1
Introduction to Social Engineering

_They say a little knowledge is a dangerous thing, but it's not one half so bad as a lot of ignorance._
—Terry Pratchett

Welcome to the twisted and deceitful world of social engineering where nothing is as it seems. What you are about to read can be used for good or for evil. The choice is yours to make. Social engineering involves convincing people to perform actions they would not normally do. This usually involves revealing certain information or bypassing certain security controls, giving the social engineer access to sensitive information or facilities. It can be as simple as slipping in through a door that someone has left open or as sophisticated as setting up a long-term scam where the social engineer becomes an internal employee at her target organization and then steals information from the company.

Because computer security is becoming more sophisticated, hackers are increasingly combining their technical expertise with social engineering skills as a means of getting what they want. Social engineering can help ease along a technical attack, making it quicker and easier to execute. Many of the technical attacks we hear about include an element of social engineering. More often than not, however, the attack goes unreported. Sometimes people don’t even realize they have been social engineered. A good social engineering attack is hard to detect, after all—although after reading this book, you will have a much greater chance of doing so! Victims may only identify the technical aspect of the attack and may not realize that it included a social engineering component. When they do recognize that they have fallen for a social engineering attack, victims are sometimes too embarrassed to report the attack, fearing it could make them appear gullible and they might lose credibility by doing so. Some people, some security professionals included, are under the misguided impression that only unwitting victims who are all too ready to be duped are at risk from social engineers. But even the most security savvy among us can fall victim to social engineering attacks.

Social engineering attacks can have disastrous consequences, both for a victim’s finances and reputation. An organization can have the best technical security controls in the world, but these controls may not protect it against a determined
Social Engineering in IT Security

and skilful social engineer. Education and awareness are key to preventing social engineering attacks. Social engineering testing can play a big role in this, by identifying weaknesses in an organization’s security program and by giving its staff the opportunity to identify social engineering techniques in practice.

The objectives of this book are twofold. First, it presents a methodology that you can use to perform an ethical social engineering test. Second, by considering the different stages of the social engineering process, you will understand the steps that a social engineer will work through and hopefully be better able to defend against social engineering attacks as a result. My intentions in writing this book are neither to tell readers how to perform malicious social engineering attacks nor to encourage them to do so. Rather, it is to inform readers of the different stages of the social engineering process so they can better defend against malicious social engineering attacks. Like the quote at the beginning of the chapter from one of my favorite authors and creator of the Discworld, Terry Pratchett, I would rather people have a little knowledge, in this case about what the bad guys are up to and how they do it, rather than a lot of ignorance on the topic.

Different Types of Social Engineering

There are many types of social engineering attacks, but they can be broadly split into physical social engineering, when the attacker attempts to gain physical access to a sensitive office or location, and remote social engineering, when the attacker attempts to gain access to information or resources remotely, for example, over the phone or via email. Some social engineering attacks combine the two; for example, the physical breach may follow a series of remote social engineering attempts. Often social engineering is combined with a technical attack, making for an extremely effective and dangerous assault. The types of social engineering attacks are reflected in the various social engineering tests you can perform.

Physical Social Engineering

In a physical social engineering attack, the social engineer attempts to gain access to a physical location. He may do this via various methods, including

- Impersonation or false pretenses, for example, pretending to be a member of staff or a third party who has authorized access to the location
- Tailgating (following someone through an entrance without the person knowing) or piggybacking (following someone through an entrance with that person’s knowledge or permission)
- Taking advantage of weaknesses in the physical security system, for example, disabling CCTV systems so security guards can’t see the breach as it is happening or bypassing a fingerprint scanner using various methods

This book describes plenty of examples of physical social engineering attacks. For now, let’s take a look at two types of attacks: dumpster diving and distraction attacks.
Chapter 1  Introduction to Social Engineering

Dumpster Diving

Dumpster diving involves going through the dumpsters or trash cans of the target organization to discover potentially sensitive information or information that can be used to further an attack—anything from printed-out snippets of code to discarded computers or electronic media. Dumpsters, both internal and external, provide rich pickings for social engineers. Even the rubbish you discard at your home can be used by social engineers, so it is important to discard sensitive information appropriately. Chapter 5 includes details on dumpster diving, including the types of information social engineers look for and what equipment they bring on the dive.

Distraction Attacks

In physical social engineering attacks in particular, social engineers may use a distraction to divert attention from the real attack. Social engineers working in groups may create a commotion that keeps the security guards busy while their accomplices sneak into the building. The classic social engineering movie Sneakers has a great example of this. An apparently very agitated Robert Redford arrives at reception and asks if his wife has left a cake for him for the surprise party on the second floor. At the same time, Redford’s colleague is disguised as a delivery man who is trying to drop off an unscheduled delivery of cleaning products. The receptionist is getting increasingly flustered. A car horn beeps and Redford, implying that it is his wife, goes out and returns holding a cake and some balloons, again supposedly for the party on the second floor. Both Redford and his colleague get upset with the receptionist. Between the two of them, they create such a furor that when Redford shouts, “Just push the goddamned buzzer, will you?” the receptionist buzzes him straight through.

Thieves often use distractions during robberies. I witnessed a distraction theft in Barcelona when a guy stopped a driver to ask her for directions. While she was leaning out the car window and pointing out the directions on the map, his accomplice reached in the other car window and grabbed the woman’s handbag. She didn’t notice a thing. Distraction theft is also common at ATMs where thieves target unsuspecting patrons as they withdraw their money. One thief distracts the victim, for instance, by dropping something or spilling a drink on the victim, while another thief grabs the victim’s cash and/or bank card. A popular distraction in the UK is to drop some money on the ground, say a £20 note, and then tell the victim that he dropped it. While the victim is either picking up the money or denying that it is his, an accomplice makes off with his cash or bank card. One of the thieves will have most likely shoulder surfed the PIN code as the victim entered it, so the victim stands to lose a lot of money rather quickly.

