© Rodolfo Clix/Dreamstime.com

Social Engineering and Cyberwarfare

CHAPTER 6

GOVERNMENTS, MILITARIES, AND PRIVATE ORGANIZATIONS around the world spend billions of dollars each year on advanced technical controls designed to protect the confidentiality, integrity, and availability of information and information systems. Almost all of these dollars are designed to combat technical threats, such as the zero-day attacks leveraged by advanced persistent threat actors, malware that may seek to infiltrate a network, and probing attacks that search for holes in perimeter defenses. Unfortunately, all of these major security investments may be easily undermined if organizations overlook a single weak link in them all—the human factor.

Unlike computer systems, human beings are complex, nuanced individuals who make decisions based on many different factors, both logical and emotional. Human beings have no firewalls, intrusion detection systems, or antivirus software that may be programmed to prevent undesired behavior. In addition, they often have the ability to override security systems, either by explicitly disabling them or by working around them. For example, a human who knows that a data loss prevention system blocks attempts to e-mail sensitive documents outside the organization may decide to simply place them on a USB drive and hand deliver them to the intended recipient.

Cyberwarfare adversaries understand the complexities of human behavior and use it to their advantage. Manipulating the actions of human beings through psychological influence tactics is a technique known as *social engineering*. Social engineers have a deep understanding of ways to influence the thoughts and actions of individuals and use that understanding to achieve cyberwarfare goals. This may include convincing an insider to divulge sensitive information needed to wage a cyberwarfare attack, perform actions that undermine security defenses prior to an attack, or actually unwittingly become a direct participant in the attack itself.

Security professionals must understand the impact that social engineering may have on cyberwarfare operations and the damage that a victim of social engineering can inflict on the larger organization. This understanding should lead the organization to invest in security controls that protect against social engineering. Most notably, organizations should include comprehensive security education and ongoing awareness programs in their communications and outreach efforts. Everyone in the organization must understand the importance of protecting information assets, the signs that a social engineering attack may be under way, and the proper action to take when he or she suspects that an attacker is engaging in social engineering.

In this chapter, you will learn how social engineers exploit human behavior to achieve their goals. You will learn about the six principles of influence used by social engineers: reciprocity, commitment and consistency, social proof, authority, liking, and scarcity. You will then learn how organizations can prepare themselves for social engineering attacks. The chapter concludes by examining a case study of a social engineer at work.

Chapter 6 Topics

This chapter covers the following topics and concepts:

- How humans are the weak link in the cybersecurity chain
- What social engineering is and how it is used as a weapon of cyberwarfare
- What the key principles of influence are and how they may be exploited by social engineers
- How social engineers use tools to achieve their goals
- How security professionals defend against social engineering attacks
- How a real-world social engineer operates

Chapter 6 Goals

When you complete this chapter, you will be able to:

- Describe how humans are often the greatest weakness in an information security program
- Explain how social engineering is a weapon of cyberwarfare

- Explain the six key principles of influence and how they may be used as social engineering weapons
- Describe the tools of the social engineer
- Explain how to defend against social engineering attacks
- Provide examples of real-world social engineering attacks

Humans: The Weak Link

Humans are the weakest link in the information security chain. Organizations invest significant financial and human resources in building strong layers of technical controls, embracing a defense-in-depth approach to information security. These technical controls are focused on protecting the confidentiality, integrity, and availability of both sensitive information and the information systems that run an organization.

Unfortunately, these controls are not sufficient on their own to maintain the security of information. Organizations must remember that human beings are operating information systems and handling sensitive information, and they often have the ability to bypass or undermine security controls. Consider a few examples:

- Scampi Systems has deployed a cutting-edge network firewall designed to block access to the Scampi network from the Internet. The firewall is configured to allow only electronic mail and Web server requests from the outside and to deny all other attempts to access Scampi's systems. Scampi also provides a virtual private network (VPN) to allow employees to bypass the firewall and gain access to the network if they need to work from home or while traveling. If an employee of Scampi provides an attacker with the username and password required to access the VPN, the attacker may then also bypass the firewall.
- Doodle Labs uses a network data loss prevention (DLP) system to monitor outgoing network traffic for the presence of sensitive information. In particular, Doodle Labs is concerned that documents related to a secret product development effort not leave the company's network. An employee with access to the documents would be thwarted by the DLP system if he or she attempted to e-mail the file or upload it to a Web site. However, if the employee simply copies the file to a removable flash drive and mails the drive to the intended recipient, there is nothing that the network-based DLP can do and Doodle's secrets may be exposed to the world.

WARNING

It's still important to *have* technical controls. The solution to this problem is to resolve the human issue and complement strong human controls with solid technical defenses. You'll learn more about defending against the human risk later in this chapter.

- Hunter Industries protects employees from visiting malicious Web sites through the use of a content filtering system that scans the URLs of outbound Web requests and compares them with a list of known malicious sites. The system blocks any attempts to access a blacklisted site and creates a log for administrator review. An employee seeking to bypass the system might use the Tor anonymous Web browser to hide the details of the destination site through the use of an encrypted connection, rendering the content filtering system useless.

