 discusses some real-life case studies. I have chosen two excellent accounts from world-renowned social engineer Kevin Mitnick. I analyze, dissect, and then propose what you can learn from these examples and identify the methods he used from the social engineering framework. Moreover, I discuss what can be learned from his attack vectors as well as how they can be used today. I discuss some personal accounts and dissect them, as well.

What social engineering guide would be complete without discussing some of the ways you can mitigate these attacks? The appendix provides this information. I answer some common questions on mitigation and give some excellent tips to help secure you and your organization against these malicious attacks.

The preceding overview is just a taste of what is to come. I truly hope you enjoy reading this book as much as I have enjoyed writing it. Social engineering is a passion for me. I do believe there are certain traits, whether learned or inherent, that can

make someone a great social engineer. I also subscribe to the belief that with enough time and energy anyone can learn the different aspects of social engineering and then practice these skills to become a proficient social engineer.

The principles in this book are not new; there is no mind-blowing technology that you will see that will change the face of security forever. There are no magic pills. As a matter of fact, the principles have been around for as long as people have. What this book *does* do is combine all of these skills in one location. It does give you clear direction on how to practice these skills as well as examples of real-life situations where they are used. All of this information can help you gain a true sense of understanding the topics discussed.

The best place to start is with the basics, by answering one fundamental question: "What is social engineering?"

Overview of Social Engineering

What is social engineering?

I once asked this question to a group of security enthusiasts and I was shocked at the answers I received:

"Social engineering is lying to people to get information."

"Social engineering is being a good actor."

"Social engineering is knowing how to get stuff for free."

Wikipedia defines it as "the act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim."

Although it has been given a bad name by the plethora of "free pizza," "free coffee," and "how to pick up chicks" sites, aspects of social engineering actually touch many parts of daily life.

Webster's Dictionary defines *social* as "of or pertaining to the life, welfare, and relations of human beings in a community." It also defines *engineering* as "the art or science of making practical application of the knowledge of pure sciences, as physics or chemistry, as in the construction of engines, bridges, buildings, mines, ships, and chemical plants or skillful or artful contrivance; maneuvering."

Combining those two definitions you can easily see that social engineering is the art or better yet, science, of skillfully maneuvering human beings to take action in some aspect of their lives.

This definition broadens the horizons of social engineers everywhere. Social engineering is used in everyday life in the way children get their parents to give in to their demands. It is used in the way teachers interact with their students, in the way doctors, lawyers, or psychologists obtain information from their patients or clients. It is definitely used in law enforcement, and in dating—it is truly used in every human interaction from babies to politicians and everyone in between.

I like to take that definition a step further and say that a true definition of social engineering is the act of manipulating a person to take an action that *may* or *may not* be in the "target's" best interest. This may include obtaining information, gaining access, or getting the target to take certain action.

For example, doctors, psychologists, and therapists often use elements I consider social engineering to "manipulate" their patients to take actions that are good for them, whereas a con man uses elements of social engineering to convince his target to take actions that lead to loss for them. Even though the end game is much different, the approach may be very much the same. A psychologist may use a series of well-conceived questions to help a patient come to a conclusion that change is needed. Similarly, a con man will use well-crafted questions to move his target into a vulnerable position.

Both of these examples are social engineering at its truest form, but have very different goals and results. Social engineering is not just about deceiving people or lying or acting a part. In a conversation I had with Chris Nickerson, a well-known social engineer from the TV series *Tiger Team,* he said, "True social engineering is not just believing you are playing a part, but for that moment you *are* that person, you are that role, it is what your life is."

Social engineering is not just any one action but a collection of the skills mentioned in the framework that when put together make up the action, the skill, and the science I call social engineering. In the same way, a wonderful meal is not just one ingredient, but is made up by the careful combining, mixing, and adding of many ingredients. This is how I imagine social engineering to be, and a good social engineer is like a master chef. Put in a little dab of elicitation, add a shake of manipulation, and a few heaping handfuls of pretexting, and *bam!*—out comes a great meal of the perfect social engineer.