A ten attack is a type of distraction attack that is frequently seen in the movies. It involves using an attractive person (someone you would rate a ten out of ten, thus the name) to distract the security guard while the accomplices sneak into the building. Someone told me that they once created the diversion for a ten attack in a most interesting manner; this person had broken both legs and was in a wheelchair and pretended to have difficulties getting into the building. While the security guards and receptionists were distracted, the other social engineers slipped in unnoticed.
4  Social Engineering in IT Security

Remote Social Engineering
Any communications system can be used by social engineers, whether it's telephone, email, social networking systems, instant messaging, or even fax machines, which rather unbelievably can still work wonders for social engineers (try sending a fax to your target organization in advance so they are expecting you, for example). Remote social engineering may involve direct, real-time communication with the target (over the phone or via instant messaging, for example) or communication that doesn't require an immediate response (email), which gives social engineers more time to plan their next steps.

Social Engineering by Email
Social engineering emails take many forms. The social engineer tries to build rapport as a precursor to the actual breach, or she tries to elicit information or spread malware by tricking the email recipient into opening a malicious attachment or visiting a malicious website. Two of the most common forms of social engineering over email are phishing and 419 scams.

Phishing emails typically take the form of fake notifications purporting to be from a well-known organization (often banks, payment systems, and auction sites), asking for the recipient's personal information including user credentials, credit card numbers, or banking information. Phishing attacks are, essentially, a bait-and-hook scam in which the email is the bait, used to lure unsuspecting victims in before hooking information from them. The social engineering really takes place during the bait, which should be enticing enough to convince the intended victims to open the message and follow the instructions within it. The hook is the method whereby the social engineer gets information from their victims, either a link to a malicious website or a telephone number that the victim is asked to call, for example.

Phishing messages used to be easy to identify, thanks to bad grammar and spelling, poorly formatted emails, and obviously fake links. However, they are becoming more sophisticated and more convincing because they have been increasingly personalized with more background research. Phishing attacks that are customized and targeted at particular individuals are known as spear phishing. When targeted toward rich or powerful targets, they are sometimes called whale phishing. And phishing is not limited to email. You can get phishing messages via social networks, SMS (SMiShing), or voicemail (vishing).

The classic Nigerian 419 or advance-fee fraud scam is named after the article of the Nigerian penal code under which the perpetrator can be prosecuted. The fraudster poses as or represents a distressed but reputable person who for one reason or another needs some money to help her out of a jam; of course, the victim will supposedly be rewarded many times over for his generosity—although the reward never quite arrives due to one complication or another, which usually requires more money to solve. The scam combines emotion (feeling sorry for the person who has made the request because her family has died, she has been wrongfully imprisoned, she is being persecuted, and so on) with the potential to make a quick and hefty profit while feeling good about helping somebody out, appealing to good Samaritans and business
people alike. Basically, the scammer tries to convince the intended victim to advance her some money in return for sharing in the profit later on.

**Social Engineering by Phone**

In social engineering attacks via the telephone, the social engineer attempts to get the victim to disclose sensitive information or to perform an action such as visiting a malicious website or granting the social engineer access to a certain system. The caller generally assumes a false identity and may use various techniques to convince the victim, such as being overly friendly, acting in an authoritative manner, or applying pressure. The caller may purport to be from tech support or an anti-virus organization, a financial institution, or even a charity. In many business cultures, challenging someone’s identity is not socially acceptable and may be seen as impolite, so getting away with assuming a false identity may be easier than you think.

**Mumble Attack**  
*Mumble attacks* are telephone social engineering attacks that are generally targeted at call center agents. The social engineer poses as a speech-impaired customer or as a person calling on behalf of the speech-impaired customer. Victims of the attack are often made to feel awkward or embarrassed and release information as a result.

Online information brokers used mumble attacks to dupe employees of Verizon Wireless into disclosing thousands of private cell phone records, which the brokers then sold. They called Verizon customer service purporting to be from the organization’s “special needs group” (a nonexistent department) and requested account information. They claimed to be making the request on behalf of a voice-impaired customer who was unable to make the request. If the Verizon customer service agent asked to speak directly to the customer, the social engineer would then impersonate a voice-impaired individual by using a mechanical device to distort his or her voice.

I often use a “mumble attack lite” during my social engineering tests. Irish people are known for speaking very quickly. As an Irish person, I sometimes take advantage of this trait. Let’s face it—you can ask someone to repeat themselves only so many times before you begin to feel awkward. I’ve used this to my advantage on social engineering tests in foreign countries, where eventually my targets have given up on trying to understand me and just comply with my request. Magicians sometimes use mishearing people or getting people’s names wrong as misdirection for their magic tricks. There is a great quote from “The Last Nazi” episode of the TV series, *The Unit*, when Jonas tells Bridget, “You muffle the name, 99 to 1, they’ll come back at you and deliver it to you.”

**Combination Attacks**

Many security breaches combine attacks to achieve their goals, whether combining remote and physical social engineering, such as the Boy Who Cries Wolf attack or the road apple attack, described next, or a combination of social engineering and the more traditional technical attacks.
Social Engineering in IT Security

Boy Who Cries Wolf Attack
When was the last time you responded to a car alarm? Did you contact the police, investigate the alarm, or look for the car’s owner? We hear car alarms every day, but few, if any, of us do anything about them. Because we hear them so much, we have become conditioned into not responding.