In each of these examples, individuals inside the company took actions that undermine the organization's security. Although they may have done this with malicious intent, it is also possible that they thought they were doing the right thing—cutting through the technical "red tape" to get the job done. Whatever the reason for their actions, the end result is the same: Technical controls are rendered useless by human actions.

Social Engineering

Social engineering is the art of manipulating human behavior through social influence tactics in order to achieve a desired behavior. When employed by a cyberwarrior, social engineering techniques may be used for a variety of purposes, including:

- Tricking an individual into divulging information about information systems, networks, or other operational details that may contribute to the Reconnaissance phase of a cyberwarfare attack—providing critical information necessary to wage an offensive cyberwar operation
- Influencing an individual to bypass physical security controls, granting an attacker access to a physical facility where he or she might undertake offensive cyberwarfare operations
- Convincing an individual to disable electronic security controls, such as bypassing a firewall or allowing a VPN connection from an unauthorized source
- Tricking an insider into installing software on a computer located within the organization's protected network that secretly creates a back door, allowing the attacker to gain access to the network

NOTE

Social engineering uses techniques similar to those engaged in during psychological operations (PSYOPS). However, one major difference is that social engineering attacks typically target a single individual, whereas PSYOPS target groups.

Advanced persistent threats often leverage social engineering as part of a comprehensive attack on an organization. They may use these techniques to perform intelligence gathering, influence user behavior to facilitate an attack, or cover their tracks after an attack takes place.

Kevin Mitnick: Master Social Engineer

Renowned hacker Kevin Mitnick is well known for his mastery of social engineering techniques. He began his social engineering career as a young boy riding the bus system of the San Fernando Valley. While riding the bus, Mitnick realized that the transfer system used by the bus line was ripe for exploitation. The system's security depended upon bus drivers using a special punch to put holes in the transfer slip noting the details of the transfer. Drivers give these slips to passengers who must take multiple buses to reach their destination but are only charged a single fare.

Mitnick realized that if he learned the transfer punch system and obtained both a punch and a book of blank transfers, he could ride the system for free. He learned the punch system by studying the transfer slips that he purchased himself. Poking around the bus depot, he realized that bus drivers often discarded partially used books in the trash at the end of their shifts. This solved the second problem, but he still didn't have access to the actual punch that the drivers used to create the transfers.

He then turned to social engineering and worked his magic with bus drivers to overcome this last hurdle. In his own words, "A friendly driver, answering my carefully-planted question, told me where to buy that special type of punch." The masterful use of social engineering techniques is a hallmark of Mitnick's many electronic misadventures.

Influence as a Weapon

The art of influencing people is one of the most studied topics in psychology. Product marketers, salespeople, lobbyists, public relations staff, and many other people use influence as one of the major tools of their trades. Those who possess the power of influence are able to achieve great things and magnify their other abilities. Hackers are no exception, especially when it comes to social engineering. Successful social engineers wield the tools of influence as a weapon.

Robert Cialdini, a marketing professor at Arizona State University, is widely recognized as one of the world's experts in the field of influence. In his book *Influence: Science and Practice*, Cialdini outlines six key principles of influence, illustrated in Figure 6-1:

- Reciprocity
- Commitment and consistency
- Social proof
- Authority
- Liking
- Scarcity

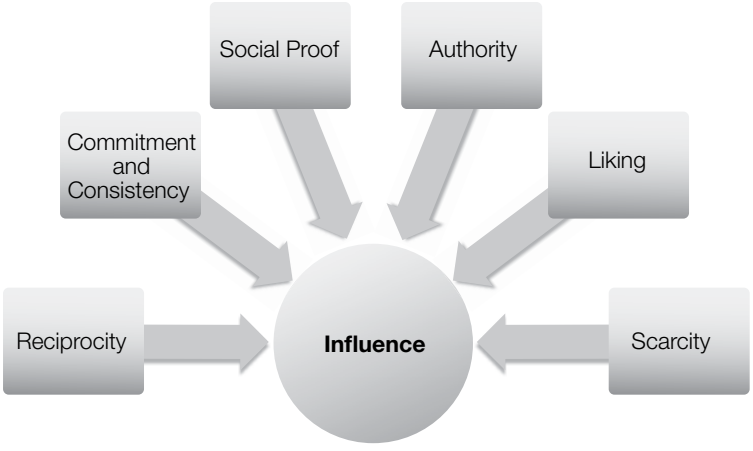


FIGURE 6-1
Cialdini's six principles of influence may be used as weapons by cyberwarriors using social engineering attacks.

Each of these tools plays an important role in all types of influence. Social engineers may exploit these techniques to manipulate their targets into performing a desired action or revealing sensitive information that is critical to a successful cyberwarfare attack. In the remainder of this section, you will learn about each of the influence principles and how it might apply in the context of a social engineering attack.

Reciprocity

Life is about give-and-take. When someone does something for you, you feel a natural obligation to return the favor. In fact, you probably feel like you owe that person a small debt that must be repaid. This is the principle of **reciprocity**—a relationship between two people that involves the exchange of goods or services of approximately equal value.

