Handling Human Hacking

Creating a Comprehensive Defensive Strategy Against Modern Social Engineering

Charles Snyder

A Senior Thesis submitted in partial fulfillment
of the requirements for graduation
in the Honors Program
Liberty University
Spring 2015

Acceptance of Senior Honors Thesis

This Senior Honors Thesis is accepted in partial fulfillment of the requirements for graduation from the Honors Program of Liberty University.

____
Mark Shaneck, Ph.D.
Thesis Chair

____
Robert Tucker, Ph.D.
Committee Member

____
Stephen Kilpatrick, Ph.D.
Committee Member

____
Brenda Ayres, Ph.D.
Honors Director

____
Date

Abstract

Social engineering is one of the most devastating threats to any company or business. Rather than relying upon technical flaws in order to break into computer networks, social engineers utilize a suave personality in order to deceive individuals through clever conversation. These devious conversations frequently provide the attacker with sufficient information to compromise the company's computer network. Unlike common technical attacks, social engineering attacks cannot be prevented by security tools and software. Instead of attacking a network directly, a social engineer exploits human psychology in order to coerce the victim to inadvertently divulge sensitive information. Further complicating the issue, the rise in popularity of social media has vastly increased the arsenal of information available to the social engineer to utilize when targeting individuals. Ultimately, this paper will describe the danger posed by social engineering attacks before detailing a comprehensive strategy to defend against the threat, accounting specifically for the dangers posed by social media and psychology.

Handling Human Hacking

Creating a Comprehensive Defensive Strategy Against Modern Social Engineering

Introduction

“Hello?” Bob answered his phone on the typical workday.

“Hi, this is Joe from IT,” explained the pleasantly calm voice on the phone. “We are seeing problems on our network and we think they may be coming from your account. Can we have your user ID and password in order to rule out this possibility?”

“I thought IT would never ask for our passwords,” responded a flustered Bob.

“We usually don’t, but this is a time-sensitive matter,” responded the voice. “Can you give me your credentials so that we can prove you are not the culprit?”

“Okay. I have nothing to hide.” Bob proceeded to divulge his user ID and password required for logging into the company network.

“Thanks. We can now see that the suspicious activity is indeed not coming from your account. Thank you for your time and patience with us in this matter.”

Click.

What just happened? At the surface, it may appear that Bob’s company had a problem with their computer network and the Information Security department wanted to ensure that Bob was not the cause of the problem. The more likely explanation, however, is that a nefarious individual from outside of the company was able to convince Bob to divulge his sensitive user credentials. As a result, the attacker likely now has the ability to log in to the corporate network. This simple example illustrates the most common tactic of the social engineer.

Information security is a point of interest for every company. Whether defending the information of employees or the personal information of clients, businesses are intensely focused on protecting this information from the public. Desperately seeking this valuable information, however, are malicious attackers, seeking to devastate these businesses and individuals for a profit. While the traditional threat to information security is the notorious computer hacker hiding in the corner of a dark room, the more realistic threat to security is the amiable social engineer. With his or her proficiency in directing conversations through psychological manipulation masked by cordiality, the social engineer is able to breach the information security of a company with a simple phone call. Exacerbating the problem is the proliferation of social media and the existence of vast amounts of personal information on these web sites. While social engineering has dangerously evolved as a result of the rise in prominence of social networking sites, rigid security policies combined with robust defensive technologies can provide companies with a formidable defense.

Background

Social engineering stands in a unique place among hacking techniques due to its reliance upon deception rather than technology. These types of attacks are dangerous due to their high success rate and simplicity. Security expert and former social engineer Kevin Mitnick explains that typical aspects of security like expensive locks, security software, and guards do not eradicate the security threat posed by human beings, for “the human factor is truly security’s weakest link” (Mitnick & Simon, 2003, p. 3). Despite the devastating nature of social engineering attacks, there seems to be a “lack of concern about social engineering … in computer professional literature,” with writers and researchers devoting their time solely to “technical security issues” (Thompson, 2006, para. 56). Despite this lack of concern, social engineering remains perhaps the most dangerous threat to information security for any company.

Security

The two main aspects of security are information security and physical security. While the world of information security is more concerned with defending against social engineering attacks, a company’s physical security is important for a successful defense as well. Social engineers frequently seek to exploit companies and individuals on both of these fronts, but they typically begin by seeking to exploit physical security.

Information security. The security of information has become a major issue in the modern world. With cybercriminals seeking to steal information from companies for fun and profit, organizations must be vigilant in protecting its information. Experts have identified data confidentiality, integrity, and availability to be the three main components to ensuring information security. Graham (2011) explains these concepts succinctly. Confidentiality describes the “assurance that information is not disclosed to unauthorized individuals” (p. 4). Availability refers to the “timely, reliable access to data and information services for authorized users” (p. 5). Additionally, data integrity assures that the data is protected “against unauthorized modification or destruction” (p. 5). When these three concepts are implemented and enforced effectively, information can be considered secure.

