7 Deception Is the Intent of Social Engineering

LEARNING OUTCOMES

After completing this chapter, you should be able to:

- Define the term "social engineering" and learn who the attackers are and whom they are targeting in their attack.
- Study the tactics, techniques, and procedures (TTPs) of social engineering attacks.
- Discuss how TTPs are inserted into phishing, spear-phishing, ransomware, and other targeted attacks on people, computers, and networks.
- Identify the particulars of extortion-based email scams and learn crime prevention tips related to these kinds of attacks.
- Assess the design of malicious websites and investigate how attackers exploit trust to deceive website visitors.
- Explore where and how social engineers learn how to attack.
- Compare key recommendations for building awareness of social engineering attacks and how to prevent them.

Using Emotions to Manipulate Human Behaviour

Social engineering attacks are one of the greatest problems facing law enforcement today. A social engineering attack targets human behaviour, trust, and the emotions of the victim. These attacks manipulate and overpower a victim's good judgment. Social engineering has been around for many years; however, because of the Internet, these attacks have become much more sophisticated and targeted.

Essentially, attackers understand that people are inherently trusting and that they want to help others and do good things. Because of this, social engineers often ask for help, and their victims respond, willingly entering into the social engineer's deliberate and deceitful trap. Some victims respond less altruistically and will enter into a scam because they believe it will benefit them.

wire fraud
A scheme to defraud or obtain money based on false pretences using electronic communications.

The term "social engineering" was coined by Kevin Mitnik, a notorious computer hacker who committed **wire fraud** and subsequently served five years in jail. Mitnik was a prolific social engineer who said it was all about "gaining access to information that people think is innocuous when it isn't, and then using that information against the real target. People are the weakest link, not technology." He went on to say, "You can have a teenage kid who is using social engineering to get into his friend's AOL screen name or you can have a military spy using it to try to break in somewhere, and everyone else in between. Social engineering is simply a tool used to gain access" (Mitnick and Simon, n.d.).

spoof
The ability of a person or program to masquerade as another by falsifying data.

The tactics, techniques, and procedures (TTPs) employed in social engineering have become more seamless because of the Internet. Under a cloak of anonymity, attackers can **spoof** a telephone number, an identity, or an email address. They can entrap victims on a global scale, communicate on the Dark Web, and, through underground forums, share information with other threat actors and learn new techniques. Social engineers are greedy fraudsters who expertly take advantage of emotions such as fear, empathy, loneliness, generosity, and greed to insinuate themselves into the everyday functions of people as they go about their lives: banking, falling in love, gambling, donating to charity, and being gainfully employed. Their attacks are so effective that, frequently, even with evidence of the crime, their victims do not believe they have been scammed.

This chapter examines social engineering attacks from many different angles and explores attacks related to cybersecurity and cybercrime. We discuss how social engineers select their target and plan their attacks, and we describe how the TTPs are positioned in the attack. This chapter will increase police officers' knowledge of social engineering and familiarize them with these attacks so that, if they do respond to an incident, they will recognize right away when

it involves social engineering. Finally, we discuss the frequency of social engineering attacks and how police officers can build awareness of them to help prevent their spread and the potential damage they cause. By being aware, diligent, and somewhat skeptical, the public may begin to understand the harm social engineering attacks can cause and how they can impact the lives of people, businesses, and organizations online and offline.

What Is Social Engineering?

Social engineering is a technique that takes advantage of natural social interactions in life. It manipulates trust in an expert ploy to trick victims into doing things against their better judgment. Social engineering targets victims online, over the phone, and face to face. The victims sometimes do not even realize that they have been deceived. "Amateurs hack systems, professionals hack people," says Bruce Schneier, a cryptographer, a computer security professional, a privacy specialist, and the author of *Secrets & Lies: Digital Security in a Networked World* and many other security books (HelloTDS, 2018). Mr. Schneier has spoken numerous times about social engineering at an annual hacking convention called DEF CON. Held every August in Las Vegas, this convention attracts hackers, federal agents, police officers, and security professionals of all ages. Each year, the convention holds a contest to test the social engineering skills of attendees. Many of these exploits are found on the Internet and have become legendary. Of course, many of these techniques are tested on attendees of the event, which makes it the perfect forum to learn how powerful these attacks can be.

Attackers understand that people are the weakest part of any security program. In fact, although human qualities may help form some of a company's greatest strengths, people are often considered to be "low-hanging fruit" because they can be compromised with very little effort. Attackers often appeal to their target's feelings because they know that emotions such as fear, empathy, and love and a sense of urgency can be incredibly effective in manipulating people online. A person's trust is often used against them because their willingness to believe is even stronger than their common sense, which, under normal circumstances, favours security. Victims may look for a reason to believe the scammer because they want to get in on the scam so much. Victims may also become emotionally invested because of a simple connection they have made with the scammer that makes them feel worthy of the special attention they are receiving. Essentially, this is why social engineering attacks are so successful. By nature, people want to trust others, and they also want to help. The combination of these two qualities is often what makes people great, but it is also what makes a security program weak. Attackers leverage the good qualities in people to execute bad intentions.

CEO fraud
Occurs when a cybercriminal pretends to be a CEO and sends an email to staff members trying to trick them into providing information or doing something; also known as business email compromise.

US Federal Bureau of Investigation (FBI)
The domestic intelligence and security service of the United States and its principal federal law enforcement agency.

A good example of this is the **CEO fraud** scam, also known as business email compromise. These attacks generally do not cost a great amount of money because attackers use email, SMS text, or the telephone to contact their targets. Recently, the **US Federal Bureau of Investigation (FBI)** warned of a 270 percent increase in CEO fraud, estimating that this scam has cost organizations more than US$2.3 billion in losses, with reports coming from many countries over the past several years (Krebs on Security, 2016).