Certainly, you can think of examples from your life where you've participated in reciprocity and felt the obligation of returning a favor or gift. When you go out to lunch with a friend or colleague and the other person picks up the tab, you naturally feel like you should do the same next time. When someone takes care of your pet while you are traveling, you feel a need to bring a gift from your trip to thank that person for spending his or her time helping you.

Although many examples of reciprocity come from agreements, "I'll do this for you, if you do that for me," not all follow this model. Many are unsolicited and impose an obligation on the recipient that is undesired or even resented. Cialdini describes a striking example of this in his book. He tells of a university professor who engaged in a simple experiment to test the power of reciprocity. The professor purchased a batch of Christmas cards and then mailed them out—to total strangers. Many of those strangers quickly responded with a card of their own without even asking about the professor's identity or his relationship to them.

The power of reciprocity is extremely strong. The social obligation and sense of indebtedness imposed upon you when someone gives you a gift is overwhelmingly strong and may lead you to take actions that you would otherwise never take. Social engineers know this and exploit it to their advantage. In an advanced, well-funded social engineering attack, a social engineer might invite a company executive to an all-expenses-paid conference hosted in a desirable location. After the executive enjoys a day or two of the conference, the social engineer might ask to sit down over a cup of coffee and discuss the company's business. The conversation might begin with very innocent questions and progress into more sensitive territory. For example, the social engineer might ask these questions in order:

1. Can you tell me more about your products?
2. What industries do you typically serve?
3. What product do you think provides you with the greatest competitive advantage?
4. How much of that product do you sell each year?
5. Is it difficult to make that product? Why?
6. That is certainly an impressive product. Who actually designed it?
7. How does the product work?

As you can see, the questions quickly move from information that is probably available on the firm's Web site into details that are likely confidential. The executive, who has already received and used the gift, likely feels a sense of obligation to the social engineer and may answer many or all of these questions out of a sense of reciprocity.

Commitment and Consistency

Human nature leads people to want to act in a consistent manner. They want to perceive their current and future actions as consistent with what they have done in the past. The principle of **commitment and consistency** states that once someone has made a commitment to a particular course of action, that person becomes confident that his or her action was correct and consistent. This confidence increases the likelihood that his or her future actions will be consistent with that committed decision.

One example, provided by Cialdini, is a study conducted by Canadian psychologists who measured the confidence of individuals placing bets at a racetrack. In the minutes before an individual places a bet, he or she has a measurable sense of uncertainty. The bettor is considering the past performance of the horses competing in the race, the track conditions, any possible weather that may come into play, and a variety of other circumstances. Eventually, the bettor reaches a decision, approaches the betting window, and places a wager with the attendant. When the professors measured the confidence level of the bettor immediately after placing a wager, they found a noticeable increase in confidence from the measurement taken immediately before placing the bet. Nothing had changed about the race. The same horses were still competing on the same track in the same weather conditions. Why had the bettor suddenly become more confident?

This is the principle of commitment and consistency at work. Once the bettor actually made a decision and put money on the line, the bettor desperately wanted his or her thoughts to be consistent with that decision. This led the bettor to develop a sense of confidence in the decision. In fact, if the experimenters had gone on to prompt the bettor to increase his or her wager (which they did not), they may have found that the bettor's newfound confidence would lead to making a substantially larger wager than he or she had originally contemplated.

Social engineers can also use the principle of commitment and consistency to their advantage. Consider the case where an attacker posing as a technical support representative is having a conversation with a target in an attempt to persuade the target to divulge a computer password. The conversation might go something like this:

TARGET: "Hello, Bob Jones here."

ATTACKER: "Hi Bob, this is Paul. I'm calling from Air Force technical support. I understand that you've been having problems with your computer?"

[*Pause while Bob struggles to recall a computer problem*]

TARGET: "Yes, actually, you're probably calling about the e-mail issue I reported a while back, correct?"

ATTACKER: "Yes, Bob, we've had some new developments and I think we might be able to fix your problem. Can you describe what you were experiencing?"

TARGET: "My e-mail is pretty slow. Sometimes it takes five minutes to send a message."

ATTACKER: "Oh, perfect. That's exactly the problem that we're fixing. Would you like me to correct your account?"

TARGET: "Yes, please!"

ATTACKER: "OK, I'll just need a little information from you to help identify and fix your account. Is that OK?"

TARGET: "Sure."

ATTACKER: "Great, and what is your e-mail address?"

TARGET: "It's bob.jones@af.mil."

ATTACKER: "Great, thanks Bob. I just need to log on to your account and make a few setting changes. What is your password?"

Now, of course, Bob has been trained to never divulge his password to anyone. In this scenario, however, he might just do that because of the principle of commitment and consistency. The social engineer cleverly led him through a series of questions where he answered "yes," committing to the fact that he had a computer problem, that it was with his e-mail, and that he wanted the attacker's help fixing the issue. Then, when the attacker asks for the password, Bob probably knows he should not provide it, but he has already committed to obtaining the help and providing information.