In order for a company to comply with industry standards and regulations, personal information of customers and employees must be protected from attackers. Attackers employ several methods in order to attempt to steal information from companies. The most well-known form of attack is malicious hacking in which the attacker utilizes technology to break into the company's network and steal information. As a result of this threat, most companies utilize antivirus software, intrusion detection systems, and other important tools to combat these technical types of hacking. Mitnick & Simon also add that "as improvements are made in the technological weapons against security breaches, the social engineering approach… will certainly become significantly more frequent and attractive to information thieves" (2003, p. 259). Social engineering refers to taking advantage of this human element of security in order to compromise vital information. In order for companies to test their own security, they frequently hire security professionals called penetration testers to attempt to break into their network and reveal any vulnerabilities to the company. These audits typically test both technical attacks and social engineering attacks.

Physical security. Although hacking and social engineering are most related to information security, a business's physical security is of particular interest to the social engineer. Long and Mitnick (2008) explain that through the use of "dumpster diving," "tailgating," "shoulder-surfing," and other methods of breaking traditional physical security, social engineers are able to glean more than enough information needed to be able to successfully execute an attack. They illustrate that dumpster diving literally refers to the practice of digging through a company's trash in order to find information about the business. Information such as health records, insurance documents, job descriptions, salaries, company calendars, company directories, and many other items are commonly discarded items from businesses. If the company does not take the precaution of shredding vital documents and securing its trash repositories, then the social engineer can easily plunder this collection of information. In addition, tailgating refers to the practice of sneaking into a badge-access building by following someone. This can occur both intentionally and unintentionally. If executed successfully and the social engineer now has physical access to the building, his or her job has become significantly easier. Furthermore, shoulder-surfing can also provide the attacker with valuable information about a company or individual. Shoulder-surfing refers to the act of watching someone’s computer while the person is not looking. This can be used to steal company information from the monitor, or it could be used to carefully watch an individual type his or her credentials into the system. Gleaning information from publicly posted sticky notes also falls under the category of shoulder surfing. Dumpster diving, tailgating, and shoulder surfing are exceedingly common methods of collecting information for social engineers, and they provide surprisingly high levels of success according to professional penetration testers. Finally, a business’s traditional physical security such as video monitoring and use of locks must be carefully implemented and enforced, otherwise these can also provide a platform from which the social engineer can launch his or her attack. If physical security is breached, and the attacker enters the building, his chance of success greatly increases. MacDougall (2012) explains that social engineering attacks performed in person add a level of validity simply because the targeted employees incorrectly assume that “surely nobody would be bold enough to come onto the premises to try and fool their way inside” (p. 59).

Social Engineering

Social engineering refers to a broad category of attacks, and it is often executed with a variety of tactics. Attackers utilize several variations of the attack, but the core concepts of the attack remain the same. Through an act of deception, the attacker malevolently manipulates his or her victim.

Definition

The precise definition of social engineering is complicated because security experts and social engineers disagree over the details. According to Allsopp (2009), a professional penetration tester, social engineering refers to the “obtaining of confidential or privileged information by manipulating legitimate sources” and that it “always requires some degree of deception” (p. 51). Similarly, renowned social engineer and security professional Kevin Mitnick explains that social engineering refers to “find[ing] a way to deceive a trusted user into revealing information” in an effort “to defeat security measures” (2003, p. 7). No one disagrees about the fact that social engineering describes the act of tricking a person into revealing valuable information; however people disagree about some of the specifics. For example, security professional MacDougall (2012) argues that social engineering must be “an interpersonal interaction” and that “phishing is not social engineering,” nor is the classic example of the Trojan Horse (p. 4). Contrary to MacDougall, Granger (2001), a professional at Symantec, argues for a more loose definition of social engineering. He argues that it simply refers to a “hacker’s clever manipulation of the natural human tendency to trust” (para. 4). While precise definitions of social engineering may all slightly differ, the underlying concept remains the same. Social engineering refers to the act of tricking another human being into divulging information.

How Does It Work?

The process of social engineering can be complex, but it follows a general template. Whether the attacks are conducted in person or over the phone, the process begins with a stage of extensive information gathering. Utilizing this wealth of information, the attacker creates a pretext and elicits an action from the victim. This simple process is overwhelmingly effective.

Information gathering. The entire act of social engineering consists of a series of steps in order for it to be effectively executed. According to Hadnagy (2011), it begins with extensive information gathering about the target of the attack. This primarily involves collecting open source intelligence (OSINT) about the target. OSINT refers to information found through publically available sources in a way that does not alert the target. Troves of information can be found about companies and individuals on the Internet, and this is a valuable source for the social engineer. Through visiting personal and corporate web sites, the attacker can frequently find physical locations of interests, contact names and phone numbers of people within the company, biographies on executives, and many special words or phrases that the company uses (Hadnagy, 2011, p. 34). These small pieces of information when utilized together greatly increase the social engineer's chance of success by providing a level of credibility. Additionally, specially crafted Google search parameters can also provide the attacker with valuable information about the target. For example, Google allows for searching with advanced operators in order to search for very specific data. When combined efficiently, it is possible to find information about an individual on the Internet that he or she did not know existed, to the chagrin of the individual.