Of course, this book discusses some of these facets, but the main focus is what you can learn from law enforcement, the politicians, the psychologists, and even

children to better your abilities to audit and then secure yourself. Analyzing how a child can manipulate a parent so easily gives the social engineer insight into how the human mind works. Noticing how a psychologist phrases questions can help to see what puts people at ease. Noticing how a law enforcement agent performs a successful interrogation gives a clear path on how to obtain information from a target. Seeing how governments and politicians frame their messages for the greatest impact can show what works and what doesn't. Analyzing how an actor gets into a role can open your eyes to the amazing world of pretexting. By dissecting the research and work of some of the leading minds in microexpressions and persuasion you can see how to use these techniques in social engineering. By reviewing some of the motivators of some of the world's greatest salespeople and persuasion experts you can learn how to build rapport, put people at ease, and close deals.

Then by researching and analyzing the flip side of this coin—the con men, scam artists, and thieves—you can learn how all of these skills come together to influence people and move people in directions they thought they would never go.

Mix this knowledge with the skills of lock picks, spies who use hidden cameras, and professional information gatherers and you have a talented social engineer.

You do not use every one of these skills in each engagement, nor can you master every one of these skills. Instead, by understanding *how* these skills work and *when* to use them, anyone can master the science of social engineering. It is true that some people have a natural talent, like Kevin Mitnick, who could talk anyone into anything, it seemed. Frank Abagnale, Jr., seemed to have the natural talents to con people into believing he was who he wanted them to believe he was. Victor Lustig did the unbelievable, actually convincing some people that he had the rights to sell the Eiffel Tower, topped only by his scam on Al Capone.

These social engineers and many more like them seem to have natural talent or a lack of fear that enables them to try things that most of us would never consider attempting. Unfortunately in the world today, malicious hackers are continually improving their skills at manipulating people and malicious social engineering attacks are increasing. DarkReading posted an article (`www.darkreading.com/database_security/security/attacks/showArticle.jhtml?articleID=226200272`) that cites that data breaches have reached between $1 and $53 million per breach. Citing research by the Ponemon Institute DarkReading states, "Ponemon found that Web-borne attacks, malicious code, and malicious insiders are the most costly types of attacks, making up more than 90 percent of all cybercrime costs per organization per year: A Web-based attack costs $143,209; malicious code, $124,083; and malicious insiders, $100,300." Malicious insiders being listed on the top three suggests

that businesses need to be more aware of the threats posed by malicious social engineering, even from employees.

Many of these attacks could have been avoided if people were educated, because they could act on that education. Sometimes just finding out how malicious people think and act can be an eye opener.

As example on a much smaller and more personal scale, I was recently discussing with a close friend her financial accounts and how she was worried about being hacked or scammed. In the course of the conversation we started to discuss how easy it is to "guess" people's passwords. I told her that many people use the same passwords for every account; I saw her face go white as she realized this is her. I told her that most people use simplistic passwords that combine things like their spouse's name, his or her birthday, or anniversary date. I saw her go an ever-brighter shade of pale. I continued by saying that most of the time people chose the simplest "security question" such as "your (or your mother's) maiden name" and how easy finding that information is via the Internet or a few fake phone calls.

Many people will list this information in Blippy, Twitter, or Facebook accounts. This particular friend didn't use social media sites too much, so I asked her that if she thought with a few phone calls she could picture herself giving over this information. Of course she said no. To illustrate how easily people hand over personal information, I told her that I once saw a placemat in a restaurant that had a $50-off coupon for a local golf course—a very attractive offer. To take advantage of this offer, you only had to provide your name, date of birth, and street address, and provide a password for an account that would be set up and sent to your e-mail address. (I only noticed this in the first place because someone had started filling out the coupon and left it on the table.) Every day websites are created to collect such sensitive information.

A phone call with a survey or some quick research on the Internet can yield a birth date or anniversary date, and armed with this information I have enough to build a password attack list. Plus, a dozen sites offer detailed records of all sorts of personal information on an individual for a mere $9–$30 USD.