Social Proof

The principle of **social proof** says that an individual in a social situation who is unsure how to act will likely follow the example of the crowd and behave in the same way as the people around him or her. Cialdini points out the example of canned laughter on television as an example of this. When asked, most people consider canned laughter silly and strange and would say that they don't find things funny just because there is a "laugh track" running on a television show. Furthermore, the actors and writers who make television shows also often object to the use of a tactic that seems phony to them. So, if audiences and talent both claim that they don't like it, why do television producers continue to use it? Quite simply, it works. Canned laughter is an example of a social proof cue. It influences the audience to react with laughter because the "crowd" is acting the same way. This is true even though the "crowd" doesn't really exist!

How could a social engineer exploit the principle of social proof? Let's return to the case of Bob and Paul, where Paul is a social engineer seeking to obtain the password to Bob's computer. If Paul were trying to exploit the principle of social proof, the conversation might go like this:

TARGET: "Hello, Bob Jones here."

ATTACKER: "Hi Bob, this is Paul. I'm calling from Air Force technical support. I'm working through some system updates and need your help."

TARGET: "OK, it's Friday afternoon, though; is this going to take long?"

ATTACKER: "No, it shouldn't be too long. My boss is on me to get 50 of these done before the weekend and I only have 2 left to go. The others took about 10 minutes each."

TARGET: "Great, what do we need to do?"

ATTACKER: "Let me walk you through the first few steps…"

[*Paul has Bob perform a number of simple steps.*]

ATTACKER: "OK, now I need to apply the security settings through the central server console. I'll add you in with the rest of the users I put in today. What's your password?"

At this point, Bob is in the same situation where he found himself in the earlier scenario. He's being asked to do something that he doesn't want to do, but Paul has introduced some social proof cues that might modify Bob's normal behavior. Paul repeatedly referred to the fact that he's already done 50 similar updates and that the other people all provided their account information.

> **NOTE**
> The principles of social influence are not normally used in isolation. In a typical social engineering attack, the attacker exploits several of these principles at the same time in an effort to persuade the victim to perform the desired action or divulge sensitive information.

Authority

Authority is one of the most powerful weapons of influence. If an individual perceives that someone making a request has power over him or her, he or she is much more likely to accommodate the request, even if it seems unreasonable or counter to policies and beliefs.

Social engineers who adopt signs and symbols of authority are sometimes able to achieve significant results.

An individual may possess three main types of authority in any given situation. These include:

- **Legal authority**—The actions of the individual are, or seem to be, backed by the authority of law. Law enforcement officers, judges, and tax collectors all operate under legal authority. A social engineer might attempt to assume a false identity of someone with legal authority before making a request. For example, the social engineer might pose as a police officer conducting an investigation that requires access to an organization's network.
- **Organizational authority**—Most organizations operate in a very hierarchical fashion, with lower levels in the organization giving deference to higher levels. A social engineer understands the organizational authority dynamics in place at a targeted organization and uses those dynamics to his or her advantage. For example, the social engineer might conduct reconnaissance to obtain a copy of the organizational chart and learn the name of a senior executive. He may then pose as the executive when making demands of others within the organization.
- **Social authority**—Every group of people has a natural "pecking order" that is determined by the leadership tendencies of the group's members. This natural leadership that emerges generates social authority. Group members are likely to defer to the leader to curry favor and remain in good graces with the group. Social engineers may develop understandings of informal social networks and then exploit them in the same way they would organizational authority.

Individuals seeking to exploit authority as a weapon of influence often attempt to assume the identity of someone with authority. To do so, they often only need to convince the other person that they seem like someone with authority. In the words of Cialdini, "The outward signs of power and authority frequently may be counterfeited with the flimsiest of materials." Social engineers often assume three major symbols of power:

- **Titles**—People are deferential to those with superior titles. Exploiting titles may be as simple as introducing yourself as the "Senior Vice President of Blahbittyblah" and proceeding to give individuals directions.
- **Clothes**—People are conditioned to interpret someone's clothing as a sign of his or her level of authority. The obvious example of this is that a social engineer posing as a senior executive should dress in the same style as executives from the targeted company. In a less-obvious example, many hackers seeking to gain physical access to a facility dress in the characteristic coveralls of a repairperson and don a tool belt. People see a repairperson working in telecom closets and usually don't even think twice, if they consciously notice it at all. They assume that someone wearing that type of clothing has the authority to work in a maintenance closet.

Using the Title of "Doctor"

Cialdini tells the story of a study into the power of titles that took place in a Midwestern hospital. The researchers placed telephone calls to the nurses stations on 22 different hospital wards, identified themselves as a doctor unknown to the nurse, and gave orders that a patient be administered 20 milligrams of the drug Astrogen.

The nurses were, of course, highly trained medical professionals who should have picked up on several problems with this request:

- Hospital policy forbade the use of telephone prescription orders.
- The drug Astrogen was not approved for use in the hospital.
- The dose the doctor ordered was double the maximum daily dose.

Despite these warning signs, almost all of the nurses hung up the phone and headed straight for the medicine cabinet. Researchers then intercepted them to make sure that the drug was not actually administered to a patient.