Like in the classic fable, in a Boy Who Cried Wolf attack, a series of false alarms are set off prior to the real attack, so that by the time the real attack actually happens, no one thinks it is an attack so they don’t bother responding. In a way, they have been social engineered into thinking the attack isn’t real. The University of British Columbia fell victim to a Boy Who Cried Wolf–style attack in 2008, when thieves made off with 15 art objects worth $2 million from their Museum of Anthropology. A few hours before the break-in, a couple of the museum’s surveillance cameras mysteriously went offline. Campus security received a call from someone purporting to be from the alarm company telling them there was a problem with the system and asking them to ignore any alarms that were triggered, which they did. That night, when the lone security guard on duty at the museum went out to have a cigarette, the thieves broke in and stole the pieces.

In the classic comedy heist movie, *How to Steal a Million*, Audrey Hepburn and Peter O’Toole execute a fantastic Boy Who Cried Wolf attack. The glamorous perpetrators hide in a utility closet of a museum and proceed to set off the hi-tech burglar alarm repeatedly. Annoyed by the continual disruption, the security guards eventually disable the system, clearing the way for Hepburn and O’Toole to make off with the goods.

Road Apples
As well as being a bit of a countryside phenomenon, a road apple is a physical object, usually a storage device, such as a USB drive, memory card, or CD, that a social engineer leaves in the vicinity of his target organization in the hope that one of the organization’s staff members will pick it up and plug it into their computer, unknowingly running a malicious program—or, in the case of an ethical social engineering test, a benign program that might do something like redirect the user to a training and awareness website.

A good road apple piques the intended victim’s curiosity or otherwise convinces him or her to plug it into the computer. It might be marked “salary information,” “naked images,” or “redundancy information,” for example—anything that a victim might find interesting. Some clever fraudsters in North Dakota created road apples in the form of traffic violation notices, placing them on cars. Recipients of the notices were then requested to visit a website where they could identify their vehicle and pay the fine. When they visited the website, they were prompted to install a toolbar to view images of their vehicles. Instead, they downloaded malware, leading to the compromise of their machines.

The name road apple is appropriate, because if you “bite a road apple,” you are well and truly in the sh!t. Think of road apples as classic bait-and-hook scams, much like phishing, except that the bait is a physical device. The original road apple was the
Trojan Horse from Greek mythology. Nowadays we just update the big wooden horse to something a little more contemporary.

Chapter 7 gives some tips on how to create an effective road apple for your social engineering test.

The History and Evolution of Social Engineering

The first references to the term social engineering date back to the late nineteenth century when “the social question,” that is, the fate of blue-collar workers, was frequently debated by philanthropic industrialists. Jacob C. van Marken, a Dutch industrialist at the time, coined the term sociale ingenieurs (social engineers) in an essay published in the Delftsche Corps-Almanak in 1894. van Marken postulated that modern employers needed the assistance of social engineers in managing the human aspects of the industrial plant, just as they needed mechanical engineers to manage the mechanical aspects of the plant. Such social engineers would manage “specifically human problems.”

In the early twentieth century, the term began to shift from industry to politics and then to social science, where it encompassed behavioral control, societal transformation, and nationalist politics, to varying degrees. Even Sigmund Freud's nephew, Edward Bernays, considered that it was necessary to manipulate society, which would otherwise be irrational and dangerous. Bernays noted that the propaganda used in the war had been extremely effective in influencing the public's opinion. He put the propaganda model to full use in peacetime, developing the field of public relations, which is essentially a type of social engineering. Social engineering was not a well-liked discipline and was frequently controversial. Not much has changed in this respect as it shifted from social sciences to technology.

The Golden Age of Con Artistry

The con artists from the late 1800s and early 1900s were the natural predecessors of today's social engineers, albeit they executed their scams with much more style and flair than we tend to see today. This was the golden age of con artistry. In fact, according to historian Karen Halttunen, police estimated that nearly one out of ten professional criminals in New York in the 1860s was a confidence man! These tricksters had a repertoire of colorful scams with equally colorful names—the gold brick, the sick engineer, the Spanish prisoner, Jamaican switch, the golden wire, and the badger game, among others. The most successful scams were elegantly simple, such as the glim dropper scam described in the following sidebar. Many of these scams will seem familiar as they are the precursors of many of today's social engineering attacks. Just add some technology into the mix and voilà—a modern social engineering scam!

---

1Many of these cons are beautifully described in David Maurer's 1940 book, The Big Con: The Story of the Confidence Man. Maurer was a linguistics professor who interviewed hundreds of con artists in the 1930s and became an expert in the language used by the underworld at the time.
The Glim Dropper

The premise of the glim dropper con is that you take something worthless (often something personal or fake jewelry) and make your victim an offer on it should it come into their possession. Then, usually with the aid of an accomplice, you arrange to sell the item to the victim for a lower price. The victim knows he can make a profit so he gladly accepts, but the original offer never rematerializes.

When this scam first appeared, the worthless item, the “glim,” was a glass eye. The scam required several accomplices, one of whom had to be a one-eyed man. The one-eyed man went into a shop where he pretended to have lost his glass eye. (I don’t have a glass eye and I’m not entirely sure how easy it would be to lose a glass eyeball, but that’s beside the point.) The one-eyed man would offer the shopkeeper a $1,000 reward for the return of the eye, leaving his contact information. The following day, an accomplice entered the shop and found the glass eye. The shopkeeper, spotting the opportunity to make a quick profit, would sometimes offer to return the eye to its original owner, but the accomplice would insist on returning it in person. Rather than lose the generous reward, the shopkeeper would offer a lesser amount, say $100, for the eye. If the accomplice was confident enough, he would bargain upward from there, sometimes as high as $250 if he was lucky. Of course, the one-eyed man never returned to collect his glass eye and could never be contacted again.

