

Running Head: SAFEGUARDING AGAINST SOCIAL ENGINEERING

Safeguarding Against Social Engineering

Colleen Rhodes

East Carolina University

Abstract

This paper will begin by discussing the critical need for security in an organization, as well as for an individual, and how social engineering threatens the integrity of each. It will then describe some of the methods that are used by social engineers to infiltrate security measures in an effort to ascertain confidential information and use it for malicious purposes. To end with, this paper will explain the importance of social engineering awareness and the measures people should incorporate to safeguard against these threats.

Safeguarding Against Social Engineering

Security Issues Today

Security has never been as important as it is today. Since the World Trade Center attacks carried out on September 11, 2001, the United States government, along with many other governments, considers homeland security a top priority and has been conscientiously working on ways to improve it. The growth of online commerce in the past decade has businesses and banks around the world focusing their attention on securing transactions. New HIPAA (Health Insurance and Portability and Accountability Act) regulations are requiring hospitals and other health care systems to be held accountable for patients' protected health information. United States' schools must adhere to FERPA (Family Educational Rights and Privacy Act) and protect the privacy of student education records. The essential need for security is not only apparent in every organization, but also for the individual.

The Federal Trade Commission (FTC) reported in 2005 that "more than one million consumer fraud and identity theft complaints that have been filed with federal, state, and local law enforcement agencies and private organizations." (2005, Consumer Fraud and Identity Theft section, para. 1) According to a survey released on April 2, 2006 by the United States Department of Justice (2006, Identity Theft Hits Three Percent, para. 1), "An estimated 3.6 million--or 3.1 percent--of American households became victims of identity theft in 2004." This means that now, more than ever, individuals are at a high

risk of having their personal information stolen and used by criminals for their own personal gain. Consequently, victims of these crimes can be left with debt, bad credit, higher interest rates, and possibly criminal charges against them until they are able to prove themselves innocent. As a result, it could take years or even a lifetime, to recover from these wrongdoings. At a minimum, sufferers of identity theft are always left with a big mess to clean up afterwards.

Whether it is to secure a company's assets, abide by a law, or guard an individual's privacy, it has become evident to organizations and individuals today that in order to protect confidential information, all possible security precautions must be taken. For an organization, these safety measures should include password requirements for access to electronic records or data equipment. In addition, only authorized personnel should be allowed entrance to a workplace where classified information or equipment is located. When transmitting across the network, data should be encrypted to prevent malicious intruders from capturing and analyzing information, otherwise known as packet sniffing. To further secure private records, tools such as firewalls, access control lists, intrusion prevention systems, and anti-spyware software can be used on the data network to prevent spying or break-ins from the outside.

It is just as important that an individual should protect his or her personal electronic information by using passwords for access and having security tools in place. Whether it is at home or at the workplace, sensitive electronic data can be and should be protected by using authentication, authorization and accounting methods. However, even with all

of these precautions in place, an organization and the individual are still at risk for having their information stolen. Granger (2006, Top five hacking moments on film section, para. 3) points out that, “by merely trying to prevent infiltration on a technical level and ignoring the physical-social level, we are leaving ourselves wide open to attack.” As Hollows (2005, Monitoring and Vulnerability Management section, para. 2) further explains, “Many security systems and technologies have been deployed to prevent intruders from accessing high value systems, [however]... an organization simply cannot patch against social engineering.”

What is Social Engineering?

“Social engineering is the human side of breaking into a corporate network.” (Gaudin, 2002, Playing Off Trust section, para. 1) A hacker will not have any luck trying to convince a firewall to give him or her access, but he or she will find that it is much easier persuading a person to allow him or her admittance to a secure area or even to disclose confidential information. As Damle (2002, What is Social Engineering section, para. 1) explains,

Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders. It is the art of manipulating people into speaking/acting contrary to their normal manner. The goal of a social engineer is to fool someone into providing valuable information or access to that information. They prey on human behavior, such as the desire to

be helpful, the attitude to trust people and the fear of getting in trouble. The sign of truly successful social engineers is that they receive the information without any suspicion.

Social engineers use many different tactics to persuade and influence others in order to achieve their goal of “[gaining] unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network.” (Granger, 2001, Target and Attack section, para. 1). A few examples of these tactics include impersonation, phishing and dumpster diving.

Impersonation

Impersonation is arguably the greatest technique used by social engineers to deceive people, such as posing as an employee of the same organization. “Most people are basically helpful, so it seems harmless to tell someone who appears to be lost where the computer room is located, or to let someone into the building who “forgot” his or her badge.” (Palmer, 2001, The ethical hack itself section, para. 3) In particular, a social engineer finds that pretending to be an employee in the Information Technology (IT) department is typically a useful guise. A simple phone call requesting an employee’s password is usually an easy way to get access to information. Once an employee learns that the call is originating from the IT department, he or she will usually disclose the password willingly and without question, especially after that employee has been told, what seems to be, a legitimate reason for the request.