In this scam, an executive assistant or someone close to the CEO is typically the target. Attackers understand that the assistant holds the "keys to the kingdom"; they have knowledge of valuable assets, such as schedules and credit card numbers, and they also know about family relationships, activities, interests, and travel plans within the organization. This is all extremely valuable information if, for example, it pertains to a multibillion-dollar organization. Assistants to CEOs are also known for their competence, their willingness to help, and their ability to get things done in a timely manner.

Consider the following example. It is a typical Monday morning, and the CEO is out of the office. An email, apparently sent by the CEO, is sent to the CEO's assistant with the subject line "Urgent Attention." The attacker may have conducted **reconnaissance** on this company or on the target beforehand and may have used either phishing or spear phishing (see Chapter 8) to gain access to the CEO's inbox. The attacker may be emailing from a look-alike domain name or one that uses **typosquatting**, or **cybersquatting**.

reconnaissance
The activity of obtaining information in advance to gather information about vulnerabilities.

typosquatting (cybersquatting)
Altering a name or brand name with the intent to target Internet users who incorrectly type a website address into their Web browser.

In typosquatting, attackers will register a domain that inserts, for example, a number "1" in place of the small letter "l" and will send messages from that domain. It takes a keen eye to spot the discrepancy, and the spoofed email from the CEO may not get caught in a spam trap. In some cases, the CEO may have had their inbox compromised while using an insecure wireless network while travelling. Regardless of how the inbox was accessed, once inside, the attackers will search for key words that demonstrate common business practices and that are used in the workplace, such as "transfer" or "deposit."

In this case, the email continued with a message from the CEO that an international payment needed to be made immediately. The assistant responded in the affirmative but did not hear back from the CEO until the end of the day. The incoming email said, "It has been busy, but can you still handle this right now?" The CEO fraud tricks the victim into responding to the urgent request, and the fraudster tests the employee's loyalty and ability by asking if the payment can be made immediately. When an email looks and sounds authentic and is written in the voice of the CEO using common words and phrases, then it becomes even more dangerous. The victim is ready and able to do just about anything the CEO asks, even wiring thousands of dollars to an account in another part of the world. Attackers thrive on well-intentioned employees, such

as those holding key positions within a company, and this is one reason why CEO fraud is so effective.

Social engineers use employees as a conduit to gain access to a network. They may approach gatekeepers, such as the executive assistant, first; however, they may also approach other employees who guard the company's secrets and assets. Even though organizations commonly incorporate layers of security, such as real-time threat detection, visualization tools, and firewalls that protect their computer network, they may not be enough. To gain access to a network, it may just take a carefully crafted spear-phishing email sent to a privileged person in the company and asking them to sidestep standard security practices in order to get a response to a convincing request for assistance.

How Does Social Engineering Work?

Attackers use **pretexting**, a term that is commonly used in the area of cybercrime to describe a fake story that is advanced to help them gain acceptance by a person or an organization. Pretexting is an important practice used in social engineering attacks as it enables attackers to use information that the victim gives to them to help legitimize their story ("What Is Pretexting," n.d.).

pretexting
The use of a fake story by attackers to legitimize their story and be accepted by a person, a business, or an organization in order to obtain information.

Letter scams are common on the Internet and employ a variety of social engineering TTPs, including pretexting. They are often categorized as advance fee, romance, inheritance, lottery, and phishing scams. They often involve sophisticated and malicious, deceptive techniques that trick their victims into voluntarily revealing personal information, sending money, or agreeing to participate in an elaborate business deal or a "get rich quick" scheme. Frequently, these letter scams result in connections and relationships that lead to the attacker and the target meeting in the real world. Unfortunately, the risk in these cases sometimes involves young people, whose better judgment can be mired in dreams of becoming rich and famous and who can be more secretive and willing to take risks.

A dangerous situation illustrating this type of scenario occurred in early 2017, with a letter scam promising a young woman the opportunity of a lucrative modelling contract. The attacker convinced the young girl to accept a lucrative offer of $15,000 and a free flight to Atlanta, Georgia, if she would help him by modelling for his photography portfolio. The attacker enticed the victim to travel to the United States to sign the deal. After he picked her up at the airport, he took her to several hotels and subsequently to his mobile trailer home in an isolated rural community in South Carolina. Over the course of several days, he physically restrained her, forced her into oral sex, and sexually assaulted her multiple times. During this time, the woman was able to take snapshots and secretly send them and coded messages to her parents via FaceTime, which police used to track her whereabouts via cellphone location

services. Officers were dispatched to the mobile home, and, as they arrived, the young woman threw herself out of the front window, sustaining an injury, but was saved by police. The attacker was criminally charged with kidnapping, first-degree criminal sexual conduct, and possession with intent to distribute methamphetamine. Although the victim was brought back safely to Alberta, the entire incident clearly illustrates that social engineering used with solid pretexting stories can be effective and can convince people to do things that they know run counter to their better judgment (Anderson, 2017).

Microsoft tech support scam
A massive global scam that tricks people into believing that their computer needs to be fixed and entices them to pay for technical support services.

Phone scams such as the **Microsoft tech support scam** have also been very effective over the years and have caused a great deal of trouble for law enforcement on a global scale. They also cause problems within the tech industry, primarily Microsoft, possibly because of its large footprint in the tech market. The role of the police in dealing with these scams has fundamentally been one of cybercrime awareness and online safety rather than investigation and enforcement, primarily because the perpetrators operate from locations all over the world.