The scam sounds pretty dated, doesn’t it? But like many of these older cons, with a new twist it can still work today. An eBay user, BadgerMatt, wrote on Reddit about how he tricked a buyer who refused to pay into handing over the money using the glim dropper con in 2011. The buyer had purchased sports tickets from him for $600 but refused to pay because she had overbid and claimed her husband wouldn’t let her buy them. BadgerMatt created a new eBay account, which he dubbed Payback, and emailed the non-paying buyer, telling her that he noticed she won the tickets, which he had meant to bid for, and offered her $1,000 for them. She said she would sell them for $1,100, despite not having actually purchased the tickets. So she contacted the original seller account BadgerMatt and agreed to purchase the tickets on condition that he drop them off for her that very night, which he obligingly did (and demanded an extra $20 for the hassle of driving over at midnight). The following day, she contacted Payback to check that they were still on for the exchange. Payback told her he could no longer make the game so the exchange was off. BadgerMatt got his $600 and an extra few bucks thanks to social engineering the buyer using the glim dropper.

William Thompson: The Original Confidence Man

The term confidence man was first coined by the New York Herald in 1849 during their coverage of the arrest of William Thompson, a swindler operating on the streets of Manhattan. Thompson, a well-dressed man with a polite manner, would approach strangers and start a conversation as if he knew them. Eventually he would ask his victim or mark, “Sir, do I have your confidence in me to trust me with your watch
Chapter 1  Introduction to Social Engineering

until tomorrow?” The mark, supposing Thompson to be an old friend, would agree and hand over his watch to the trickster. Needless to say, Thompson disappeared and the victim would see neither Thompson nor his valuable watch again.

Thompson tricked several New Yorkers out of their expensive watches before a victim from whom Thompson had absconded with his $110 pocket watch, recognized him on the street and had him arrested. The trial made newspaper headlines across the country when he was arrested in 1849 and again in 1855. Although Thompson was by no means the first con artist, he was reportedly the first to use the word “confidence” to his victims, resulting in the term confidence man, or con man for short.

Victor “The Count” Lustig (1890–1947)

Thompson’s confidence scam pales in comparison with the sheer audacity of Victor Lustig’s Eiffel Tower scam. Lustig was born in what is now the Czech Republic in 1890. He became a successful con man and was wanted by the police in several European countries. He relocated to the United States and decided to give himself the title of “Count” as he thought it sounded important. While in the US, he perpetrated many scams, including swindling none other than Al Capone himself out of $1,000. Lustig convinced Capone to invest $50,000 in a scam he was planning. He promised the notorious gangster that he would double his money within 60 days. When the 60 days were up, he returned to Capone and confessed that the scam had fallen through. Lustig returned Capone’s investment to him and the gangster was so impressed that he gave the Count a $1,000 reward, which was supposedly what Lustig had been playing for all along.

On his return to Europe, Lustig played out one of his most famous and daring capers. It was widely reported by the press that the Eiffel Tower was in need of repair. Some people were campaigning for the tower to be torn down. Lustig appointed himself “Deputy Director-General of the Ministry of Mail and Telegraphs” and contacted five of the most prominent scrap metal dealers in Paris. He requested that the dealers meet with him in the suite of a prestigious Parisian hotel, Hôtel de Crillon, to discuss a confidential business matter. He explained to the dealers that it would be too expensive to repair the Eiffel Tower so they were going to dismantle it for scrap metal and sell it to the highest bidder. He reminded the potential buyers that the Eiffel Tower was never meant to be a permanent structure and quoted Alexander Dumas, who had called it “a loathsome construction.” He asked them to keep the controversial meeting secret or risk public outcry. His scenario was well played out and well researched; the scrap metal dealers swallowed it hook, line, and sinker.

Lustig spoke to each of the dealers and selected the one who he felt was most likely to fall for his scam, one Monsieur André Poisson. Lustig drew up a fake contract handing over ownership of the Eiffel Tower, cashed the check he received from Poisson and fled to Austria. Lustig scanned the newspapers every day for reports of the scam, but Poisson never reported it, most likely out of embarrassment.

A short time later, Lustig felt confident enough to go back to Paris to pull the stunt again. This time, the victim reported his $100,000 loss to the police and the story hit the press, prompting Lustig to return to America.
Social Engineering in IT Security

It’s Just Another Case of History Repeating Itself

Lustig’s Eiffel Tower scam was similar in many ways to the social engineering scams we see today. He took advantage of current events (the state of the economy and proposed plans to dismantle the Eiffel Tower) to create a plausible back story for his scam. He impersonated someone of authority—a fictional government official—sending forged letters on letterhead. It was an extremely good deal for buyers—like many scams, maybe a bit too good to be true, but his victims bit the bullet and fell for the scam regardless. Finally, Lustig sold the Eiffel Tower twice over because the first victim was supposedly too embarrassed to go to the police, just as many victims are today, allowing crooks to get away with their scams and continue to prey on other victims.

Many fraudsters have since sold popular landmarks. It’s not as unusual as you might expect. In 1947, George C. Parker regularly sold New York landmarks to unsuspecting tourists. He sold the Brooklyn Bridge twice a week, telling buyers they could charge people a toll to cross the bridge. More recently, in 2010, a British truck driver, Anthony Lee, was sentenced to five years’ imprisonment for trying to sell one of London’s most prestigious properties, the Ritz Hotel and Casino. Lee contacted a director from property-source.com, a specialist in finding property for private clients, purporting to be a “close friend and associate” of the reclusive billionaire Barclay brothers who own the Ritz Hotel. He explained that he was going to buy the Ritz for £200 million and planned to sell it immediately for “the bargain price of £250 million,” offering to split the £50 million difference with the director if she could find a buyer. At the time, the Ritz was valued at between £450 and £600 million, so as with the Eiffel Tower scam, it was another case of the deal being too good to be true. The buyers put down a £1 million deposit to secure the deal. Lee claimed he received a better offer, but the deposit was nonrefundable. He was later found guilty of obtaining the £1 million by deception and sentenced to five years in prison.