Just as humans have a natural tendency to be helpful and trust others, as mentioned earlier, they also have a tendency to protect themselves and fear getting in trouble. That is why the use of impersonating authority also works very well for social engineers.

“People are highly likely, in the right situation, to be highly responsive to assertions of authority, even when the person who purports to be in a position of authority is not physically present.” (Rusch, 1999, Persuasion and Influence Techniques section, para. 1)

For example, a Help Desk employee, low on the company ladder, would most likely be intimidated if a person calls in claiming to be the Vice President of Marketing and is demanding that his or her password be reset so that he or she may log in to the system immediately. In this case, the Help Desk employee might be fearful of the aftermath if he or she did not abide by the request, and may not ask for the proper credentials of the caller.

Using the phone is not only frequently used at the workplace to conduct a social engineering attack, but it is also a means for obtaining private information from people at home. It is common for individuals to receive phone calls at home from credit card companies regarding their account. Therefore, people are often not apprehensive to divulge information concerning their account to someone over the phone that claims to be representing their credit card company. Almost always, the goal of the social engineering attack aimed at the individual at home is to acquire that person’s credit card number, social security number, and/or bank account number. In many cases, the social engineer is able to get this information by offering something of value to the cardholder or by using fear that his or her account is in jeopardy.

Phishing

“Phishing is the most common form of social engineering online, and most notably includes email spoofs.”(Granger, 2006, Phishing trips section, para. 1). Webopedia (2005) defines phishing as,

The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user’s information.

Phishing can be considered a form of impersonation except that instead of the intruder masquerading as an authorized individual, the social engineering attack comes in the form of an email or other online mechanism.

Dumpster Diving

Although it might not be the most sophisticated manner for a hacker to ascertain information, dumpster diving tends to be a valuable social engineering attack method. SearchSecurity (2005) reveals that “social engineers rely on the fact that people are not aware of the value of the information they possess and are careless about protecting it.” Most employees would probably not think twice about throwing away a company phone book or company policy manuals. In the hands of a hacker though, this information

could be used for footprinting. Granger (2006, Types of Attacks section, para. 3) defines footprinting as “the art of gathering information (or pre-hacking)...It’s commonly done to research a predetermined target and determine the best opportunities for exploitation.” Dumpsters are usually not locked or in protected areas. As a result, this makes them very attractive to hackers.

The individual at home is just as vulnerable to dumpster diving as an organization. Many people throw away credit card statements, bank statements, and other mail that contains personal information without hesitation. However, just as the saying goes, one man’s trash is another man’s treasure. Even if the dumpster diver is unable to use the information found in the trash to suit his or her purposes immediately, once again it can be used for footprinting. After all, impersonating a representative of a credit card company is a lot easier for a social engineer when he or she possesses the cardholder’s account information.

How to Safeguard Against Social Engineering

Social engineering attacks are one of the hardest threats to defend against because they involve the human element. As Granger (2001, Definitions section, para. 2) so eloquently puts it, “Security is all about trust. Trust in protection and authenticity. Generally agreed upon as the weakest link in the security chain, the natural human willingness to accept someone at his or her word leaves many of us vulnerable to attack.”

Social engineering attacks may be inevitable in the world today for the reason that humans are such easy targets, nevertheless, that does not mean that they are unpreventable. “Prevention includes educating people about the value of information, training them to protect it, and increasing people’s awareness of how social engineers operate.” (2005, Social Engineering, para. 2)

Social engineering training and awareness is absolutely necessary in order for an organization, or an individual, to defend against attacks. Social engineers not only thrive on people’s ignorance of the value of the information they possess, but also of the fact that they are oblivious to the possible attacks against themselves. An organization should provide training programs to all employees including, but not limited to, security guards, receptionists, Help Desk employees, and management. This training should emphasize the need for security and inform people of the various social engineering attacks, as well as the actions they can take to prevent unwittingly giving out confidential information. Businesses, such as credit card companies and banks, should also educate its’ customers by supplying them information and instruction on social engineering attacks so that they, too, will be aware of the possible security risks associated with the individual at home.

In addition to training and awareness programs, security measures against social engineering attacks should be documented in an organizations’ policies and procedures. Documentation will help support these programs not only by increasing awareness, but by providing a consistent manner in which employees should act. The employee will know that by acting according to the regulations, he or she does not have to fear any

possible repercussions. For instance, if a Help Desk employee is commanded by the Vice President of Marketing to reset his or her password, the Help Desk employee could insist on receiving proper credentials before resetting the password and not have to fear the aftermath, as he or she would be abiding by documented procedures.

