Social Engineering –The Human Side

Mark Heckle

East Carolina University

ICTN 6865 Section 601

Dr. Phil Lunsford

Date: November 17, 2019

Abstract

Social Engineering is one of the most widely used methods by cybercriminals to penetrate many networks across the globe. This type of attack is an easy way for criminals to infiltrate the defenses of any organization. Social Engineering attacks seem to be increasing every year due to the lack of awareness and knowledge of end-users. This sensitive data is collected through mobile devices, SMS, emails, or direct contact with a user. While prevention is almost impossible, this paper will examine the definition of social engineering, examples of Social Engineering, methods used by the attacker, the motivators of the attacker, and understanding why humans are easy prey to such attacks. By learning and understanding more about social engineering, it will go a long way in reducing the success of these penetration efforts.

Introduction

Every week there are more stories about hackers and intruders finding ways to exploit vulnerabilities in systems to gain valuable information either for personal gains or other financial benefits. As technical attacks have increased over the years, so have many of the technical countermeasures. The technology countermeasures have done a better job in the last few years to block such attacks. Social Engineering has been around for many years, but attackers have increased their efforts around one of the oldest methods for obtaining relevant information. A lot of the times, these types of attacks go unnoticed by an organization (Thapar, A., 2007).

Social Engineering has involved in sophistication over the last decade, but countermeasures still fall behind. The one real countermeasure is to make people aware of security awareness training in your organization. There is a widely accepted fact that people are the weakest link when it comes to Social Engineering attacks (Power & Forte, 2006). Most organizations admit it is a problem but treat it as a nuisance instead of a severe issue. These organizations do not invest enough in powerful, empowering, and effective security awareness training for all users. All users should have this type of training from the help desk, human resources, executives, and assistants. The training should not scare users but empower them in knowing that play an essential part of security in the organization (Power & Forte, 2006).

This paper will provide definitions of social engineering, the framework around social engineering, motivators of the attackers, discuss the attack model, and the human behavior around these attacks. With more knowledge around Social Engineering, it is the hope that future attacks are detected before significant disruption to the organization.

Social Engineering: Definitions

Social Engineering, defined by Wikipedia, "in the context of information security, is the psychological manipulation of people into performing actions or divulging confidential information" (Social Engineering, 2019).

Social Engineering defined by SANS, "Social engineering is a psychological attack where an attacker tricks you into doing something you should not do" (SANS, 2017). Social Engineering is the art of having users give up confidential information or to access systems. These attacks aren't technical, but instead, they target humans with access to certain information. Technical measures do very little in stopping engineering attacks. Most users think they are good at detecting attacks, although research shows people aren't that good at detecting lies and deception (Krombholz, Hobel, Huber, & Weippl, 2015). As Kevin Mitnick has demonstrated through the years, Social Engineering can be devasting to companies and government agencies (Mitnick, K. D., & Simon, W. L. 2002).

Psychological Motivations

What motivates a social engineering attack? According to the SANS white paper titled *Social Engineering: A Means to Violate a Computer System* by Malcom Allen, identifies four triggers for motivations. The four triggers that discussed are self-interest, external pressures, financial gains, and revenge (Allen, M., 2006).

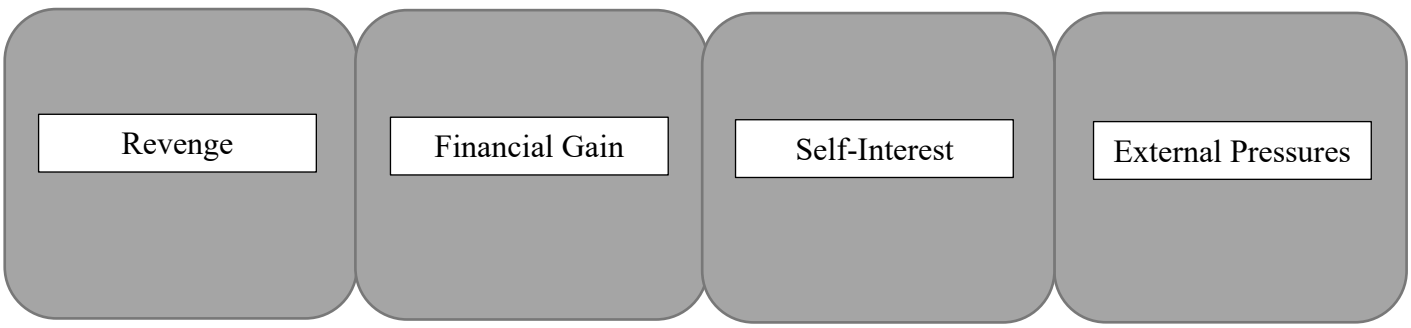

Figure 1. Motivations (Allen, M., 2006)

Revenge: An attack motivated by hate is personal in most cases. In some cases, this could be an attack on an organization, friend, co-worker, or a stranger to satisfy the need for vengeance.

Financial Gain: This can be for various reasons, such as someone that wants a monetary gain because of feelings of owed more. This type of motivation could also be because of debts that need to be paid off.