This scenario, scary as it may seem, is a perfect illustration of how an individual's title can convey immediate authority. The nurses did not know the doctor, but given the social dynamics of a hospital, chose to unquestioningly obey an order that they should have known was dangerous, merely because a "doctor" told them to do so.

- **Trappings of power**—People also expect individuals with authority to have possessions that match their level of power. For example, if you are impersonating a corporate executive, you'd better pull up to the meeting in a luxury car. No CEO is going to show up driving a clunker!

Social engineers use these signs and symbols of power as a way to project authority that they do not have. Through the use of a combination of titles, clothing, and trappings of power, they may assume the false identity of someone who has legal, organizational, or social power. Once they have successfully adopted the role, they may then use the authority to influence the actions of individuals, achieving their end goals.

Liking

The principle of **liking** says that people are more apt to be influenced by people whom they know and appreciate. It should come as no surprise that people are willing to do things for those whom they like. The principle of liking is closely related to the principle of authority in that they both represent situations where the relationship between two individuals guides the willingness of the individuals to do things for one another. In authority situations, the relationship is based upon power, with one individual having legal, organizational, or social power over the other. In liking situations, the relationship is based upon friendship or affinity and one individual is willing to help the other because of that relationship.

Social engineers can take advantage of the liking principle by engaging in activities that might make the target like them more. Some examples of this include:

- Complimenting the target on his or her personal appearance
- Praising the professional background of the target
- Smiling and projecting a friendly attitude

Many social engineers combine the liking principle with small gifts that also trigger the need for reciprocity. A beautiful woman might approach a male target, smile, and compliment him on his appearance and then offer to buy him a cup of coffee. That's quite a bit of influence all rolled into one small encounter.

Scarcity

The scarcity principle says that people are likely to respond to a situation where they believe they might experience a loss. This might be due to the limited availability of a resource, time limitations on an offer, or an exclusivity of access that would normally preclude them from a resource or experience.

Some of the most glaring examples of scarcity at work are the television commercials that scream, "Time is limited, only 30 seconds remain in this offer. Operators are standing by!" Of course, the same commercial airs over and over again and there really is no time limit. The advertiser is leveraging the principle of scarcity, trying to create a sense of urgency on behalf of the viewer. They hope that the scarcity will prompt the viewer to purchase now, before the product is never again available at this low, low price.

Imagine again the scenario of Paul and Bob, where Paul is attempting to social engineer Bob into providing access to his system. Here's how the conversation might go if Paul decides to use the principle of scarcity:

TARGET: "Hello, Bob Jones here."

ATTACKER: "Hi Bob, this is Paul. I'm calling from Air Force technical support. I'm working through a set of urgent system updates and need your help."

TARGET: "How can I help you?"

ATTACKER: "The payroll system was infected by a virus and we are up against a deadline. If the system isn't corrected by 5:00, the month's payroll won't run and nobody will be paid!"

TARGET: "Oh my gosh! That would be terrible! You only have an hour left. What do you need me to do?"

ATTACKER: "There is a utility that must be run on your computer to update the accounting software. Once we have your update complete, we can then clear out the master system and remove the virus."

TARGET: "Of course, what do I need to do?"

The attacker now has gained the confidence of the victim and created a sense of scarcity—he must act quickly to save the payroll system or nobody will be paid. Bob certainly does not want to be the person who disrupted the paychecks of his coworkers, so he may be prone to comply. Furthermore, the short deadline reduces the likelihood that Bob will follow up with his supervisor or security officials—he needs to act quickly to save everyone's paycheck.

Tools of the Social Engineer

In the previous section, you learned about the weapons of influence that social engineers use to influence the thoughts and actions of their targets. In this section, you will discover the tools and techniques that social engineers wield to exploit these influence principles. These are the actual tactics they engage in to wage cyberwarfare against unsuspecting human targets.

> **NOTE**
> The tactics used by social engineers aren't that much different from those used by swindlers and grifters throughout history. They've become much more effective, however, with the massive communications power of modern networks.

Pretexting

Pretexting is one of the trickiest weapons of the social engineer. In a pretexting attack, the social engineer creates a false set of circumstances and uses them to convince the target to take some form of action. Essentially, pretexting is weaving a web of mistruth that convinces someone else that he or she should take an action.

Social engineers engaging in pretexting commonly assume the identity of someone with the authority to perform an action and then use that identity to execute the action. Here are some common examples of pretexting at work:

- Calling the customer service line of a bank and requesting that the representative change the home address of an account belonging to the assumed identity. The pretexter might do this in an attempt to delay the discovery of fraudulent transactions.
- Phoning an online retailer and changing the e-mail address associated with an account. The pretexter can then visit the Web site and use the "forgot password" link to trigger an account reset e-mail to the pretexter's e-mail address, gaining access to a third party's account.
- E-mailing the customer service department of a telephone company and requesting that a detailed call history be sent to the assumed identity. This might be an attempt by the pretexter to learn whom the target communicates with on a regular basis.

> **NOTE**
> Notice that the examples all involve the use of the telephone and e-mail. Although not all pretexting attacks take place over the phone or e-mail, the vast majority do. This is because a pretexter is more likely to be caught if he or she shows up in person.