Pretexting and elicitation. After the attacker has accumulated sufficient information about the target, he or she initiates the attack through pretexting and elicitation. Pretexting is the "act of creating an invented scenario to persuade a targeted victim to release information or perform some action" (Hadnagy, 2011, p. 78). Elicitation refers to "a stimulation that calls up a particular class of behaviors," and it is used by social engineers because he or she "wants the target to take an action" (p. 56-58). The attacker creates a simple pretext and begins elicitation with the target. This can be done in person, on the phone, or in email. The attacker uses information gleaned from the information gathering step in order to carry the conversation in such a way that the target will not be suspicious of malicious intent. Frequently, the work of a social engineer consists of several distinct interactions with different targeted individuals in order to accumulate sufficient information to carry out the ultimate attack. For example, the social engineer may convince one employee to divulge the name of his or her immediate supervisor. Through a cleverly devised pretext, the social engineer can then convince another employee through elicitation that the employee's boss (whose name is now known) needs him or her to perform some function. Thompson (2011) remarks that "social engineering succeeds because most people work under the assumption that others are essentially obvious," and the attacker's seemingly innocent pretexting and elicitation go under the radar (para. 18).

Phishing

While experts disagree about whether or not a phishing attack is an example of a social engineering attack, it is certainly a tool used by many social engineers. Phishing refers to the use of "false emails, chats, or websites designed to impersonate real systems with the goal of capturing sensitive data" (Shaw, 2013, "Computer-Based," para. 2). The most common example of a phishing attack is an email containing a malicious file attachment. Something in the body of the email seeks to gain the trust of the reader, however, if the recipient opens the email attachment, it will install malicious software on the recipient's computer. Most frequently, phishing attacks are conducted when the attacker sends the same fake email to hundreds or thousands of individuals. When the attacker chooses a specific target and specially crafts his or her phishing emails with details to trick this specific target, the attack is called a spear-phishing attack. These are particularly effective due to the attacker's use of legitimate information in the email. In order to avoid falling into the traps set by phishing emails, individuals must be wise enough not open attachments or visit links to the Internet from within emails from unverified senders. However, in the case that an individual falls for this trickery, the company ought to have other security systems in place to prevent the attack from escalating.

Problems with Defending Social Engineering

There are a few key aspects that greatly increase the danger posed by social engineering. First, these attacks are far more prevalent than most people assume, so social engineers are able to take advantage of its lack of popularity. Additionally, the social engineer's ability to use psychology to manipulate his or her victims drastically increases the effectiveness of the attack. Furthermore, the dramatic increase in the use of social media by individuals has allowed social engineers to perform quicker and more effective reconnaissance on individuals and companies. These aspects create several problems that must be addressed in order to defend against the attacks.

Prevalence

Social engineering is exceedingly prevalent in society due to its simplicity. For several reasons, it is difficult to place an exact number on the amount of social engineering attacks that occur on a regular basis. Primarily, most companies will not disclose social engineering attacks to the public because it will tarnish their reputation as a company. Additionally, due to its discreet nature, social engineering can frequently succeed without the target company even realizing anything has happened. Despite it being difficult to discern from companies how frequently social engineering occurs, professional penetration testers reaffirm the threat that it poses. Professionals such as Johnny Long, Kevin Mitnick, Chris Hadnagy, and others have all proven through their work that the vast majority of companies are vulnerable. In particular, Jack Wiles indicates that in his fifteen years of professional experience breaking into buildings and performing social engineering attacks, his team was never caught or noticed once (Long & Mitnick, 2009, "How easy?"). Furthermore, Rößling & Müller (2009) report that in their real-life attempt to use social engineering to break into Müller's own company, four out of their eight attempts to acquire login credentials over the phone were successful. Finally, Mitnick & Simon (2003) explain that "companies that conduct security penetration tests report that their attempts to break into client company computer systems by social engineering methods are nearly *100* percent successful" (p. 245). When the ease of use and cost of execution of social engineering are compared to more technical attacks on companies, it becomes apparent why social engineering is such a common tool.