Realizing how malicious social engineers think, how scammers react to information, and how con men will try anything, can help people to be more aware of what is going on around them.

A team of security enthusiasts and I have scoured the Internet collecting stories that show many different aspects of social engineering. These stories can help answer a vital question—"how is social engineering used in society over time?"—and see where social engineering's place is and how it is used maliciously.

Social Engineering and Its Place in Society

As already discussed social engineering can be used in many areas of life, but not all of these uses are malicious or bad. Many times social engineering can be used to motivate a person to take an action that is good for them. How?

Think about this: John needs to lose weight. He knows he is unhealthy and needs to do something about it. All of John's friends are overweight, too. They even make jokes about the joys of being overweight and say things like, "I love not worrying about my figure." On one hand, this is an aspect of social engineering. It is social proof or consensus, where what you find or deem acceptable is determined by those around you. Because John's close associations view being overweight as acceptable, it is easier for John to accept it. However, if one of those friends lost weight and did not become judgmental but was motivated to help, the possibility exists that John's mental frame about his weight might change and he might start to feel that losing weight is possible and good.

This is, in essence, social engineering. So you can clearly see how social engineering fits into society and everyday life, the following sections present a few examples of social engineering, scams, and manipulation and a review of how they worked.

The 419 Scam

The 419 scam, better known as the Nigerian Scam, has grown into an epidemic. You can find an archived story and article about this scam at `www.social-engineer.org/wiki/archives/ConMen/ConMen-Scam-NigerianFee.html`.

Basically an email (or as of late, a letter) comes to the target telling him he has been singled out for a very lucrative deal and all he needs to do is offer a little bit of help. If the victim will help the letter sender extract a large sum of money from foreign banks he can have a percentage. After the target is confident and "signs on," a problem arises that causes the target to pay a fee. After the fee is paid another problem comes up, along with another fee. Each problem is "the last" with "one final fee" and this can be stretched out over many months. The victim never sees any money and loses from $10,000–$50,000 USD in the process. What makes this scam so amazing is that in the past, official documents, papers, letterhead, and even face-to-face meetings have been reported.

Recently a variation of this scam has popped up where victims are literally sent a real check. The scammers promise a huge sum of money and want in return only a small portion for their efforts. If the target will wire transfer a small sum (in comparison) of $10,000, when they receive the promised check they can deposit the

check and keep the difference. The problem is that the check that comes is a fraud and when the victim goes to cash it she is slapped with check fraud charges and fines, in some cases *after* the victim has already wired money to the scammer.

This scam is successful because it plays on the victim's greed. Who wouldn't give $10,000 to make $1,000,000 or even $100,000? Most smart people would. When these people are presented with official documents, passports, receipts, and even official offices with "government personnel" then their belief is set and they will go to great lengths to complete the deal. Commitment and consistency play a part in this scam as well as obligation. I discuss these attributes in greater detail in later chapters, and when I do, you will see why this scam is so powerful.

The Power of Scarcity

The article archived at `www.social-engineer.org/wiki/archives/Governments/Governments-FoodElectionWeapon.html` talks about a principle called *scarcity*.

Scarcity is when people are told something they need or want has limited availability and to get it they must comply with a certain attitude or action. Many times the desired behavior is not even spoken, but the way it is conveyed is by showing people who are acting "properly" getting rewards.

The article talks about the use of food to win elections in South Africa. When a group or person does not support the "right" leader, foodstuffs become scarce and jobs people once had are given to others who are more supportive. When people see this in action, it doesn't take long to get them in line. This is a very malicious and hurtful form of social engineering, but nonetheless, one to learn from. It is often the case that people want what is scarce and they will do anything if they are lead to believe that certain actions will cause them to lose out on those items. What makes certain cases even worse, as in the earlier example, is that a government took something necessary to life and made it "scarce" and available only to supporters—a malicious, but very effective, manipulation tactic.

The Dalai Lama and Social Engineering

The interesting article archived at `www.social-engineer.org/wiki/archives/Spies/Spies-DalaiLama.html` details an attack made on the Dalai Lama in 2009.