The most important ingredient to a pretexting attack is information, especially when the attack takes place in person or over a live telephone call. The pretexter needs enough information about the victim to be able to answer security questions and intelligently discuss the account. For example, if the pretexter provides the victim's street address and the representative follows up with "Oh, and what county is that in?" the pretexter had better be able to quickly respond. It would be highly unusual for someone to not know the name of his or her county.

Here are some basic facts that the pretexter will want to have lined up about a victim before conducting an attack:

- Name
- Home and work addresses
- Telephone numbers
- E-mail addresses
- Mother's maiden name
- Enough personal history to answer most security questions
- Work history
- Information about the individual's relationship with the firm

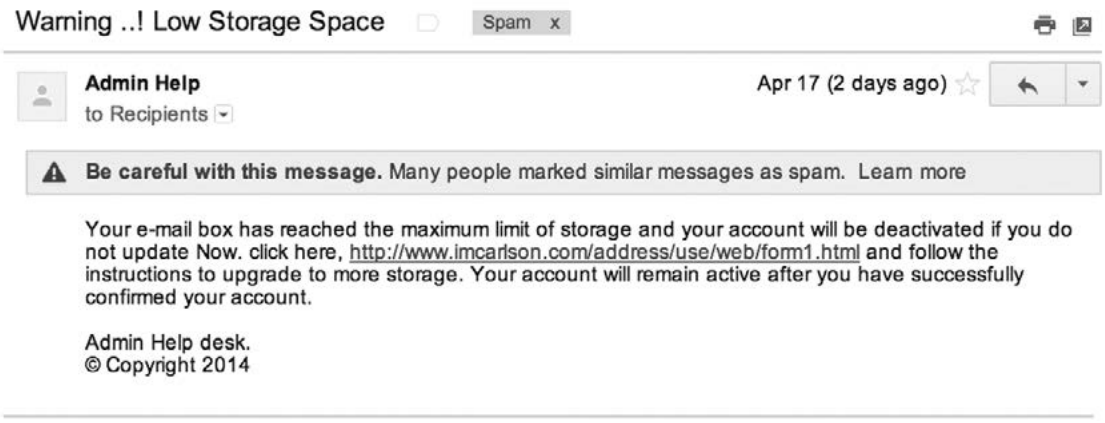
The specific details will vary depending on the type of account being attacked. Some pretexters conduct "test runs" by attempting to pretext accounts other than the victim's in an attempt to learn the types of questions they will be asked when attempting the true pretexting attack.

HP Caught in the Act of Pretexting

Hewlett-Packard, one of the largest computer manufacturers in the world, found itself embroiled in a pretexting scandal in 2006. The company experienced a leak of confidential information and suspected that a member of the company's Board of Directors was responsible for sharing proprietary information with journalists.

Newsweek conducted an investigation, which uncovered that board chairwoman Patricia Dunn ordered an intelligence operation that employed security consultants and private investigators to look into the leaks. They investigated several of the Board of Directors members as well as journalists. The private investigators engaged in pretexting attacks to obtain the telephone records of the investigation targets and concluded that George Keyworth, a Board member, was the source of the leak. Keyworth denied his involvement but resigned from the Board.

After *Newsweek* revealed the pretexting operation, both Congress and state and federal prosecutors launched investigations of HP and the investigative firms. Three investigators pled no contest to state wire fraud charges and received 96 hours of community service. A fourth investigator pled guilty to federal charges of conspiracy and identity theft and was sentenced to serve three months in prison.


Warning ..! Low Storage Space Spam x

Admin Help
to Recipients
Apr 17 (2 days ago)

Be careful with this message. Many people marked similar messages as spam. Learn more

Your e-mail box has reached the maximum limit of storage and your account will be deactivated if you do not update Now. click here, http://www.imcarlson.com/address/use/web/form1.html and follow the instructions to upgrade to more storage. Your account will remain active after you have successfully confirmed your account.

Admin Help desk.
© Copyright 2014

FIGURE 6-2
Example of a phishing e-mail seeking to obtain personal information from unsuspecting individuals.

Phishing

Phishing is one of the most common social engineering tactics in use today. In a phishing attack, the attacker sends the victim an electronic message (via e-mail, text, or other means) attempting to solicit sensitive information from the victim. The message is usually disguised to look as if it originated from an entity that the victim has a relationship with. It is forged, of course.

Figure 6-2 provides an example of a phishing message. Notice that the message uses the social influence tactic of scarcity. The user is warned that if he or she does not follow the instructions at the linked Web site, the account will be deactivated. After clicking the link, the user is redirected to a Web site that asks him or her to log on, providing the username and password associated with the account. This information is then sent to the attacker, who can now access the victim's account.