Social engineering is much more appealing to hackers than more traditional forms of technical hacking for several reasons. As Wiles notes, the steps to break into a corporate network and steal company secrets through technical means can be difficult, expensive, and nearly impossible. He explains that one technical attack will typically have to consist of extensive network scanning, malware installation, network enumeration, and exfiltration of sensitive data (Long & Mitnick, 2009, “How easy?”). These steps each require far more time and generate far more risk than the OSINT and phone calls required by social engineering attacks. Additionally, if the social engineer conducts his or her attack over email or through the phone, it is fairly simply to hide his or her identity. With a more technical attack, there is a greater chance that the company will be able to find evidence pointing toward the attacker due to his or her wide array of steps in implementing the attack. Furthermore, social engineering can be incredibly inexpensive compared to technical hacking. Wiles continues that while the technical hacker may need expensive hardware or software to find and exploit vulnerabilities, the social engineer can spend next to nothing for his work (Long & Mitnick, 2009). Mitnick & Simon (2003) accurately asserts that “cracking the human firewall is often easy, requires no investment beyond the cost of a phone call, and involves minimal risk” (p. 4). For all of these reasons and others, social engineering continues to be an issue that must be addressed.

Psychology

One of the main reasons social engineering is so prevalent is because of its high rate of success. The high rate of success of social engineering is directly related to the psychology behind the attack. Attackers intentionally prey on certain emotions of the targets in order for the attack to succeed. Additionally, Chris Hadnagy explains in detail how reading microexpressions and utilizing neurolinguistic programming are vital tactics for the social engineer to employ when conducting an attack. It is only when recognizing the effectiveness of these methods that individuals can hope to be able to defend against them.

Emotions. According to Allsopp (2009), targets can be psychologically manipulated on the basis of trust, ignorance, gullibility, greed, a desire to help, and a desire to be liked. Each of these emotions provide an avenue for the social engineer to deceive the victim into performing requested actions. Mitnick & Simon (2003) correctly explain that "most people go on the assumption that they will not be deceived by others, based on the belief that the possibility of being deceived is very low; the attacker… [in turn] makes his request sound so reasonable that it raises no suspicion, all the while exploiting the victim's trust" (p. 8). Additionally, Hadnagy (2011) remarks that the most successful tactics for manipulating a target are to appeal to someone's ego, express a mutual interest, deliberately make false statements in order to prompt the victim to respond with more information in anger, or assume the victim know more than he or she does (p. 66-68). Furthermore, Heary (2009) comments that the social engineer's ability to read body language and emotions is the "ticket" to a social engineer successfully exploiting his victim (para. 9-10).

Perhaps the emotions exploited the most by social engineers are trust and fear. For example, one of the most effective ways the social engineer convinces someone to perform an action is by mentioning one of that person's superiors at his or her company. Allsopp (2009) explains that "name dropping" is "a good way to establish trust," because the target assumes that since the social engineer knows the superior's name, the attacker must be legitimately from inside the company (p. 54-55). According to MacDougall

(2012), attackers typically use humor, sympathy, and other emotions in order to create an even greater sense of trust with the target. Once the attacker has established this level of trust, the attacker can usually convince the target to perform any action. In addition to exploiting the target's trust, a more cruel method of attack is to exploit the target's fear. Allsopp explains that inducing fear is "an unpleasant but extremely effective tactic" that social engineers frequently employ (2009, p. 62). The social engineer essentially has to "create a problem (or the belief that a problem exists) and convince the target that he or she is the cause… This creates fear… [and] if you can keep people afraid you can make them do anything" (p. 62). When the attacker assures the target that only a few steps need to be taken to fix the supposed problem, the fearful target usually obliges. This type of attack also encourages the exploited employee to remain quiet about the attack because he or she does not want his or her superiors to know that he or she actually created a "problem" in the first place. While trust and fear are the simplest examples of emotions that can be exploited by social engineers, all of the aforementioned emotions are susceptible to attack.

Microexpressions. Another key to a social engineer successfully performing an attack relies on his or her ability to discern the target's emotions and change the conversation accordingly. Hadnagy (2011) explains that there are "certain muscular reactions in a face [that] are not easily controllable" that "occur in reaction to emotions" ("Microexpressions," para. 4). A noted researcher in this area has identified anger, disgust, fear, joy, sadness, and surprise as emotions easily distinguishable by microexpressions (Hadnagy, 2011). For example, anger can easily be recognized because "the lips become narrow and tense… the eyebrows slant downward and are pushed together," and the person exhibits a distinct glare ("Microexpressions," para. 17). Additionally, both disgust and contempt are characterized by a "wrinkling [of] the nose and raising [of] the lip"; however with contempt, it only occurs on half of a person's face ("Microexpressions," para. 18-20). Understanding the microexpressions that are caused by anger, disgust, contempt, and other emotions can both allow an attacker to accurately understand the emotions of his or her target, as well as provide the attacker with the opportunity to mimic the emotion if necessary. Furthermore, Hadnagy explains that people have the ability to evoke an emotion in another by exhibiting certain microexpressions, even if they are not genuine. As a result, social engineers can "flash subtle hints of sad microexpressions" in order to evoke empathy from the target, lowering the target's defenses ("How Social Engineers Use Microexpressions," para. 7).