These scammers telephone people randomly using a spoofed phone number. They surprise the victim by pretending to be from Microsoft or another software security company, shocking the victim when they announce that they can see that their computer is infected with malware. They build fear in the victim by using a serious tone of voice and attempting to sound professional. The caller will direct the victim to a "free" service on their website that will quickly save the victim from all kinds of problems if they visit it and install an application. Relieved, the victim gives the attacker **remote access** to their computer. Once they have control of the victim's computer, they display fake error messages and display pop-up messages that won't go away, essentially locking the browser. This triggers the victim even more and prompts them into quickly acting to fix the problem.

remote access
The ability to access a computer from another—for example, the ability to connect to a home computer from another location.

These calls essentially frighten victims into paying for "unnecessary technical support services that supposedly fix contrived device, platform, or software problems" (Microsoft, 2019). Essentially, the victim is tricked into paying for fake solutions to fake problems. Victims commonly provide attackers with their credit cards, and, in general, the entire scenario places the victim at greater risk of identity crime and fraud. When police respond to these incidents, they should advise victims to change their passwords and immediately contact their credit card provider to reverse any charges paid to the scammers. They may even recommend that the victim have a security checkup conducted on their computer and report the incident to the Canadian Anti-Fraud Centre.

Who Are the Social Engineers?

It is difficult to specifically define who the social engineers are; they could be anyone. These people or groups range from simple opportunists to very sophisticated

members of organized crime. Social engineering is commonly associated with hacking, an activity in which people or groups attempt to gain access to computers, networks, or information that they are not authorized to access.

Hackers use TTPs to break down or bypass security measures and gain unauthorized access to computers, devices, and networks. In general, hacking is illegal if it is done without the owner's permission. There are three common forms of hacking: white hat, grey hat, and black hat. Generally, white-hat hacking is associated with paid employees or contractors working to look for holes or vulnerabilities in a network. Grey-hat hacking involves people who access networks without the owner's permission or knowledge but will report issues to the owner when or if they find vulnerabilities. A famous hacker who has been described as both a white-hat and a grey-hat hacker is Stephen "Woz" Wozniak, the co-founder of Apple. While attending university, Wozniak bypassed the phone system, which allowed his friends to make free long-distance phone calls. During this time, Woz made a name for himself by allegedly using one of these devices to call the Pope ("Top 10 Most Famous Hackers," 2009). Another famous grey-hat hacker is Gary McKinnon, a computer nerd who began hacking when he was 14 years old. McKinnon is known to have illegally infiltrated close to 100 US military networks, where he left a message on their system reading, "your security is crap" ("Top 10 Grey Hat Hackers 2018," 2017). Black-hat hacking, on the other hand, entails acting with malicious intent by writing malware, causing damage, stealing information, and leaving the network vulnerable to future harm. One famous black-hat hacker is David L. Smith, the author of the Melissa worm virus. This virus, distributed via email, caused over $80 million worth of damage to businesses and organizations ("Top 10 Most Famous Hackers," 2009). But possibly one of the most famous black-hat hackers is Canadian Michael Calce, otherwise known as Mafiaboy. At 15 years of age, Mafiaboy hacked into several large commercial websites and committed a series of denial-of-service attacks against eBay, Amazon, and Yahoo. He caused $1.7 billion worth of damages and was arrested but, likely due to his age, spent only eight months in a probation centre. He is now working as a cybersecurity consultant (Hetherington, 2018).

Social engineering techniques are also used by international fugitives or terrorists to avoid custody. They use TTPs to share information, recruit people, build networks, and transport weapons for terrorist activity. In some cases, hacking is state sponsored, and the actors use TTPs to conduct espionage—that is, spying in order to gain state secrets. Similarly, state-sponsored attacks are launched for financial gain. Take, for example, a prolific hacking group called APT37, which stole US$81 million from a bank in Bangladesh in 2016. A security firm named FireEye was able to track the malware deployed by APT37 to its targets and then trace this activity back to its source, the North Korean government (Greenberg, 2018). Another North Korean hacking group,

Lazarus, used social engineering, malware, and spear phishing to gain access to information and computer networks to steal US$571 million over the course of 14 hacking attacks on cryptocurrency exchanges in 2017 ("North Korean Hackers," 2018). Hacking has also been widely associated with aspects of organized crime, such as drugs, human trafficking, money laundering, illegal gambling, extortion, counterfeit goods, and cybercrime (Royal Canadian Mounted Police, 2014).

What Are the Tactics Used in an Attack by Social Engineers?

Social engineers invest a great deal of time and effort into perfecting their skills. The more they practise, the more deceptive they can get. As stated earlier, social engineers often conduct reconnaissance on people in positions of power and privilege or on the people closest to the target. They may research social media or look for organizational charts that offer valuable information about key positions in a company. They frequently conduct open-source intelligence gathering in social media, such as LinkedIn, Facebook, or Twitter. These websites encourage the sharing of personal and confidential information, such as favourite holiday locations or business and family relationships. By scraping together useful tidbits of personal information and understanding relationships within companies, fraudsters can build a more informed and convincing attack.

In some cases, attackers will make phone calls or visit a company to test its security protocols, which may include testing how the company handles guest visits. Attackers might make phone calls pretending to be a co-worker, such as someone from IT support, to gain access to a company and speak directly to an employee in an attempt to gain remote access to their system (Goodchild, 2018). Many office buildings use a visitor's pass system, but gaining access into a secure office or a building could be as simple as taking advantage of smoking areas or busy doorways, where the attacker can slip back into the office with a legitimate worker.

email naming convention
The process of standardizing email addresses to ensure that new email addresses for each person or employee are unique.