Social engineers commonly use several subtypes of phishing attacks. Some standard phishing attacks may be rudimentary, such as the one shown in Figure 6-2. However, other types of phishing may be quite advanced. The subtypes of phishing include:

- **Clone phishing** captures an e-mail message being sent from one individual to another, modifies it slightly, and sends a new copy, appearing to be a resend of a message. One clone phishing tactic involves resending a copy of a legitimate message with the header "Sorry, I forgot the attachment" and with a malicious file attached.
- **Spear phishing** attacks are directed at a specific individual. Before engaging in a spear phishing attempt, the attacker gathers personal information about the individual and the organization and uses it to lend credibility to the communication.
- *Whaling attacks* are a subtype of spear phishing attacks that are directed at senior executives and leaders of organizations.

```
Dropbox — ubuntu@domU-12-31-39-10-66-91: ~/set — ssh — 80×24
[---]       Homepage: https://www.trustedsec.com       [---]

       Welcome to the Social-Engineer Toolkit (SET).
        The one stop shop for all of your SE needs.

     Join us on irc.freenode.net in channel #setoolkit

   The Social-Engineer Toolkit is a product of TrustedSec.

            Visit: https://www.trustedsec.com

 Select from the menu:

   1) Social-Engineering Attacks
   2) Fast-Track Penetration Testing
   3) Third Party Modules
   4) Update the Metasploit Framework
   5) Update the Social-Engineer Toolkit
   6) Update SET configuration
   7) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```

FIGURE 6-3

The Social-Engineer Toolkit automates the creation and execution of social engineering attacks.

Social engineers make widespread use of these techniques and, in fact, have a set of tools available to them that facilitate the automation of phishing attacks. These toolkits can automatically scrape the contents of a legitimate Web site, create a false version of the site that captures password information, and then automatically send out links to that Web site in customized phishing messages. Figure 6-3 shows an example of one of these toolkits, the Social-Engineer Toolkit (SET).

Dumpster Diving

Closely related to social engineering is the art of dumpster diving—combing through the trash and recycling bins of an organization seeking out documents that contain sensitive information. This is a time-honored practice of social engineers, who can often use the information that they find to help inform their social engineering attacks by identifying targets, obtaining information about organizational structures, and adding details to their pretexting attacks.

Free Tablets!

In a recent example of baiting uncovered by government investigators, a foreign government sponsored a high-profile keynote speaker at a conference. They provided the speaker with a brand-new tablet computer as a token of thanks for participating in the conference.

When counterintelligence investigators studied the device, they discovered that the tablet came with more than a standard operating system. It had been infected with several backdoor Trojans that would provide the foreign government with the ability to access content on the device at a later date. This is a very clever attack that could be effective against senior executives.

Baiting

In a **baiting** attack, the attacker creates a flash drive that contains malicious code and leaves it in a parking lot, lobby, or other location where a target is likely to discover it. The target may then plug the flash drive into a USB port on a computer within the organization to view the contents. When this takes place, the flash drive installs the malicious code on the victim's computer and the attacker gains access to the organization.

It is widely believed that baiting was used in the Stuxnet attack against the Iranian nuclear program. Analysts believe that flash drives seeded with the Stuxnet worm were placed in areas where nuclear facility personnel were likely to find them and that one of those drives made its way into the Natanz nuclear facility. There it triggered a malware outbreak that caused substantial damage to the facility's high-speed uranium-enrichment centrifuges.

Defending Against Social Engineering

Defending an organization against social engineering is of paramount importance. Throughout this chapter, you learned about the havoc that social engineering can cause in your enterprise and discovered the dangers of social engineering attacks. You also learned that technical controls are not always effective against this type of attack because the attack relies on the human ability to circumvent security controls. In this section, you will learn some techniques that may be used to defend against social engineering.

Security Awareness and Education

The primary and most effective defense against social engineering attacks is user education. Users must understand the tools of the social engineer and learn to recognize when attacks are under way. This training should involve the use of specific examples and take place in several forms:

TIP

Many organizations already have a wide variety of required training programs. You may want to combine social engineering training with related security training programs to avoid aggravating users with yet another mandatory training session.

- *Initial training* that introduces users to the concepts of social engineering, provides them with examples of social engineering attacks, and helps them learn strategies for dealing with suspected social engineers
- *Refresher training* that takes place on a periodic basis and reminds users of the lessons that they learned during their initial training
- *Ongoing awareness programs* that keep social engineering at the top of users' minds, reminding them that these attacks take place every day

Training programs are the most effective way to arm users to live in a world where social engineering is a clear and present danger. Training programs should be on the top of your agenda when it comes to protecting against cyberwarfare threats.

Incident Reporting and Response

One of the messages that your training program should deliver to users is that they need to report any and all suspected incidents of social engineering to appropriate authorities. The reporting mechanism should be easy to use and users should be thanked and/or rewarded for filing reports.

TIP

When using real-world examples in your social engineering awareness program, it is a good idea to remove the name of the victim as well as identifying details. You don't want to stigmatize the victim, as this will result in decreased future reporting.

The information obtained through reporting may be used to immediately bolster the organization's defenses against a specific social engineering threat. If a social engineer is targeting one employee of an organization, it is very likely that he or she is simultaneously targeting other employees. If the original victim cuts off contact with the social engineer, this may prompt contact with other employees as the attacker seeks an avenue of entry into the organization.