Neurolinguistic Programming. In addition to taking advantage of the target's emotions, social engineers can sometimes utilize principles of neurolinguistic programming (NLP) in order to manipulate their target. Hadnagy (2011) explains that NLP describes a "model of interpersonal communication chiefly concerned with the relationship between successful patterns of behavior and the subjective experiences underlying them" ("Neurolinguistic Programming," para. 2). While an abstract concept beyond the scope of this paper, a few key characteristics of NLP are particularly relevant to social engineers. Through the attacker manipulating his or her speaking voice, he or she can discreetly inject commands into seemingly innocent statements. For example, Hadnagy demonstrates that "instead of putting an upswing on the word *agree*" at the end of the question "*don't you agree*," "put[ting] a downswing on the word *agree* can make the question sound remarkably like a command ("How to Use NLP as a Social Engineer," para. 3). In addition, speaking certain words in a sentence with a major emphasis has the ability to drastically alter the impression the target hears. Pontiroli (2013) agrees with Hadnagy's sentiments, explaining that "even though [NLP was] invented for therapeutic purposes," it is "used by many social engineers as a tool to influence and manipulate their victims in order to get them to do the actions needed to deliver a successful attack" (p. 5). While many social engineers claim to rely on aspects of NLP in attacks, a portion of psychologists and scientific researchers insist that NLP represents "pseudoscientific rubbish, which should be mothballed forever" (Witkowski, 2010, p. 64). Despite the controversy surrounding NLP as a valid psychotherapy technique, social engineers indicate that they frequently utilize NLP alongside research in microexpressions in order to effectively coerce individuals psychologically.

Social Media

In addition to elements of human psychology adding to the effectiveness of social engineering attacks, the drastic rise in prominence of social media has contributed to the devastating nature of these attacks as well. As both a means to accumulate personal information and impersonate others, these web sites provide social engineers with a platform for intensifying these attacks.

Information Heap. Primarily, social media sites provide a plethora of personal information about its users, frequently without the user realizing the extent of this revelation. The existence of social networking sites such as Facebook and Twitter often provide social engineers with far more information about the individuals than any other means. Security expert MacDougall (2012) remarks that social networks are "OSINT goldmine[s]" (p. 27). Furthermore, Shaw (2013) demonstrates how sites like Facebook can reveal hints about an individual's email address by utilizing the "forgot my password" link. For example, when entering a person's username on the "forgot my password" link, Facebook asks the user which means of communication he or she would like to use. In the process, it reveals several letters of the individual's email address, which is sometimes enough to decipher the target's entire email address. Finally, there even exist automated tools that allow social engineers to gain extensive information about their targets. For example, Be'ery (2011) explains the existence of a publicly available tool *fbpwn* that provides the attacker with a way to automate the process of acquiring information about a target. The tool first creates a bogus account on Facebook. It will then clone the account of a legitimate friend of the target, taking that person's name and profile picture as its own. Finally the new account will send a friend request to the target, posing as a legitimate friend. If the target accepts the request, even for a second, the application will download all information about that user (including biography, photos, post history, etc.). The target will typically notice that the account is fake after looking at the account, but if the request was accepted, it is too late. Social networking sites have provided such a large trove of information about individuals that hackers have created automated tools to take advantage of this amazing collection of information.

Impersonation. The second major security risk to companies and organizations due to the rise in prominence of social networking sites is that these sites provide social engineers with more than enough information to impersonate someone else. Due to the vast amount of information users include on these web sites, the attacker can easily glean details about names, relatives, friends, addresses, employers, schools, and other details (Timm & Perez, 2010). Wielding this plethora of personal details about the individual, the attacker can more easily claim the identity of someone else, especially over the phone. This provides the attacker with a means of impersonating a supervisor over the phone, potentially convincing the target to commit a foolish act.

Communication. The final risk posed by social networking sites is the ability to communicate with anyone. Through a fake profile on one of these sites, an attacker can directly communicate with his or her target, effectively posing as someone else. For example, in a security assessment, one company assumed the role of a young and attractive woman to successfully entice a targeted individual to click on a malicious link (“Social engineering you way around security,” 2009). These sites can also provide attackers with direct access to leadership in the company if they have a presence on social media. This exposure can be dangerous for companies.

Defenses

Regardless of the high success rate of social engineers and the vast array of techniques they employ, there are several steps that can be taken to render these attacks ineffective. Specifically, through raising awareness, providing training, and enforcing strict security policies, these attacks can be mostly prevented. Realistically, however, many steps must also be taken to secure a company’s network in order to defend against attacks that break through initial lines of defense.

Prevention

Preventing social engineering attacks from devastating a company is a complicated task. Through learning from the experience of experts; however, many steps can be taken to drastically reduce the chance of a successful attack occurring. Most of these defenses focus on equipping individuals rather than fortifying technology.