Attackers may also try to learn the **email naming convention** within an organization. This convention is a set of rules that apply to the creation of email addresses within an organization. With only an employee name and knowledge of the naming convention, an attacker can directly email any employee in the company.

Common naming convention rules start with standard email address formation, and, depending on the size of the organization, the rules become increasingly complex. For example, an email rule might start with standard address formation, such as "firstname_lastname@yourdomain.com" or "lastname.initial@company.com." This is an important point in social engineering

attacks because attackers typically target the most common business practices, and most companies still use email. With very little effort, an attacker can obtain the target's cellphone number from the signature line in a return email. With an email, a cellphone number, and personal and professional knowledge about a potential victim, the attacker can carefully craft and direct messages to that person. They may then use the following common tactics:

1. *Emotional manipulation.* Often the subject line or content of an email will contain words that produce an emotional response in the recipient. For example, this subject line tugs at the heartstrings of those who wish to help after a natural disaster: "It didn't happen to you, but it could have. Help those less fortunate by just sending $5. Just provide your credit card, and we will donate $5 to those less fortunate." Other common emotions used include anger, officiousness, love, disgust, fear, guilt, excitement, urgency, greed, sadness, or surprise.
2. *Professional materials.* Social engineers have the ability to present professional-looking business cards, badges, and brochures to help corroborate their story. Business cards are very inexpensive and are commonly used at conferences, where attackers may target their victims around the dinner table or in smoking areas. Uniforms and badges are also used by fraudsters and are readily available for purchase on the Internet.
3. *Well-crafted scripts.* Social engineers frequently use well-researched scripts to help build their pretext and practise answers to questions that potential victims could ask. They might use apps that provide background noises such as babies crying, traffic noises, or warehouse sounds to reinforce their storyline. Attackers are making fewer spelling mistakes and grammatical errors in emails than in previous years; therefore, this is not always a clue to a phishing attack. Attackers can access templates and logos to help corroborate their story. They may have conducted an open-source investigation on a company or region and could be well informed about the victim's physical surroundings or political leanings, for example.
4. *Timing.* Social engineers know that when certain events occur, there is an opportunity to take advantage of them. Scams surface at tax season, after natural disasters, before concerts or major sporting events, and at other newsworthy events when people are excited, sad, anxious, or distracted. Political campaigns often attract spear-phishing attacks (discussed in greater detail in Chapter 8). Attackers focus on tragedy, such as the fire at the Notre-Dame Cathedral in

Paris in 2019, when people were upset and were looking to quickly support any effort to help people, the cleanup effort, and the restoration of the church ("Fraudsters Exploiting," 2019). At these times, social engineers will create fraudulent donation websites and send email links to visit the fake site or will distribute spam asking for donations and credit card numbers.

5. *Friendly demeanour.* Social engineers can be friendly, outgoing, and humorous. They can carry on a conversation, and in cases of romance or vehicle sale scams, they are very responsive to the victims by frequently sending photos or messages of affection and offers of service.
6. *Impersonation.* During an attack, social engineers will impersonate businesses, charities, or causes and will not hesitate to change their persona or anonymize their identity to deceive victims. Attackers will commonly work in teams with other fraudsters to make themselves available day and night.

What Are the Common Techniques Used in Social Engineering Attacks?

Social engineers use several old and new techniques to steal personal information, obtain credentials to a network, or trick people into handing over their credit card number, for example. The following are some of the most common techniques used in social engineering attacks:

1. *Advance fee scams.* These scams use social engineering techniques based on emotions of excitement, greed, and the thrill of the sale. In these scams, attackers send the target more money than was expected from a sale, using a stolen cheque or a counterfeit money order. The attacker will then make an excuse to ask for a certain portion of the money to be returned. The good-hearted, honest victim will refund money back to the attacker, only to find out later that the cheque was a fraud.
2. *Baiting.* Baiting is often used as part of a social engineering attack. It commonly occurs on gaming sites, in peer-to-peer networks, or in social media. In peer-to-peer networks, attackers may wait for an opportunity or follow a target until such time that they can make a friendly offer to share information, steal credentials, or help them. A form of baiting that makes use of a USB drive is similar to the legend of the Trojan Horse. In a modern-day cyberattack, however,

peer-to-peer network
A computing or networking architecture that partitions tasks or workloads between peers, who are equally privileged participants in an application.

the victim is tricked or baited into plugging in a USB device that has been infected with malware. As one of the most commonly retold stories goes, infected USBs were scattered in a parking lot, and after finding them, curious employees subsequently plugged the USBs into their computers to find out what was on them (Nichols, 2016). Baiting may also occur when targets are enticed into downloading pornography or opening links that could infect the network with malware.

3. *Conversion theft.* This social engineering technique is commonly used these days because more people than ever are buying items online and having them delivered to their home. Conversion theft typically occurs when social engineers redirect the delivery of the product to somewhere other than the intended location.
4. *Fraudulent websites.* These scams involve registering websites to defraud people by selling goods and services that are never delivered. The perpetrators collect personal or financial information in order to commit identity theft, or they commit theft by convincing victims to wire money. Scammers may also sell "fictional" vehicles, or counterfeiters set up websites to sell fake designer and knockoff luxury brands at very low prices.
5. *Honeypots.* Traditionally, honeypots are associated with sexual seduction and romantic or sexual relationships. This common technique may be used to attract a person for sextortion, blackmail, or ransom. It may also be used to build a relationship with the goal of obtaining secrets, money, or sexualized photographs from a victim.
6. *Phishing.* Phishing incorporates social engineering tactics into an email or SMS text, with the attacker masquerading as or acting like a trustworthy entity, such as a bank, a retailer, an Internet service provider, or a charitable organization. Phishing is very prolific and can affect millions of recipients at a time through spam. Often these messages use emotions to trick recipients into sending money or bait them into clicking on a link that is infected with malware. The content of these emails is designed to entice the recipient into giving out their credentials or directs them to a webpage or website where their credentials are required. The website they subsequently visit may also be infected with some type of malware.
7. *Quid pro quo.* In this technique, the victim is offered a benefit by exchanging information for something in return. For example, the attacker will promise a quick fix in exchange for the employee disabling the company's antivirus program. This has been used for

many years with the tech support scam that offers solutions for "computer problems that only they can see" and asks for payment in the form of a one-time fee or subscription for their ongoing support service.