As another example, a person may try to be helpful by holding a door open for someone who “forgot” his or her badge. However, if this action was clearly documented as unacceptable, and an employee had previously attended training on such incidents, then he or she would be mindful that this could be a social engineering attack. An employee would decide to act in the best interest of him or her self, as well as the organization, by not going against company policy.

Once people are aware of possible social engineering attacks, they are able to use their best judgment as a defense mechanism. In the case where an email is received from a company requesting that an individual update his or her account information, a person who is knowledgeable of phishing attacks would not consent to being directed to a possible bogus website through a link on that email. That person would either go directly to the company’s web site through a separate browser window, or call the company to verify that the email was in fact legitimate.

Awareness would also allow people to be more heedful of what they throw away in the trash. When people are cognizant of the value of the information they possess, they will be more careful of how they handle it. Furthermore, when people are mindful that there

are hackers willing to go through their trash and “dumpster dive” for this valuable information, then they will take the appropriate precautions of disposing of the trash properly. This should include using a shredder to do away with confidential information and being attentive to those who handle trash removal.

Conclusion

With the abundance of confidential information that organizations must protect, and with consumer fraud and identity theft at an all time high, security has never been as important as it is today for businesses and individuals alike. Social engineering is a technique used by hackers and other criminals to persuade people to divulge confidential information, or allow unauthorized access, for their personal gain or for malicious purposes. Techniques such as impersonation, phishing and dumpster diving are used by social engineers to achieve their goals. Although social engineering attacks are difficult to defend against because they involve the human element, it is possible for organizations and individuals to protect themselves by being trained on the importance of security and gaining awareness of the possible social engineering attacks that they may encounter.

Individuals and organizations can try to protect their confidential information by storing their data on a system that requires password-only access, putting that system in a secure room that allows only authorized admission, and by spending as much money as possible on security tools to protect that data. Even after implementing all of these necessary

precautions, they are still susceptible to social engineering attacks because every security measure involves some sort of human intervention.

While training people on different methods used by social engineers will help prevent some attacks from being successful, methods change and countless other schemes can be used. The only viable solution to protecting against these threats is by generating overall awareness. Once people are aware of the critical data that they possess, the crucial need to protect it, along with the strong possibility of exploitation, subsequently a strong defense will be built and social engineering attacks will begin to decline.

References

- *Damle, Pramod. (2002). *Social Engineering: A Tip of the Iceberg*. Information Systems Control Journal. Retrieved April 5, 2005 from <http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=17032&TEMPLATE=/ContentManagement/ContentDisplay.cfm>
- Facts and Statistics*. (2005). Insurance Information Institute. Retrieved March 29, 2005 from <http://www.iii.org/media/facts/statsbyissue/idtheft/>
- Gaudin, Sharon. (2002). *Social Engineering: The Human Side of Hacking*. Earthweb. Retrieved April 3, 2006 from <http://itmanagement.earthweb.com/secu/article.php/1040881>
- *Granger, Sarah. (2006). *Social Engineering Reloaded*. Security Focus. Retrieved April 3, 2006 from <http://www.securityfocus.com/print/infocus/1860>
- *Granger, Sarah. (2001). *Social Engineering Fundamentals, Part I: Hacker Tactics*. Security Focus. Retrieved April 3, 2006 from <http://www.securityfocus.com/print/infocus/1527>
- *Hollows, Phil. (2005). *Hackers are Real-Time. Are You?* Sarbanes-Oxley Compliance Journal. Retrieved April 3, 2006 from <http://www.s-ox.com/Feature/detail.cfm?ArticleID=623>
- Lemos, Robert. (2006). *Survey: Identity Theft Hits Three Percent*. Security Focus. Retrieved April 3, 2006 from <http://www.securityfocus.com/print/brief/177>
- *Palmer, C.C. (2001). *Ethical Hacking*. IBM Systems Journal Volume 40, Number 3. Retrieved April 6, 2006 from <http://www.research.ibm.com/journal/sj/403/palmer.html>
- Phishing*. (2005) Webopedia. Retrieved April 10, 2006 from <http://www.webopedia.com/TERM/p/phishing.html>
- *Rusch, Jonathon J. (1999). *The "Social Engineering" of Internet Fraud*. INET '99 Proceedings. Retrieved April 6, 2006 from http://www.isoc.org/inet99/proceedings/3g/3g_2.htm
- Social Engineering*. (2005). SearchSecurity.com Definitions. Retrieved April 3, 2006 from http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci531120_00.html

* Denotes a journal, technical proceeding or paper that has at least 5 references listed at the end of the article.