When the organization receives a report of social engineering, it should communicate it to security professionals and consider taking actions to block the attacker's continued access to personnel. The example may also be used as part of the organization's ongoing awareness program.

Content Filtering

Many social engineering attacks depend on electronic communication to succeed. Organizations can monitor the content of electronic communications and filter out those believed to be part of phishing attacks before they reach the intended recipient. Organizations can use content filtering in two main ways to combat social engineering.

First, e-mail messages can be screened at the mail gateway to identify those that contain malicious links or match the patterns of previous phishing attacks. This may include verifying the reputation of the sender with a security service and analyzing the content of the message for suspicious content. Messages that resemble phishing attacks may be either quarantined or completely blocked.

Second, Web content filtering may be used to block the URLs of Web sites known to be participating in social engineering attacks. Organizations may subscribe to services that catalog known malicious Web sites and then use a content filtering tool to block all access to those Web sites from the organization's network.

The downside of these techniques is that they are only effective against known threats. Although content filtering is quite good at blocking large-scale phishing attacks, it does not work very well against highly targeted attacks in which the social engineer sends an extremely small volume of messages and directs the recipient to a Web site that has not previously been used in a phishing attack. Therefore, the site would not appear in any malicious Web site database.

Penetration Testing

Penetration testing is the final weapon in the arsenal of cyberwarriors seeking to block social engineering attacks. In a penetration test, the organization attempts to attack itself using the techniques used by real attackers. This allows the organization to identify potential security weaknesses and improve its security.

Social engineering penetration tests conduct phishing, pretexting, and other social engineering tactics against an organization's own employees. The penetration testing team then educates victims about the risks of social engineering and tells them that, had this been an actual attack, they may have been compromised.

> **WARNING**
> Penetration testing carries quite a bit of political risk. You may anger people when you perform these tests, so you should only do so after careful consideration and with appropriate permission.

Robin Sage: A Case Study in Social Engineering

In one of the most stunning examples of social network–based social engineering, Thomas Ryan of Provide Security conducted an operation known as "Robin Sage." In his words, the operation was an experiment that "seeks to exploit the fundamental levels of information leakage—the outflow of information as a result of people's haphazard and unquestioned trust." It provides a telling example of the dangers of social engineering.

Ryan created fake social networking profiles belonging to a fictitious woman named Robin Sage. He used a photo lifted from an adult Web site as the profile photo and created an entirely false background for her, giving her excellent professional credentials as a Cyber Threat Analyst with the Naval Network Warfare Command. He then sought out social networking connections with members of the military and intelligence community.

In his social engineering attack, Ryan took advantage of several of the principles of social influence discussed in this chapter. First, Ryan made use of the principle of liking. He deliberately created a profile belonging to an attractive female. In Ryan's words:

> Choosing a young, attractive and edgy female was a deliberate decision on the part of the creator. Today, the vast majority of the security industry is comprised of males. The heavily male dominated sector allows women to be a commodity in more ways than one.

Second, Ryan took advantage of the principle of social proof. After gaining a few well-respected connections within the security community, Robin Sage quickly attracted the attention of hundreds of other members of that community. When evaluating her friend request, those individuals saw that Robin was already connected to people whom they knew and trusted.

Was Ryan's attack successful? By the end of his 28-day experiment, Robin Sage had gathered hundreds of social networking connections from across the security industry. Her contacts included line staff and senior executives from the National Security Agency, the Department of Defense, the military, Fortune 500 companies, and other sources. Some of the specific contacts made with Robin included:

- A lecturer at NASA's Ames Research Center asked Robin to review a paper that he had written and provide her opinion on it.
- A senior executive in the homeland security field requested a telephone conversation to discuss Robin's background in more detail.
- Connections offered her gifts, job opportunities, and invitations to speak at upcoming information security conferences.

Had Ryan been a malicious actor, he could have attempted to take the Robin Sage experiment a step further and actually continued the contact with her new network, seeking to obtain access to sensitive information and systems. It is clear from this short experiment that social engineering attacks pose a clear and definite risk to cybersecurity.

CHAPTER SUMMARY

Social engineering is a substantial weapon in the toolkit of the cyberwarrior. The effective use of influence techniques to obtain sensitive information and modify the behavior of human subjects can yield significant results. Social engineers know that the six influence techniques of reciprocity, commitment and consistency, social proof, authority, liking, and scarcity are powerful weapons for cyberwarfare. They use these techniques while engaging in pretexting, phishing, baiting, and other social engineering activities. Organizations must take measures to defend themselves against social engineering attacks and ensure that they do not fall victim to this threat.

The case study of Robin Sage illustrates the effectiveness of combining social influence knowledge with real-world social networks. In the case, a security consultant was able to quickly build a network of respected security professionals by baiting them with the profile of an attractive woman with an impressive security background. The military, government, and corporate officials who fell victim to the Robin Sage experiment were later embarrassed to discover that they had been the victims of a social engineering hoax.

KEY CONCEPTS AND TERMS

Authority
Baiting
Clone phishing
Commitment and consistency
Liking
Phishing
Pretexting
Reciprocity
Social engineering
Social proof
Spear phishing