8. *Rogue websites.* These websites are set up to simulate authentic websites; however, they sell fake software and antivirus programs, which the victim pays for by credit card. Rogue websites claim that their programs remove malware or prevent viruses from entering the network.

9. *Spear phishing.* This technique is similar to phishing; however, as noted above, it is more targeted, and attackers generally conduct reconnaissance in social media prior to sending or texting a message to a privileged person within a corporation or business. The perpetrators use well-crafted material to deceive the target. The target trusts the sender and responds out of a sense of urgency, surprise, fear, empathy, or greed.

10. *Tailgating.* This technique commonly occurs in the physical world in office towers, in large businesses with many employees, or in businesses or organizations with connected underground parking garages. The attacker will hang around an elevator or entrance door and slip inside when employees enter the workplace. They may use the pretext that they forgot their access card or keys and just need to quickly return to their desk. Many employees don't feel qualified to challenge unknown people in the workplace, so attackers prey on them, knowing that workers are often busy and distracted. Attackers have been known to use high-end photography to print badges that appear genuine. If attackers enter these workplaces, they will pick up laptop computers, jackets, wallets, or papers lying on desks. If challenged, they will quickly leave under the pretext of being lost or on the wrong floor.

11. *Watering hole attack.* This type of cyberattack takes advantage of websites that people regularly trust and visit, particularly when the target is associated with a certain industry. For example, a police officer may receive an email inviting them to visit a website that sells tactical clothing or hunting supplies. The link may be infected with malware or may take them to a website where malware is located. In either case, the malicious link may introduce a threat to the network ("Social Engineering," n.d.; Thornton, 2018).

routing transit number
A nine-digit number used to identify a financial institution in a transaction.

SWIFT (Society for Worldwide Interbank Financial Telecommunication) code
The popular term for a bank identifier code, an 8- or 11-digit code that identifies the country, city, and bank branch.

Case Study

An Online Car Swindle Is Uncovered Just in Time

One day Jason decided that he would like to buy his wife a new car. They had been thinking about it recently, and Jason finally decided to take some steps to find one. He had set his sights on a high-end vehicle called a Porsche Panamera. This vehicle was highly rated in many car magazines, and Jason thought his wife would love driving it. Jason wanted to surprise his wife for her birthday, so he started looking for one available anywhere in Ontario. With no luck at first, Jason was thrilled to finally find one offered for sale on a flashy website called "Ultimate JR Motors." Jason checked the website closely, viewed all the testimonials, and read about the owner named Frank. Jason was impressed by all the positive testimonials indicating how service-oriented Frank was. Some of the comments mentioned by customers indicated that they had bought cars such as Ferraris and Maseratis in the past from Frank, and his service was so good they were thinking about buying a second one. Jason was relieved that he could reach Frank on his desk phone, cellphone, and fax and through an online contact form.

Jason had never bought anything as expensive as a car online, but he decided to give Frank a call to ask him questions. Frank personally answered the phone on the first ring each time Jason called, and he was friendly, helpful, and very knowledgeable about Porsche Panameras and other high-end vehicles. Jason felt very fortunate to find out that Frank had only one left in stock, likely the last one available in North America, and was willing to sell it to him. Jason agreed to the selling price, US$58,000, which was a really good deal compared to the $125,000 it was selling for in Canada. Frank sent Jason a professional-looking invoice with his logo, bank name and address, bank account number, **routing transit number**, **SWIFT code**, business location, and bank fax number. Frank directed Jason to promptly wire the money to close the deal. All Jason had to do was pick up this luxurious new car in Dallas, but Frank was going to help with this detail as well.

Before wiring the money to Frank, Jason decided to ask a friend for advice about the deal. The friend suggested that Jason hire someone to visit the shop to inspect the car. Jason thought this was a good idea, so he quickly found a person in Dallas, paid him $250, and asked him to visit the shop that was pictured on the website. This fellow went to the shop, saw cars parked around the building, knocked, and spoke to a person who said there was no Porsche Panamera on the property and no person named Frank worked there. The swindle was uncovered just in time.

Debrief

Jason was relieved to learn that he avoided being defrauded. This would have devastated him financially. Jason stated that he really liked and trusted Frank. Although he was happy to pay $250 for a vehicle inspection, he said he would not have paid $500. Nevertheless, Jason was ready to wire US$58,000 to Frank because he trusted him. A subsequent investigation conducted on the website Ultimate JR Motors determined that the registrant for the website was not Frank but someone with the email address "DonaldDuck123@hotmail.com." That person's home address led to a house for sale, and the phone number on the website domain belonged to the state's probation department. Essentially, the entire website was a well-crafted scam with an impressive, interactive design intended to foster trust in its visitors. Frank built on that trust by using deceit and pretexting and

by presenting a friendly personality that preyed on victims by providing exactly the circumstances that the victim was looking for. He was also patient enough to wait for the right victim and the perfect situation. Jason subsequently reported the fraud to the Internet Crime Complaint Center (IC3), a fraud prevention and investigation agency in the United States.