Awareness. In order for a company to successfully defend against social engineering attacks, the first piece to the puzzle is awareness. Neely (1999) argues that the "first and best protection against social engineering is user awareness" (para. 7). Each and every employee within the company needs to be aware that the problem exists. And not only does the problem exist, it is devastatingly effective. In addition to simply realizing the existence of social engineering threats, everyone at the company, especially supervisors and security experts, must be able to recognize common examples of social engineering. Mitnick & Simon (2003) say that the first step in awareness is to ensure that "everyone in the enterprise [is] aware that unscrupulous people exist who will use deception to psychologically manipulate them" (p. 246). In order to ensure that the entire company is aware of the issue, specific security awareness training must take place regularly.

Training. In order to effectively equip employees to defend against social engineering, the company must employ extensive security education and training for all employees. Ultimately, the "goal of any security awareness program is to… [motivate] every employee to want to chip in and do his part to protect the organization's information assets" (Mitnick & Simon, 2003, p. 249-250). When each employee is equipped with this defensive mentality, he or she is more alert and vigilant. Hadnagy (2011) adds that this program must be engaging and interactive, otherwise it can quickly grow dull and the average employee will not see its relevance. Hadnagy (2011) explains as an example of excitement that he has frequently cracked a password on-stage while presenting, and Mitnick & Simon (2003) and MacDougall (2012) both argue that live examples of social engineering should be presented to the employees in order for them to see its relevance and understand it better. MacDougall even recommends that each employee be given an assignment to create a profile about a randomly assigned coworker, collecting as much OSINT about that individual as possible from the Internet (2012, p. 71). While this may seem eerie, it will certainly be engaging and eye-opening for employees. These are the simplest ways to keep it exciting and engaging. Additionally, training must be part of a greater program that is ongoing in order to stay up-to-date and relevant. The appendix includes an extensive list provided by Mitnick & Simon of topics that should be discussed at the training sessions. Additionally, the training should briefly touch on policies related to computer passwords, disclosing sensitive information, email safety, physical security (including the wearing of badges), and the classification of information (Mitnick & Simon, 2003, p. 255). Each of these items are important security items to be mentioned at training sessions to effectively combat social engineering attacks. Furthermore, throughout the process, the training to "defen[d] against social engineering must be focused on behaviors" in order for it to have any application to each employee (Andress, Winterfeld, & Rogers, 2011, p. 152). Long continues that "security awareness training is the overall least expensive and most effective countermeasure that [a company] can employ in [its] security plan" (Long & Mitnick, 2009, "Beware of Social Engineers," para. 3). Finally, training needs to indicate to employees that even seemingly innocent pieces of information about the company (such as employee names) can provide social engineers with leverage, so these must be protected as well (Hadnagy, 2011, "Being Aware of the Value of the Information You Are Being Asked For"). Andress, Winterfeld, & Rogers astutely conclude that "people are not stupid; they just don’t understand the risks they are taking with their actions. Training can fix that” (p. 152).

Policies. In order for security training and awareness to successfully defend against social engineering, it must be “combined with security policies that set ground rules for employee behavior” (Mitnick & Simon, 2003, p. 245). These policies cover anything from data classifications (confidential, private, sensitive, public, etc.) to steps for verifying identities and authorization of unverified persons. The policies must be carefully explained to all employees as well as emphasized and enforced. Many of these policies, if followed, can effectively render social engineering attempts useless. For example, Mitnick & Simon recommend security policies against running requested programs, executing requested computer commands, downloading requested files, sharing passwords, and many other seemingly obvious policies unless the issuer of the requests has been verified and can be trusted (2003, p. 307). If these four policies are carefully followed by each individual at the company, four of the main avenues of attack for social engineers will have been effectively eliminated. Additionally, policies should be in place that ensure that employees will never be punished “for erring on the side of security,” as promoting security should be a goal of the organization (MacDougall, 2012, p. 76).

Additional Tools. In addition to robust user awareness provided by extensive security training, there are a few other tools that can be utilized to fight social engineering. For example, developing scripts for certain situations and giving these to all employees provides each employee with a way to respond to suspicious callers (Hadnagy, 2011, “Developing Scripts”). Simply requiring that the employee not answer any questions until the person has divulged his or her employee ID number and name will protect against the employee accidentally giving in to a social engineer's clever use of conversation. Along with this script there should be a "list of hot button questions" for employees to be on the lookout for in conversations (MacDougall, 2012, p. 74). Additionally, MacDougall, Hadnagy, and Mitnick all argue that companies should conduct extensive security audits frequently, and these should include social engineering attacks. These should be carried out by professional penetration testers, and they should test areas of security including phishing, pretexting, baiting (with media such as malicious USBs), tailgating, and physical security such as breaking in and stealing (Hadnagy, 2011, "Learning from Social Engineering Audits"). However, if the contract for these external audits allow the testers to call employees, the company should notify its employees beforehand.