Over the course of his career, Lustig had 45 known aliases and counted nearly 50 arrests in the US alone. In 1935, Lustig was finally sentenced to 20 years in Alcatraz because of a counterfeit dollar scheme he had running. Ironically, he was protected by order of another prisoner—Al Capone! He died from pneumonia in prison having served 12 years of his sentence. Before he died, Lustig wrote his “Ten Commandments for Aspiring Con Men.” They apply just as easily to social engineers today:

1. Be a patient listener (it is this, not fast talking, that gets a con man his coups).
3. Wait for the other person to reveal any political opinions, then agree with them.
4. Let the other person reveal religious views, then have the same ones.

---

2Kathryn Lindskoog, Fakes, Frauds & Other Malarkey (Zondervan Publishing House, 1992). I’m not sure about number 5 on the list if it’s part of an ethical social engineering test...
Chapter 1  Introduction to Social Engineering

5. Hint at sex talk, but don't follow it up unless the other fellow shows a strong interest.
6. Never discuss illness, unless some special concern is shown.
7. Never pry into a person's personal circumstances (they'll tell you all eventually).
8. Never boast. Just let your importance be quietly obvious.
9. Never be untidy.
10. Never get drunk.

Social Engineering in the 1920s: Charles Ponzi

A Ponzi scheme is a pyramid scheme scam that pays early investors returns from the investments of later investors. Although Charles Ponzi did not actually invent the Ponzi scheme, he practiced it so extensively and so successfully that the scam came to be named after him.

Ponzi arrived in the United States from Italy in 1903. He drifted from job to job, often getting into trouble for cheating or stealing from customers and even for smuggling illegal immigrants across the border. Ponzi noticed that you could buy international postal reply coupons in Italy and redeem them at a profit in the US because of the difference in currency values. He set up a very official-sounding business in Boston, which he called the "Securities Exchange Company" to take advantage of this arbitrage. He sought investors for his company, promising them a hefty profit on their investment of 50 percent within 45 days or a full 100 percent within 90 days. He paid returns to early investors with later investors' money, pocketing much of the money himself, although most investors chose to reinvest the money rather than taking their profits. People began to line up to give cash to this apparent financial wizard. Ponzi reportedly had over 40,000 investors and by mid-1920 was making $250,000 a day!

It wasn't to last. Newspapers and banks started to investigate him and rumors of Ponzi's criminal past began to emerge. Investors panicked and started to withdraw their money, causing the scheme to crash and six banks to crumble in the process. Ponzi's victims collectively lost an estimated $20 million, with the story making headlines across the world. Ponzi served three-and-a-half years in jail and had frequent brushes with the law for the rest of his life. He ended his days in poverty, living in Brazil where he got occasional work as a translator. Ponzi died a pauper in a charity hospital in 1949. Ponzi schemes are still all-too-common today, as Robert Allen Stanford's $7 billion scheme and Bernie Madoff's even bigger $50 billion scheme have shown.

Social Engineering in the 1940s: The War Magician

Magicians are often very accomplished social engineers. They are masters of deception, manipulation, and misdirection. No history of deception would be complete without a nod to Jasper Maskelyne, also known as The War Magician. Maskelyne was a third-

---

3Stanford is a former US billionaire who is currently serving a 110-year federal prison sentence for running an international Ponzi scheme which involved selling fraudulent certificates of deposit from his offshore bank in Antigua.
12 Social Engineering in IT Security

generation magician in the United Kingdom. He worked as a stage magician in the
1930s and '40s. When World War II broke out, he joined the camouflage department in
the military, where he claimed to be responsible for some incredible feats of large-scale
deception against the Axis forces.

The story goes that Maskelyne created the illusion of a German battleship on the
river Thames to convince the British military that it could use an illusionist on the
battlefield. He used a small balloon model and a system of mirrors to conjure up the
illusion of a 61-foot-long juggernaut! The military was convinced and put Maskelyne's
skills to use. What better way to fight the Nazis than through magic and illusion!

Maskelyne was put to work for MI9 in Cairo, where he created devices that were
intended to help soldiers to escape if captured, such as playing cards that contained
maps, shoelaces with hidden wire that could saw through bars, and real currency
hidden in board games. His MI9 team reportedly smuggled almost 2,000 such devices
into German Prisoner of War camps.

During his time in Egypt, Alexandra harbor was a ripe target for Axis forces,
owing to its proximity to the Suez Canal. In a feat that beggars belief, Maskelyne
managed to hide the entire harbor from aerial bombers. He set up a full-scale dummy
harbor three miles away from the real one using canvas ships and plywood buildings.
He duplicated the light grid and harbor lighthouse. When the Luftwaffe came to
attack, Maskelyne switched the lights off at the real Alexandra Harbor and switched
them on at the fake harbor instead. The Germans fell for it. They believed they had
actually engaged in battle and won. Maskelyne encouraged the illusion by pretending
to fight back with fake shells and setting up the real harbor to look as if it had been
attacked, with fake rubble made of papier-mâché and canvases that were painted to
look like bomb craters deployed around the harbor. Maskelyne went on to hide the
Suez Canal and to allegedly mastermind Operation Bertram, to mislead the Germans
about where and when the Battle of Alamein was to take place.

Maskelyne described some of his achievements in his book, Magic: Top Secret
(S. Paul, 1949). Some of his stories have been confirmed; others have been questioned
by skeptics. They are all entertaining. Maskelyne was undoubtedly a great social
engineer; whether he put his skills to use against the Axis Forces or against a
susceptible public.