The information in this case study is derived from the author's interview with the victim. "Jason" is a fictional name. Ultimate JR Motors is no longer in operation.

DISCUSSION QUESTIONS

1. List four tactics used in social engineering attacks.
2. Explain what an email naming convention is and how a person would identify one.
3. What is the difference between phishing emails and spear-phishing emails?
4. List four types of information about a target that social engineers would try to find.
5. What is the term that describes when a product is delivered somewhere other than to the intended location?
6. List five techniques commonly used in social engineering attacks.

What Does a Social Engineering Attack Look Like?

Intent defines social engineers; their attacks are primarily waged for psychological manipulation, and their motivation encompasses criminal, political, and financial gain. In some cases, social engineers will attack because they wish to satisfy their egos or gain peer recognition, as in the case of grey-hat and black-hat hacking. Sometimes attackers are simply disgruntled employees who are dissatisfied with their organization and wish to do it harm.

Several years ago at DEF CON, the annual hacking convention mentioned earlier in the chapter, a Canadian won the social engineering contest by convincing a Walmart employee that NATO needed help in the event of a pandemic. In the course of a 20-minute telephone call, the caller obtained 75 key pieces of information about Walmart's security program, how much employees were paid, who provided IT support, and what computers, operating systems, and antivirus programs are used by the mega-retailing chain (McDiarmid, 2012).

Any kind of incident that an officer responds to in their regular duties may involve some kind of social engineering. The following case study is another example of the kinds of TTPs used in an attack.

Case Study

Victims Often Ask, "How Did This Person Get My Password?"

Susan walks by the river every day as part of her fitness schedule. She typically sees a few people walking and biking along the route, and one day a well-dressed, middle-aged man stopped his bike and asked her for help. He mentioned he was a tourist from Europe and needed Wi-Fi for his cellphone to make an urgent call. Instead, Susan agreed to let him borrow her phone for a few minutes. When he was done, he handed back her phone, and she never thought about it again until a few weeks later when she received an email. Susan thought back to that day, became upset with herself, and could not sleep that night because she was so worried. The email read as follows:

> **From:** Johnxxx (mailto:xxxxx@outlook.com)
>
> **Sent:** November 13, 2018 5:11 PM
>
> **To:** Susanxxx
>
> **Subject:** - shadow
>
> Btw, I actually know the sneaky secrets of your life. I will not explain you just what exactly I know, I've every piece of information along with me.
>
> To prove my point, please let myself say to you that one of your security passwords is shadow. Pay me $8000 via Bitcoin to the address 1M7VCVpDaQjuuqBJ1Lz9iWTBF-2GRgkaqi within the next 48 hours. I will make one thing clear, that I will damage your life totally if I do not get the payment. If I get the payment, I'm going to remove each and every info I have with me, and i'll go away and you will definitely don't ever hear anything from me.
>
> This is actually the first and also last mail from me and also the offer is non negotiables, and so do not answer to this email.

Debrief

The first issue to consider was that the tourist's request to borrow Susan's phone may have been completely innocent—or it may have been a scam. Susan may never know for sure, but she was worried and, looking back on the situation, wondered how this person could have gotten her password. It turned out that it had nothing to do with the email she later received, but the timing was alarming. Susan's intuition tells her that giving a stranger access to her cellphone during a chance meeting was not a good idea. She tells herself that this fellow seemed so nice, and although it seemed like a good idea to lend her phone to him at the time, it was against her better judgment. This scenario clearly demonstrates that good people respond in risky ways when asked for help.

In this case, the email was a scam. This kind of letter is called an extortion-based scam. When sex is used in these letters, they are known as sextortion scams. The email clearly employed social engineering tactics, including fear, surprise, and urgency. The attacker was preying directly on Susan's emotions. When she received this email, she was afraid and immediately feared that the stranger on the bike had access to her entire personal online life. She had used "shadow" at one time as a password, but that had been years ago. She wondered how the fellow on the bike found this out. Susan was ready to send the extortion money until she spoke to a police officer, who informed her that this was a scam.

Essentially, these attackers do not have access to emails, accounts, or anyone's "sneaky secrets." They have not installed malicious code on the victim's computer; however, they would like the victim to believe that their every keystroke is being captured. In these scams, the perpetrator has likely obtained a password from an underground forum following the breach of a company's database. The attackers draw directly from countless usernames and passwords found on the Dark Web or traded in hacker forums. By simply entering Susan's

email address into the website haveibeenpwned.com, it was quickly determined that her email and password had been compromised on four websites that had been breached in the past. Perpetrators can use a variety of means to obtain or crack a password, which they then use in an email to send to their targets. The victims often ask, "How did this person get my password?" These scare tactics are being used more and more often to bait recipients into sending the attacker extortion and blackmail money via Bitcoin because they believe so strongly that the perpetrator has access to their private information.

The information in this case study is derived from the author's interview with the victim. "Susan" is a fictional name. An email similar to the one provided in the case study was shared with the author.

When police officers respond to a complaint like this, they may not know that they are dealing with some form of social engineering. They should assess the totality of the facts presented to them knowing that social engineering TTPs are commonly used and typically involve some type of pretexting or use of a story that seems believable. The following information may assist officers when dealing with incidents like this:

- Advise the recipient to visit haveibeenpwned.com to see if their email address has ever been stolen in a data breach.
- Change passwords to important accounts on a regular basis, using long and strong random words strung together.
- Use a password manager or some other system that effectively ensures that each account has a unique password.
- Use two-factor authentication (2FA), especially on important accounts, such as banking or social media.
- Turn off or cover the lens on a web camera when not in use to avoid being targeted in sex-based extortion schemes.