Minimizing Damage

Even though "there is no technology in the world that can prevent a social engineering attack," there are several steps that can be taken to ensure that when a breach occurs, the damage is minimal (Mitnick & Simon, 2003, p. 245). For example, extensive use of file encryption can provide a level of security against intruders who gain physical access to computers. This stops intruders from stealing useful information from hard drives upon break-in. In addition, each company's network should be segmented according to 'least privilege' principles, ensuring that "employees have access to only what's needed to perform their job" ("Actions to strengthen your defense," 2014, para. 13). For example, in this instance, if an employee in the marketing department divulges his or her system credentials in a social engineering attack, then the attacker would not have access to any information outside of the marketing department. Additionally, two-factor authentication can provide another layer of safety in the case that an employee accidentally divulges a password. Even with the stolen password, the social engineer will be forced to procure another piece of information or a physical device in order for his or her access to be granted. Moreover, “data loss prevention can stop data exfiltration and alert [the company of] problems” (“Actions to strengthen your defense,” 2014, para. 15). This software has the ability to monitor data moving across the company network and potentially alert the company if an intruder is attempting to extract information from the network. Furthermore, companies should practice defense in depth in all areas of security. This means that there are multiple layers of defense in place at all times. An example of this would be to include each of the aforementioned aspects of security in one system. It is wise for companies to assume that it will eventually be breached, so they should “design [their] network with this inevitability in mind” (“Actions to strengthen your defense,” 2014, para. 11). Finally, it is wise for companies to keep software up to date as this can minimize damage effectively as well (Hadnagy, 2011, “Keeping Software Updated”). For instance, if an employee accidentally divulges to an attacker which Internet browser the company uses and it is a version that contains vulnerabilities, then the attacker now has an easy foothold into the company. However if the company has the most up-to-date version of the software, then this accidental revelation about Internet browser will pose no significant threat.

Comprehensive Defensive Strategy

A thorough defensive strategy can be created by effectively synthesizing these strategies and compensating for the danger posed by social media. The modern threat posed by social media has greatly contributed to the social engineer's arsenal; however, individuals can learn to use social media securely.

Defeating the Social Media Threat

The rise of social media in the past decade has greatly contributed to the social engineer's arsenal when it comes to gathering information about his or her target. Due to this danger, many companies may be tempted to block access to these sites from the employees when they are at work, but this is a bad idea. Disallowing social networks at work becomes dangerous because it simply pushes users to utilize proxy servers, potentially creating even worse security problems ("Social engineering your way around Facebook," 2009). As usual with security, the company needs to maintain a "balance between security and the needs of the users" ("Social engineering your way around Facebook," 2009, para. 11). A better policy than disallowing social networking sites would be for employees not to publish the name of their employer on these sites, as this information can immediately make them a target. Additionally, companies should spend a significant amount of time in training to demonstrate the amount of personal information that can be found on these sites, encouraging employees to be careful and hesitant to post personal information. Employees should be made aware of the potential for attackers to utilize information found on social media sites as well as the potential for someone to impersonate a friend in order to deceive. Furthermore, companies can monitor their own employees on social media to a limited extent, perhaps looking out for places where too much information has been made available (MacDougall, 2012, p. 76).

Comprehensive Defense

In order to have a winning strategy against social engineering, it must be a robust and extensive strategy. First, the company's information security policies must thoroughly address social engineering and its threats. Secondly, each and every employee at the company must be trained according to these policies to be vigilant and aware at all times that he or she can become the victim of a social engineering attack. This training and education must consist of concrete examples of social engineering (e.g. roleplaying) in order to demonstrate the simplicity of the attack. Additionally, the training must address the psychological manipulation that social engineers utilize in order to effectively carry out the attacks. Moreover, employees need to be informed about the security and privacy issues presented by social media, particularly how they provide ammunition for the social engineer to use in a targeted attack. After this robust training has taken place, the company needs to utilize audits that perform social engineering attacks in order to learn the success of the training. Subsequent training can be adjusted depending on the success rate of the auditors. After the entire company has been made aware of the threat and trained to recognize social engineering attacks, the company needs to ensure that its physical security does not provide a foothold for the attacker. Finally, after conducting security awareness training and hardening physical security, the company needs to ensure that it practices general security principles such as defense in depth and least privilege in order to minimize the damage done by any successful attacks. After these steps have been carefully executed, the company has a solid defense against social engineering.

Conclusion

The goal of every company is to succeed, and the security of information is undoubtedly essential for this success to occur. In an effort for a company to comprehensively protect its information, it must pay careful attention to both technical security breaches and non-technical forms of hacking like social engineering. Even with the dangers of social media, companies possess the ability to inform their employees of the vast dangers these sites pose to both the individual and the company. Through an effective security awareness training program and extensive audits, a company can ensure that its employees understand the threat that social engineering poses to each employee. When employees collectively recognize potential signs of attacks and take personal responsibility for securing the company's information, the security culture of the company strengthens. When a company effectively equips its employees to protect themselves on social media and to recognize the psychological manipulation of social engineers, the company has completed the first and most important step in countering social engineering attacks.