Social Engineering in the 1950s: Frank Abagnale
Frank William Abagnale, Jr. is one of the world's best-known social engineers,
thanks largely to the Hollywood blockbuster based on his biography of the same
title, Catch Me If You Can. Abagnale was a career con artist between the ages of 16
and 21, specializing in impersonation and check forgery. He excelled in using social
engineering techniques. Abagnale posed as a pilot for Pan Am Airlines to get free
flights (although he never actually flew any planes) when he was just 16 years old.
In the five short years before he was arrested, Abagnale assumed no less than eight
different identities, from teaching assistant to attorney, airline pilot to doctor. He
cashed $2.5 million in fake checks in every US state and in 26 foreign countries.
Chapter 1  Introduction to Social Engineering

Abagnale served 5 years of his 12-year sentence. Despite two attempts to escape, he was paroled on the condition that he would help the FBI to uncover other check forgers. He has since made a very successful career as a security consultant, with a reported net worth of over $10 million!

Social Engineering in the 1970s–1990s: Kevin Mitnick
Kevin Mitnick was at one point the most-wanted computer criminal in the US. Like Abagnale before him, he used social engineering from an early age. When he was just 12 years old, the young Mitnick discovered a way to get free transport on the LA bus network, which used a punch-card ticketing system at the time. He social engineered a bus driver into telling him where he could purchase the same kind of punch that bus drivers used for the transfer passes by telling the driver that he needed one for a school project. He bought his own ticket punch and collected unused transfers from the trash, which he punched himself whenever he needed a free bus ride.

When Mitnick was still in high school, some friends dared him to hack into a system called The Ark, which was used at Digital Equipment Corporation (DEC) as a development platform. Mitnick called the system manager claiming to be a member of the project team and convinced the guy to give him access to the system and select a new password. It took him less than five minutes. Mitnick did several stints in juvenile prison for various hacking-related offenses.

From the 1970s until his final arrest in 1995, Mitnick hacked into multiple organizations, including Pacific Bell, Sun Microsystems, Nokia, and Motorola, among others. Mitnick attributed much of his success to what he called social engineering, which he explained in his book *The Art of Deception: Controlling the Human Element of Security* as "Social engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology."

Mitnick served five years in jail, including eight months spent in solitary confinement. He now runs a security consulting firm, Mitnick Security Consulting LLC.

Social Engineering Since 2000
Just as the turn of the twentieth century was a golden age for con artists, the turn of the millennium has been a golden age for social engineers. Social engineering attacks have become more sophisticated and widespread in recent years. The rise of social media has provided a great resource for social engineers looking to create a believable attack. We live in an increasingly connected society where everyone is a potential target for social engineers. Many organizations have been victimized by social engineers. The next section looks at the different types of social engineers who exist today.

---

Where Are All the Ladies?

There has been no shortage of female con artists, imposters, and social engineers throughout the ages, although we don’t tend to hear as much about them for some reason. But as Beyoncé said, “Who runs the world? Girls!”

Barbara Erni in the 1700s

Barbara Erni, also known as Golden Boos, was a con artist from Liechtenstein who robbed inns across Western Europe throughout the 1700s. Erni would arrive at an inn in possession of a large trunk that she would request be locked away in the most secure room in the house as it contained valuable treasure. The valuable treasure was, in fact, a dwarf. At night, the dwarf would climb out of the trunk and pilfer the room. Erni ran the scam for decades without being caught. Finally, the law caught up with her, and she was beheaded in 1785. Golden Boos was the last person to be executed in Liechtenstein before they abolished the death penalty more than 200 years later in 1989.

The “man in a suitcase” scam is still going strong. A couple of people were arrested on an airport bus in Ireland in 2008 after passengers reported hearing noises from the baggage hold. Police found a 17-year-old youth inside a suitcase; he had a laptop and a camera in his possession, taken from the bag of another passenger. A follow-up search revealed a haul of suspected stolen goods to the value of €10,000 (approximately $14,000).

The Fox Sisters in the 1800s

The young Fox sisters of Hydesville, New York, were the unlikely founders of modern spiritualism in the mid-1800s. Soon after the Fox family moved into their new home in 1848, they began to hear mysterious rapping sounds, which the sisters claimed were messages from the spirit world and clear evidence of life after death. Two of the sisters, Margaret and Kate, discovered a way to communicate with the “spirit” that inhabited their home through a system of clapping their hands and snapping their fingers, which would, in turn, elicit more rapping sounds. They eventually learned that their resident spirit was that of a murdered peddler, Charles B. Rosna, whose remains were buried in their cellar. (In fact, some bones were found in the cellar, but not until over half a century later in 1904.) The Fox sisters became national celebrities and inspired a wave of spiritualism in the US and Europe. In 1888, Margaret revealed that they had faked it all by tying an apple to a string and bumping it on the floor or by cracking their knuckles and joints (including their toes). Spiritualism continues to fascinate people to this day, in spite of its dubious origins by the social engineering siblings.
Chapter 1  Introduction to Social Engineering

**Big Bertha Heyman in the 1800s**

Around the same time as the Fox sisters, Prussian-born Bertha Heyman, also known as “Big Bertha,” was busy defrauding (mostly) men in New York City. Bertha was dubbed the “Confidence Queen” and was described as “one of the smartest confidence women in America.” Her ruse involved pretending to be a woman of considerable means who was unable, for one reason or another, to access her fortune. To this effect, she stayed in luxurious hotels, had an entourage of servants, and wore expensive clothes. She convinced various individuals to lend her significant sums of money, including an attorney, a train conductor, a businessman, a Wall Street broker, and even her jailer when she was behind bars! She lived it up while she was in prison, using her charm on public officials to convince them to allow her to go on carriage drives and visits to the theater. They called her “The Princess.”