There have been a number of well-publicized research projects devoted to the study of social engineering. In one study frequently discussed in security circles, the researchers manipulated computer users into voluntarily divulging their login names and passwords. They learned that people would give up their login and password if they received a chocolate before being asked for this information. If the chocolate was received afterward, then fewer respondents would share this information. The study showed how easy it is for people to be manipulated into providing information as important as a password with something as simple as a piece of chocolate (Université du Luxembourg, 2016).

How to Prevent Social Engineering Attacks

One of the best methods to prevent a social engineering attack is by building awareness of the tactics, techniques, and procedures used in these attacks. These TTPs are not new, and they have been used to gain access to offices and homes simply by name dropping, presenting fake identification, or using a stolen or found access card. The risks, however, have increased and morphed into a clear and present danger through the ability of attackers to use the Internet to research and perfect a pretexting story. An example of how serious this threat can be occurred in early 2019 when a woman carrying two Chinese passports, four cellphones, a laptop, an external hard drive, and a USB thumb drive social engineered her way into Mar-a-Lago, the Florida home of the president of the United States. The staff at the estate believed that the woman was the daughter of a staff member with the same surname, and because she took advantage of a language barrier, including producing an alleged invitation to an event at the estate written in Chinese, the United States Secret Service (USSS) agent could not verify her story. In fact, the suspect gave security and police three different stories as to why she was at the estate, and then she became argumentative when her cover story was challenged. Police interviewed her and soon learned that she could speak English very well. Upon further examination, they also determined that the USB thumb drive she was carrying contained malicious software that could have infected the computer network at the president's home and placed extremely sensitive information at risk. The USSS subsequently charged Yujing Zhang, 32 years of age, with making false statements to federal agents and illegally entering a restricted area (Smith, 2019).

Employee education is essential, and police officers can play an important role when communicating the benefits of awareness and prevention of and response to social engineering. Security experts expound on the importance of storytelling. News articles and stories related to social engineering attacks are emotional, interesting, and engaging. Police are a credible source for telling these stories, and they can do it when they speak to the media or when they are invited to present at public forums and conferences. This can be accomplished without releasing personal information, TTPs, or specific details. Social engineering has been the subject of many Hollywood movies over the years. The major motion picture *Catch Me If You Can* was based on Frank Abagnale, a self-proclaimed social engineer. Abagnale beat the system for several years posing as a doctor, a lawyer, and an airline pilot, and he used a variety of common TTPs while manipulating and evading police. He was eventually arrested and brought to justice, and once he was released from jail, he wrote a book and was hired as a security consultant for the US Treasury and several major companies.

Other movies and TV series that are based on social engineering include *Six Degrees of Separation*, *Matchstick Men*, *The Sting*, *Sneakers*, and *Mr. Robot*.

Avoiding Social Engineering Attacks

The following are recommendations that law enforcement can share with others to help spread the word about social engineering. The following advice helps potential victims defend themselves against TTPs:

1. Conduct educational events on a regular basis (e.g., annually or semi-annually) in addition to organizing conventional group meetings, training modules, group briefings, presentations, videos, and Web-based training to discuss this topic.
2. Motivate employees to become more security aware by explaining how social engineers operate and talk about the TTPs they employ.
3. Encourage reporting of suspicious behaviour in the workplace, whether it occurs over the telephone, face to face, or online. Make it easy to report suspicious incidents in the workplace.
4. Talk to employees about tailgating and teach them how to approach and report suspicious people in the workplace. Speak about the importance of physical security in the workplace, paying special attention to protecting stairwells and parking garages.
5. Organize regular exercises, such as tabletop and virtual tabletop exercises, to test the internal security systems.
6. Communicate the policy of the corporation and the responsibility that each employee has to ask questions if something they have encountered in the workplace does not seem normal. Employees should be encouraged to help protect corporate assets, email, and social media and be empowered to speak to supervisors or to security personnel to share security concerns.
7. Make security interesting and engaging through the use of posters, contests, and themes.
8. Review policy, processes, and procedures at home and at work in relation to emailing personal information, conducting financial transactions, and collecting sensitive personal information.
9. Share information about some of the latest techniques being deployed by cybercriminals.
10. Test the incident management and phishing reporting systems used by your organization. Test controls and conduct tests on areas of vulnerability.

Source: Hulme and Goodchild (2017).

Conclusion

This chapter explored social engineering attacks from the perspective of how victims are targeted and attacks are planned. We discussed the tactics, techniques, and procedures commonly used in social engineering attacks and the role that trust plays in deceiving victims. The chapter familiarized officers with why emotions are such an important target for attacks and the role they play in motivating the target to respond. Police agencies tend to be reactive in nature and do not have the resources, expertise, or even the experience to be the primary source of information on cybersecurity. A clear message from police should always convey the importance of being diligent about using email safely, cautious when taking telephone calls from unknown people, and careful when sharing personal information with others. The public should proactively seek advice and solutions on topics related to cybersecurity to ensure that they remain up to date and well informed.

As we discussed, attackers invest a great deal of time and effort into their attacks. They study the news to stay current; conduct reconnaissance on businesses, organizations, and people; and test security protocols in an effort to tailor their attacks so that they are as effective as possible. The Internet has enhanced the ability of social engineers to deceive. Along with an amplified ability to gather intelligence about specific people, they can also acquire fake identification, conceal themselves more effectively, and communicate securely with other criminal actors. Police officers must stay current and watch for situations that could be characterized as social engineering. Whenever they are presented with stories of deliberate lies that appear to play on a person's emotions or are met with facts that do not correspond to the circumstances presented, they may wish to ask additional questions to learn why a perpetrator would have gone to such great lengths to commit a particular crime. These factors may reveal signs of deception and social engineering.