References

Actions to strengthen your defense, minimize damage (2014). *Help Net Security*. Retrieved from http://www.net-security.org/secworld.php?id=17779

Allsopp, W. (2009). *Unauthorised access physical penetration testing for IT security teams.* Chichester, West Sussex, UK: Wiley.

Andress, J., Winterfeld, S., & Rogers, R. (2011). *Cyber warfare techniques, tactics and tools for security practitioners.* Amsterdam: Elsevier/Syngress.

Be'ery, T. (2011). New tool enables the automation of social engineering attacks on Facebook. *Software World, 42*(6), 23. Retrieved from http://go.galegroup.com/ps/i.do?id=GALE%7CA271324964&v=2.1&u=vic_liberty&it=r&p=ITOF&sw=w&asid=461785b9cbefad7a1ceb375523f0b47d

Graham, J. (2011). *Cyber security essentials*. Boca Raton, FL: Auerbach Publications. Retrieved from http://www.crcnetbase.com/doi/book/10.1201/b10485

Granger, S. (2010). Social engineering fundamentals, part I: hacker tactics. *Symantec Connect*. Retrieved from http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics

Hadnagy, C. (2011). *Social engineering: The art of human hacking*. Indianapolis: Wiley Publishing, Inc. Retrieved from http://proquest.safaribooksonline.com/book/networking/security/9780470639535

Heary, J. (2009). Top 5 social engineering exploit techniques. *PCWorld*. Retrieved from http://www.pcworld.com/article/182180/top_5_social_engineering_exploit_techniques.html

Long, J., & Mitnick, K. D. (2008). *No tech hacking a guide to social engineering, dumpster diving, and shoulder surfing*. Rockland, MA: Syngress. Retrieved from http://proquest.safaribooksonline.com/9781597492157

MacDougall, S. (2012). Social engineering threats & countermeasures in an overly connected world [PDF document]. Retrieved from https://media.blackhat.com/ad-12/MacDougall/bh-ad-12-social-engineering-threats-MacDougall-Slides.pdf

Mitnick, K., & Simon, W. (2002). *The art of deception: controlling the human element of security*. Indianapolis: Wiley Publishing, Inc.

Neeley, D. (1999). Beware of social engineering. *Security Management, 43*(9)*, 46.* Retrieved from http://search.proquest.com/docview/231222357

Pontiroli, S. (2013). Social engineering, hacking the human OS. *Kaspersky Lab Daily*. Retrieved from https://blog.kaspersky.com/social-engineering-hacking-the-human-os/

Rößling, G., & Müller, M. (2009). Social engineering: A serious underestimated problem. *Innovation and Technology in Computer Science Education '09 Proceeding of the 14th annual ACM SIGCSE*. Retrieved from http://dl.acm.org/citation.cfm?id=1563026

Shaw, R. (2013). Social engineering: a hacking story. *InfoSec Institute*. Retrieved from http://resources.infosecinstitute.com/social-engineering-a-hacking-story/

Social engineering your way around security with Facebook (2009). *eWeek*. Retrieved from http://go.galegroup.com/ps/i.do?id=GALE%7CA217822371&v=2.1&u=vic_liberty&it=r&p=AONE&sw=w&asid=def9a9c0f7e1718fa2eb0abbfd16f81d

Thompson, S. T. C. (2006). Helping the hacker? Library information, security, and social engineering. *Information Technology and Libraries, 25*(4), 222-225. Retrieved from http://search.proquest.com/docview/215828364

Timm, C., & Perez, R. (2010). *Seven deadliest social networks attacks*. Boston: Syngress/Elsevier.

Witkowski, T. (2010). Thirty-five years of research on neuro-linguistic programming. NLP research data base. State of the art or pseudoscientific decoration? *Polish Psychological Bulletin, 41*(2), 58-66. Retrieved from http://search.proquest.com/docview/1323961464

Appendix

Mitnick and Simon (2003) provide the following list of items that must be discussed in order for security awareness training to be effective:

- A description of how attackers use social engineering skills to deceive people.
- The methods used by social engineers to accomplish their objectives.
- How to recognize a possible social engineering attack
- The procedure for handling a suspicious request
- Where to report social engineering attempts or successful attacks
- The importance of challenging anyone who makes a suspicious request, regardless of the person’s claimed position or importance
- The fact that they should not implicitly trust others without verification, even though their impulse is to give others the benefit of the doubt
- The importance of verifying the identity and authority of any person making a request for information or action
- Procedures for protecting sensitive information including familiarity with any data classification system
- The location of the company’s security policies and procedures, and their importance to the protection of information and corporate information systems
- A summary of key security policies and an explanation of their meaning. For example, every employee should be instructed in how to devise a difficult-to-guess password

- The obligation of every employee to comply with the policies, and the consequences for noncompliance (pp. 254-255).