A Chinese hacker group wanted to access the servers and files on the network owned by the Dalai Lama. What methods were used in this successful attack?

The attackers convinced the office staff at the Dalai Lama's office to download and open malicious software on their servers. This attack is interesting because it blends both technology hacking and social engineering.

The article states, "The software was attached to e-mails that purported to come from colleagues or contacts in the Tibetan movement, according to researcher Ross Anderson, professor of security engineering at the University of Cambridge Computer Laboratory, cited by the *Washington Times* Monday. The software stole passwords and other information, which in turn gave the hackers access to the office's e-mail system and documents stored on computers there."

Manipulation was used as well as common attack vectors such as phishing (the practice of sending out emails with enticing messages and links or files that must be opened to receive more information; often those links or files lead to malicious payloads) and exploitation. This attack can work and has worked against major corporations as well as governments. This example is just one in a large pool of examples where these vectors cause massive damage.

Employee Theft

The topic of employee theft could fill volumes, especially in light of the staggering statistic found at `www.social-engineer.org/wiki/archives/DisgruntledEmployees/DisgruntledEmployees-EmployeeTheft.html` that more than 60 percent of employees interviewed admitted to taking data of one sort or another from their employers.

Many times this data is sold to competitors (as happened in this story from a Morgan Stanley employee: `www.social-engineer.org/wiki/archives/DisgruntledEmployees/DisgruntledEmployees-MorganStanley.html`). Other times employee theft is in time or other resources; in some cases a disgruntled employee can cause major damage.

I once talked to a client about employee discharge policies, things like disabling key cards, disconnecting network accounts, and escorting discharged employees out of the building. The company felt that everyone was part of the "family" and that those policies wouldn't apply.

Unfortunately, the time came to let go of "Jim," one of the higher-ranking people in the company. The "firing" went well; it was amicable and Jim said he understood. The one thing the company did right was to handle the firing around closing time to avoid embarrassment and distraction. Hands were shook and then Jim asked the fateful question, "Can I take an hour to clean out my desk and take some personal pictures off my computer? I will turn my key card into the security guard before I leave."

Feeling good about the meeting, they all quickly agreed and left with smiles and a few laughs. Then Jim went to his office, packed a box of all his personal items, took the pictures and other data off his computer, connected to the network, and

wiped clean 11 servers' worth of data—accounting records, payroll, invoices, orders, history, graphics, and much more just deleted in a matter of minutes. Jim turned in his key card as he promised and calmly left the building with no proof that he was the one to initiate these attacks.

The next morning a call came in to me from the owner describing the carnage in the ex-employee's wake. Hoping for a silver bullet, the client had no choice but try to recover what could be recovered forensically and start over from the backups, which were more than two months old.

A disgruntled employee who is left unchecked can be more devastating than a team of determined and skilled hackers. To the tune of $15 billion USD, that is what the loss is estimated at being to businesses in the U.S. alone due to employee theft.

These stories may leave a question about what different categories of social engineers are out there and whether they can be classified.

DarkMarket and Master Splynter

In 2009 a story broke about an underground group called DarkMarket—the so-called eBay for criminals, a very tight group that traded stolen credit card numbers and identity theft tools, as well as the items needed to make fake credentials and more.

An FBI agent by the name of J. Keith Mularski went under deep cover and infiltrated the DarkMarket site. After a while, Agent Mularski was made an administrator of the site. Despite many trying to discredit him he hung in for more than three years as the admin of the site.

During this time, Mularski had to live as a malicious hacker, speak and act as one, and think as one. His pretext was one of a malicious spammer and he was knowledgeable enough to pull it off. His pretext and his social engineering skills paid off because Agent Mularski infiltrated DarkMarket as the infamous Master Splynter, and after three years was essential in shutting down a massive identity theft ring.

The three-year social engineering sting operation netted 59 arrests and prevented over $70 million in bank fraud. This is just one example of how social engineering skills can be used for good.