DISCUSSION QUESTIONS

1. What is the primary target in a social engineering attack?
2. What is the technique called that misspells letters in a domain name and causes users to access a fake website? How does it work?
3. List five types of letter scams.
4. List five categories of criminals who commonly use social engineering attacks.
5. Describe pretexting.
6. Give examples of five types of emotions that are commonly targeted in social engineering attacks.
7. List five recommendations to reduce the opportunity for social engineering in the workplace.
8. What website should be used to find out if an email address has been breached?
9. List two ideas that will help build awareness of the risks arising from social engineering attacks.
10. What is the term used to describe something that can be stolen or breached with very little effort?

KEY TERMS

CEO fraud, 140
email naming convention, 144
Microsoft tech support scam, 142
peer-to-peer network, 146
pretexting, 141
reconnaissance, 140
remote access, 142
routing transit number, 148
spoof, 138
SWIFT (Society for Worldwide Interbank Financial Telecommunication) code, 148
typosquatting (cybersquatting), 140
US Federal Bureau of Investigation (FBI), 140
wire fraud, 138

REFERENCES

Anderson, D. (2017, May 26). Alberta woman kidnapped, held for 5 days in South Carolina trailer. *CBC News*. Retrieved from https://www.cbc.ca/news/canada/calgary/alberta-woman-kidnapped-south-carolina-1.4133064

Fraudsters exploiting the Notre Dame tragedy. (2019, April 16). Retrieved from https://www.zerofox.com/blog/notre-dame-fire-social-media-scams/

Goodchild, J. (2018, May 21). 4 social engineering tricks that fool unsuspecting employees. Retrieved from https://securityintelligence.com/4-social-engineering-tricks-that-fool-unsuspecting-employees

Greenberg, A. (2018, February 20). The toolset of an elite North Korean hacker group on the rise. *Wired*. Retrieved from https://www.wired.com/story/north-korean-hacker-group-apt37/

HelloTDS. (2018, November 21). Hacking humans: The dangers of social engineering. Retrieved from https://blog.hellotds.com/hacking-humans-the-dangers-of-social-engineering

Hetherington, T. (2018, April 19). Former teen hacker Mafiaboy was hunted by the FBI but now fights cyber crime. *Herald Sun*. Retrieved from https://www.heraldsun.com.au/news/victoria/former-teen-hacker-mafiaboy-was-hunted-by-the-fbi-but-now-fights-cyber-crime/news-story/7f322b8403d023d5c7de662fd14072fb

Hulme, G.V., and Goodchild, J. (2017, August 3). What is social engineering? How criminals exploit human behaviour. Retrieved from https://www.csoonline.com/article/2124681/what-is-social-engineering.html

Krebs on Security. (2016, April). FBI: $2.3 billion lost to CEO email scams. Retrieved from https://krebsonsecurity.com/2016/04/fbi-2-3-billion-lost-to-ceo-email-scams

McDiarmid, J. (2012, August 8). Canadian hacker dupes Walmart to win Def Con prize. *Toronto Star*. Retrieved from https://www.thestar.com/business/2012/08/08/canadian_hacker_dupes_walmart_to_win_def_con_prize.html

Microsoft. (2019, June 3). Protect yourself from tech support scams. Retrieved from https://support.microsoft.com/en-ca/help/4013405/windows-protect-from-tech-support-scams

Mitnick, K.D., and Simon, W.L. (n.d.). *The art of deception: Controlling the human element of society*. Retrieved from http://sbisc.ut.ac.ir/wp-content/uploads/2015/10/mitnick.pdf

Nichols, S. (2016, April 11). Half of people plug in USB drives they find in the parking lot. *The Register*. Retrieved from https://www.theregister.co.uk/2016/04/11/half_plug_in_found_drives/

North Korean hackers stole cryptocurrencies worth $571 million this year. (2018, October 20). *NDTV*. Retrieved from https://www.ndtv.com/world-news/north-korean-hackers-group-lazarus-steals-cryptocurrencies-worth-571-million-this-year-1934849

Royal Canadian Mounted Police. (2014, December 16). Cybercrime: An overview of incidents and issues in Canada. Retrieved from http://www.rcmp-grc.gc.ca/en/cybercrime-an-overview-incidents-and-issues-canada#sec5.3

Smith, D. (2019, April 3). Mar-a-Lago security under scrutiny after Chinese woman gained access. *The Guardian*. Retrieved from https://www.theguardian.com/us-news/2019/apr/03/mar-a-lago-security-scrutiny-chinese-woman-access

Social engineering. (n.d.). Retrieved from https://www.knowbe4.com/what-is-social-engineering/

Thornton, K. (2018, September 12). 5 types of social engineering attacks. Retrieved from https://www.datto.com/blog/5-types-of-social-engineering-attacks

Top 10 grey hat hackers 2018. (2017, May 22). Retrieved from https://www.wikitechy.com/technology/top-10-grey-hat-hackers-2017/

Top 10 most famous hackers. (2009, November 27). *The Telegraph*. Retrieved from https://www.telegraph.co.uk/technology/6670127/Top-10-most-famous-hackers.html

Université du Luxembourg. (2016, May 12). Social engineering: Password in exchange for chocolate. *ScienceDaily*. Retrieved from https://www.sciencedaily.com/releases/2016/05/160512085123.htm

What is pretexting, and what does it have to do with identity theft? (n.d.). Retrieved from http://www.financialinfo.org/what-is-pretexting.html