In his 1886 book, *Professional Criminals of America*, which profiled some 400 of the nation’s leading criminals at that time, Thomas Byrnes said of Heyman: “When plotting her schemes she would glibly talk about her dear friends, always men well known for their wealth and social position. She possesses a wonderful knowledge of human nature, and can deceive those who consider themselves particularly shrewd in business matters.”

**Dina Wein Reis in the 1900s**

Former New York socialite and con artist Dina Wein Reis scammed her victims for over a decade in her guise as the CEO of a retail distribution company. She would contact companies pretending to be looking to hire someone to replace her, and she would convince them to ship her merchandise from their current company, promising them access to lucrative markets through her completely fabricated and nonexistent “National Distribution Program.” She would sell the merchandise to a middleman who then sold it on to the end retailers. This practice is known as *product diversion*. Wein Reiss was reported to have swindled companies across the United States out of at least $20 million. She was arrested for conspiracy and wire fraud in 2008. She agreed to pay $7 million in restitution to her victims and was given a five-year prison sentence of which she would serve 31 months.

**Esther Reed in the 2000s**

High-school dropout Esther Reed is best known for faking her way into several Ivy League universities using false identities. Reed attended Harvard under the name of a friend’s sister for several years and even made it on to their debating team. She assumed the identity of a missing person, Brooke Henson, and was admitted to Columbia University. Her ruse began to unravel when police contacted Brooke’s family to let them know she had been found. When the police visited her, Reed told them that she did not want to be reunited with her family as she had been a victim of domestic abuse. The police became suspicious (among other reasons, a police

*(continued)*
investigator on the original missing-person case said that Brooke could never have gotten into Columbia) and requested a DNA test. Reed went on the run. She was finally arrested in 2008 and was sentenced to 51 months in prison followed by 3 years of probation, and was ordered to pay $125,916 in restitution. Reed’s brother was quoted as telling the police that she could argue either side of an argument and that, “She could convince you it was daylight outside in the middle of the night.” Her story is being made into a movie, The Girl Who Conned the Ivy League.

Who Are the Social Engineers Today?

We are all social engineers to some extent. Any situation in which you interact with other people has an element of social engineering in it—that’s how society functions. Some roles require more social engineering than others, such as sales and marketing professionals, politicians and headhunters, among others. There are some people, however, who will always use social engineering maliciously for their own ends.

Malicious social engineers tend to fall into three categories:

- Opportunists with little preparation and little to no budget
- Well-funded attackers with lots of preparation
- Trusted insiders

They vary in terms of the level of skill they have, the amount of preparation and resources they assign to their attacks, and the level of risk they are willing to take. Some malicious social engineers may fall into a combination of these categories. For example, a trusted insider could be someone recruited from within an organization, or someone who spends a lot of money and preparation to get a job within that organization with the intention of using social engineering techniques to access sensitive information or resources.

Opportunists with Little Preparation

Many organizations are targeted at some stage by opportunists or petty criminals who are looking to make a quick buck. This type of attacker tends to utilize an unsophisticated attack scenario and does not invest in the attack either financially or by preparing. An example could be a thief looking to steal valuables from an organization’s building (although he may steal laptops, it’s usually for their resale value rather than the information on them), or a scammer who sends out a customized blanket phishing email. It may even be a prankster playing a joke for her own or other people’s amusement. When prankster DJs fooled the Duchess of Cambridge’s maternity hospital into disclosing information about the pregnant duchess, the only preparation they did was to obtain the telephone number for the hospital. This prank is discussed further in Chapter 2 from an ethical and legal point of view.
Chapter 1  Introduction to Social Engineering

Such attackers can nevertheless be dangerous from an information security or financial point of view. As well as the potential loss of physical assets, organizations risk information on assets lost becoming public. In 2005, T-Mobile had a security breach in which the contents of socialite Paris Hilton's cell phone were published online, including her address book containing other celebrities' contact details, her personal notes, and intimate photos. This story hit the headlines in a big way. A teenager was subsequently prosecuted and sent to jail for 11 months. Reports vary on how the teenager got access to Hilton's handset, but they all include some element of social engineering. One report claims he social engineered a T-Mobile store worker into telling him a password for the firm's internal computer system. Another report claims he social engineered a T-Mobile employee into opening an email infected with a virus that allowed him to access its system. Either way, it impacted T-Mobile's reputation.

Organized External Attackers

The second category of social engineers are organized attackers who want to obtain sensitive information, make a significant financial windfall from the attack, or cause disruption to a particular target. Examples of this kind of attack include corporate espionage, organized crime, and politically motivated attacks, for example, certain environmentalist groups trying to disrupt oil or gas conferences.

These adversaries are often well funded and can afford more sophisticated attacks that take place over a longer period of time. For example, in January 2010 Google announced on its blog that it had been targeted by a highly sophisticated operation, eventually dubbed Operation Aurora by McAfee. The attackers identified employees at Google with access to proprietary data and then looked at who their friends were on social media. Rather than targeting Google employees directly, they compromised the social networking accounts of their friends and sent the Google staff messages with malicious links. These attacks were aimed at least 33 corporations, in addition to Google, including Adobe Systems, Juniper Networks, and Rackspace, who all publicly confirmed they had been targeted. The primary goal of the attack, according to McAfee, was to gain access to and potentially modify source code repositories at the targeted organizations. The attacks were reported to have originated in China and resulted in Google reviewing its Chinese business operations. Operation Aurora was clearly a very sophisticated and targeted attack that involved a lot of preparation and research, rather than just sheer opportunism like the previous T-Mobile example.