The Different Types of Social Engineers

As previously discussed, social engineering can take on many forms. It can be malicious and it can be friendly, it can build up and it can tear down. Before moving on

to the core of this book, take a brief look at the different forms of social engineers and a very short description of each:

- **Hackers:** Software vendors are becoming more skilled at creating software that is *hardened*, or more difficult to break into. As hackers are hitting more hardened software and as software and network attack vectors, such as remote hacking, are becoming more difficult, hackers are turning to social engineering skills. Often using a blend of hardware and personal skills, hackers are using social engineering in major attacks as well as in minor breaches throughout the world.
- **Penetration testers:** Since a real-world penetration tester (also known as a pentester) is very offensive in nature, this category must follow after hackers. True penetration testers learn and use the skills that the malicious hackers use to truly help ensure a client's security. Penetration testers are people who might have the skills of a malicious black hat but who never use the information for personal gain or harm to the target.
- **Spies:** Spies use social engineering as a way of life. Often employing every aspect of the social engineering framework (discussed later in this chapter), spies are experts in this science. Spies from all around the world are taught different methods of "fooling" victims into believing they are someone or something they are not. In addition to being taught the art of social engineering, many times spies also build on credibility by knowing a little or even a lot about the business or government they are trying to social engineer.
- **Identity thieves:** Identity theft is the use of information such as a person's name, bank account numbers, address, birth date, and social security number without the owner's knowledge. This crime can range from putting on a uniform to impersonating someone to much more elaborate scams. Identity thieves employ many aspects of social engineering and as time passes they seem more emboldened and indifferent to the suffering they cause.
- **Disgruntled employees:** After an employee has become disgruntled, they often enter into an adversarial relationship with their employer. This can often be a one-sided situation, because the employee will typically try to hide their level of displeasure to not put their employment at risk. Yet

the more disgruntled they become, the easier it becomes to justify acts of theft, vandalism, or other crimes.

- **Scam artist:** Scams or cons appeal to greed or other principles that attract people's beliefs and desires to "make a buck." Scam artists or con men master the ability to read people and pick out little cues that make a person a good "mark." They also are skillful at creating situations that present as unbeatable opportunities to a mark.
- **Executive recruiters:** Recruiters also must master many aspects of social engineering. Having to master elicitation as well as many of the psychological principles of social engineering, they become very adept at not only reading people but also understanding what motivates people. Many times a recruiter must take into consideration and please not only the job seeker but also the job poster.
- **Salespeople:** Similar to recruiters, salespeople must master many people skills. Many sales gurus say that a good salesperson does not manipulate people but uses their skills to find out what people's needs are and then sees whether they can fill it. The art of sales takes many skills such as information gathering, elicitation, influence, psychological principles, as well as many other people skills.
- **Governments:** Not often looked at as social engineers, governments utilize social engineering to control the messages they release as well as the people they govern. Many governments utilize social proof, authority, and scarcity to make sure their subjects are in control. This type of social engineering is not always negative, because some of the messages governments relay are for the good of the people and using certain elements of social engineering can make the message more appealing and more widely accepted.
- **Doctors, psychologists, and lawyers:** Although the people in these careers might not seem like they fit into the same category as many of these other social engineers, this group employs the same methods used by the other groups in this list. They must use elicitation and proper interview and interrogation tactics as well as many if not all of the psychological principles of social engineering to manipulate their "targets" (clients) into the direction they want them to take.

Regardless of the field, it seems that you can find social engineering or an aspect of it. This is why I hold firmly to the belief that social engineering is a science. Set equations exist that enable a person to "add up" elements of social engineering to lead to the goal. In the example of a con man, think of the equation like this: pretext + manipulation + attachment to greed = target being social engineered.

In every situation, knowing what elements will work is the hard part, but then learning how to utilize those elements is where the skill comes in. This was the basis for thought behind developing the social engineering framework. This framework has revolutionized the way social engineering is dissected, as discussed in the next section.