Internal Attackers

Insider threats to information security are a serious problem for organizations. Even the NSA is not immune to insider security breaches, as former employee Edward Snowden demonstrated when he leaked information about the NSA PRISM program, making headlines around the world. Insiders working for an organization already have a great deal of information about how the organization operates. They know where sensitive information is kept and the processes and procedures for how to access it. They already have authorized access to internal systems and to the building itself. Insiders know where the soft spots are.
18 Social Engineering in IT Security

An insider attack can be undertaken by insiders in various roles:

- Someone who has physical access to the building with authorized access to IT systems, such as a disgruntled employee
- Someone who has physical access to the building but no access to IT systems, such as a cleaner
- Someone who has physical access to the building but limited access to IT systems, such as a third-party contractor
- Someone who has already gained unauthorized remote access to the IT systems

Introduction to Social Engineering Testing

Social engineering is a huge problem for organizations today. Performing a social engineering test is an extremely worthwhile exercise to improve defenses against malicious social engineers. A social engineering test can

- Test the effectiveness of physical and logical security controls and provide recommendations on how to improve them
- Test the level of and even improve security awareness among staff
- Give staff practice at identifying the techniques that social engineers may use and at learning how to deal with social engineering situations

However, knowing how to conduct a social engineering test can be difficult, as a number of challenges are involved. How do you create an effective scenario? What are you allowed to do from a legal perspective? How do you report on a social engineering test? This book will teach readers how to perform an ethical social engineering test using a repeatable social engineering test methodology.

The Social Engineering Test Methodology

The social engineering test should be approached like any business project and the methodology is largely reflective of that used for penetration tests. The social engineering methodology has five phases, as shown in Figure 1-1. It starts with project planning and target identification, moving through to research and reconnaissance, scenario creation, and finally to attack execution and reporting. This methodology can be tailored for each test and no two social engineering assignments are the same. The purpose of the methodology is to design social engineering tests that are systematic, repeatable, and consider the legal and ethical implications of the actions taken.

In the planning and target identification phase, you work with your client to identify who or what you will or will not test, when you will run the test, and how you will go about it. The objective of this phase is to define a project plan with clear goals that have been authorized by the appropriate people. It includes the following activities:

- Threat assessment
- Scoping the test and setting goals
Chapter 1  Introduction to Social Engineering

1. Planning and Target Identification
2. Research & Reconnaissance
3. Scenario Creation
4. Attack Execution and Exit
5. Reporting

FIGURE 1-1  The social engineering testing methodology

- Project planning
- Defining the rules of engagement

The research and reconnaissance phase involves gathering as much information as possible about your target in the time you have allowed within your budget for this phase. If you are doing a physical test, you visit the location you are targeting to gather information about it. What time do people arrive for work? Are there any unofficial entrances, fire escapes, and so forth? For remote tests, the research and reconnaissance phase involves gathering information from publicly available sources such as corporate websites, social networks, and newspapers.

You use the information you have gathered through your research and reconnaissance activities to create a plausible attack scenario, in the scenario creation phase. In this phase, you design the back story that gives you a reason for requesting the information or access that you are seeking. Your scenario will be used to convince your target to comply with your request. To create a good scenario, you brainstorm potential scenarios and choose the one that is both achievable and most likely to succeed. You develop the scenario further and practice, practice, practice until it is time to execute the test.

Executing the test is the most exciting phase of the social engineering test methodology. The execution phase for a remote attack in which there is no real-time interaction (such as a phishing test) is relatively straightforward—you lay the bait and
wait for your victim to respond. It gets more complicated as soon as you start having
direct real-time interaction with your target, for example, over the phone or in person.
You play out your scenario to attempt to gain access to the information or resources
that you are targeting. Then you attempt to exit the execution phase without alerting
your target that they have been social engineered.

Reporting on your social engineering exploits can seem rather dull after the
excitement of the test itself, but it has to be done. The report is the deliverable that
your client receives from the project. Your report is likely to consist of two sections:
the executive summary and the technical details (methodology used, timeline,
findings, and recommendations). As you are writing your report, keep the audience
for each section in mind.

How Much Information or Levels of Access Should
Be Provided for the Social Engineering Test?

When you are planning a social engineering test, you will need to decide how much
information the testers will receive and what level of access they will have to perform
the test. First, like a penetration test, a social engineering test can be performed with
varying levels of knowledge about the target, from a black-box test where the testers
know nothing about their targets to a white-box test where the testers have a deep
understanding of how the target organization works. Usually, social engineering tests
are performed as gray-box tests, with some information, such as contact details or
floor plans, provided in advance in the interest of saving time and money.

Second, the level of access the social engineering testers will have depends on
what role the social engineers will play. Social engineering tests can be done from a
variety of perspectives, including

- That of an outsider who is a stranger to the target organization
- That of a third party who has limited access to the organization
- That of an internal employee

Keep in mind, however, that even internal employees have varying levels of access
within an organization.

Your social engineering testers will work with you to decide which is the most
appropriate perspective to perform the test from and what kind of information should
be provided in advance. Chapter 4 covers planning the social engineering test.
Final Thoughts

Defending against malicious social engineers is becoming more difficult. Their attacks are becoming more targeted and more believable, which is exactly why we need to understand how social engineers operate. We need to educate ourselves and our colleagues and start thinking like social engineers. We need to get into the mindset of social engineers, understand what drives them, and how they can use our information against us. We can't predict every attack. And we can't issue patches for social engineering. But by thinking like a social engineer, we can detect where some of our vulnerabilities lie and better defend them.

You can be the person who stops the social engineering attack from being successful. You can refuse to give information over the phone; you can opt to not visit that link; you can question the person who followed you into the office. To defend against social engineers, you need to understand how they operate. Consider the following questions:

- What would be a social engineer's motivation for targeting your company?
- What would a social engineer want to steal?
- What would the social engineer's likely budget and skill set be?
- How might the social engineer get in?

Now read on while keeping these questions in mind.