The Social Engineering Framework and How to Use It

Through experience and research I have tried to outline the elements that make up a social engineer. Each of these elements defines a part of the equation that equals a whole social engineer. These aspects are not set in stone; as a matter of fact, from its original state until now the framework has grown.

The purpose of the framework is to give enough information for anyone to build on these skills. The framework is not designed to be an all-inclusive resource for all information in each chapter. For example, the portion of Chapter 5 that covers microexpressions is based on the research of some of the greatest minds in this field and my experience in using that information. By no means is it meant to replace the 50 years of research by such great minds as Dr. Paul Ekman.

As you read through the framework you will see that by utilizing the many skills within it, you can not only enhance your security practice, but also your mindset about how to remain secure, how to communicate more fully, and how to understand how people think.

Refer to the table of contents for a clear picture of the framework or view it online at `www.social-engineer.org/framework`. At first glance the framework may appear daunting, but inside this book you will find an analysis of each topic that will enable you to apply, enhance, and build these skills.

Knowledge is power—it is true. In this sense, education is the best defense against most social engineering attacks. Even the ones that knowledge can't protect 100 percent against, having details of these attacks keeps you alert. Education can help you enhance your own skills, as well as be alert.

Along with education, though, you need practice. This book was not designed to be a once-read manual; instead it was designed to be a study guide. You can practice

and customize each section for your needs. The framework is progressive in the sense that it is the way a social engineering attack is laid out. Each section of the framework discusses the next topic in the order that a social engineer might utilize that skill in their engagement or planning phases.

The framework shows how an attack might be outlined. After the attack is planned out, the skills that are needed can be studied, enhanced, and practiced before delivery.

Suppose, for example, that you are planning a social engineering audit against a company that wanted to see whether you could gain access to its server room and steal data.

Maybe your plan of attack would be to pretend to be a tech support person who needs access to the server room. You would want to gather information, maybe even perform a dumpster dive.

Then under the pretext of being the tech guy, you could utilize some covert camera tools as well as practice the proper language and facial/vocal cues for how to act, sound, and look like a tech guy.

If you locate what company your client uses for tech support you may need to do info gathering on it. Who does your client normally get to service them? What are the names of the employees with whom they interact? The attack needs to be planned out properly.

This book is not just for those who perform audits, though. Many readers are curious about what the attacks are, not because they are protecting a company, but because they need to protect themselves. Not being aware of the way a malicious social engineer thinks can lead someone down the path toward being hacked.

College students in the field of security have also used the framework. The information in the framework outlines a realistic path for these vectors, or methods of attack, and enables the reader to study them in depth.

Generally, this information can also help enhance your ability to communicate in everyday life. Knowing how to read facial expressions or how to use questions to put people at ease and elicit positive responses can enhance your ability to communicate with your family and friends. It can assist you in becoming a good listener and more aware of people's feelings.

Being able to read people's body language, facial expressions, and vocal tones can also enhance your ability to be an effective communicator. Understanding how to protect yourself and your loved ones will only make you more valuable and more aware of the world around you.

Summary

Like any book, the knowledge contained herein is only useful if it you put it into practice. The more you practice the more you will succeed at mastering these skills.

Previously, I discussed how social engineering is like mastering the art of cooking. By mixing the right ingredients in the right quantity you can have a meal that is full of flavor and excitement. The first time you try to cook a meal it might have too much salt or it might lack flavor altogether, but you don't immediately throw in the towel—you keep trying until you get it right. The same goes for social engineering. Some of the necessary skills may come more naturally to you and others may be more difficult.

If a particular topic is hard to understand or difficult for you to grasp, do not give up, and do not assume you cannot learn it. Anyone can learn and use these skills with the right amount of effort and work.

Also keep in mind that, just like a real recipe, many "ingredients" go into a good social engineering gig. The first ingredient might make more sense after you get down the line a little more. Certain skills—such as "the human buffer overflow" covered in Chapter 5—will only make sense after you master some of the other skills discussed in this book.

Regardless, keep practicing and make sure to do extra research on topics for which you need clarity. Now let's start cooking. Your "recipe" starts in the next chapter with the first ingredient, information gathering.