Self-Interest: This attack is more personally motivated. A self-interest attack can involve modification of data for a loved one, friend, or even a neighbor. It is also an attack to gain credit in hacking communities, and to do it for the fun of it.

External Pressures: A person may be receiving pressure for someone else, such as a friend or co-worker. The attacker may feel so much weight that an attack is carried out. This attack is associated with one of the three other motivations above that have been discussed (Allen, M., 2006).

Social Engineering Attack Cycle

There seem to be various models concerning social engineering attacks that have been explored over the years. As you study these models, they all consist of four phases. The wording of the stages is slightly different with different model comparisons. For this paper, we will use a blend of Kevin Mitnick and Malcolm Allen's four-phase attack cycle approach. The four phases consist of Research/Information Gathering, Developing Trust/Relationships, Exploiting trust, and Utilize Information/Execution (Mouton, Malan, Leenen, & Venter, 2014) (Allen, M., 2006).

In the information gathering/research phase, the gathering process of information about the specific target is retrieved. The information about the particular company (target) can be found in various locations such as a dumpster, company website, physical interactions with staff,

or public documentation. After gathering the information, it is essential to determine if the information is sufficient enough for the attack (Mouton, Malan, Leenen, & Venter, 2014). Once gathered, the data then can be used to build a relationship with the company or an individual that plays an essential part in the attack.

The development of trust and building relationships is the next phase of the cycle. Communication is a requirement for any trust to be built with the target. The gathered information is used to assist in making the communication. While developing the relationship with communication, the attacker will position themselves into gaining trust with the target, in which he will then exploit (Allen, M.,2006).

The third phase is the exploitation phase. Different manipulation techniques are used; for these to be effective, the target has in an emotional state for the exploitation to be possible. All human beings are different; thus, it is essential to determine the state of the target. The idea of this attack is to have the target feel good about giving out unauthorized information to the attacker. The target could easily give out passwords to the company or their password for you to gain access to the network (Mouton, Malan, Leenen, & Venter, 2014).

The fourth phase of the cycle is to utilize the information/execute. This cycle isn't considered to be a part of the social engineering attack. The attacker will use the information exploited from the target, such as a password to break into a system or network. This particular phase doesn't have a human element involved; thus isn't considered part of the social engineering attack. The cycle has now been completed (Mouton, Malan, Leenen, & Venter, 2014).

The attacker might decide that more information is needed to complete the entire attack and revisit a portion of the cycle. If the attacker feels successful, then the goal has been achieved.

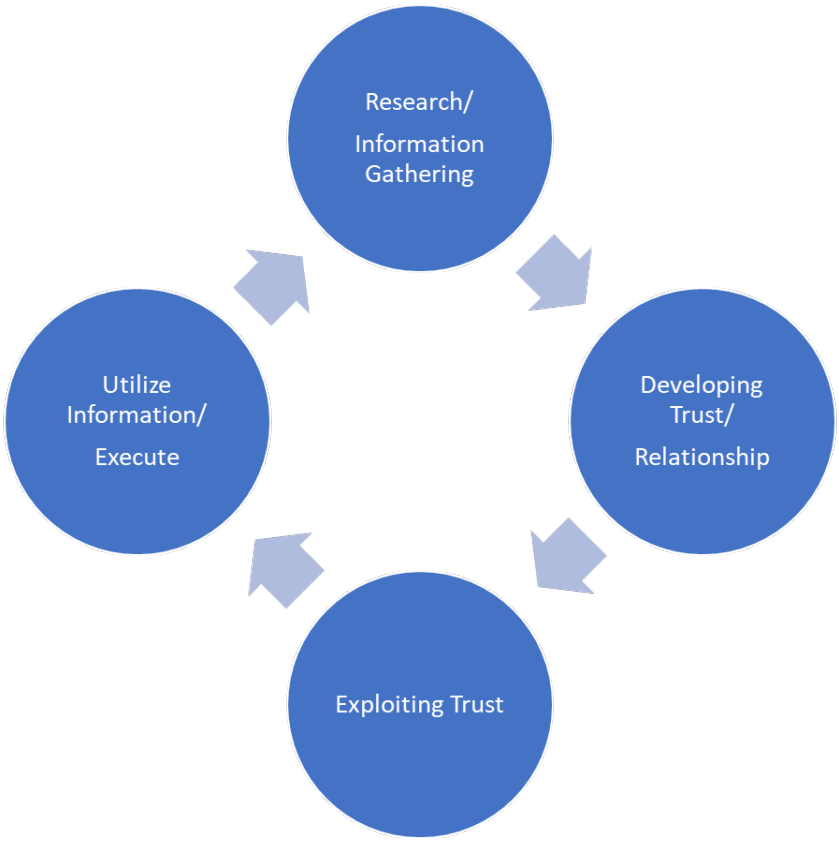

Figure 2. Social Engineering Attack Cycle (Mouton, Malan, Leenen, & Venter, 2014)

(Allen, M.,2006)

Classification of Social Engineering Attacks

Social Engineering attacks can be classified into two categories: human-based or computer-based attacks.

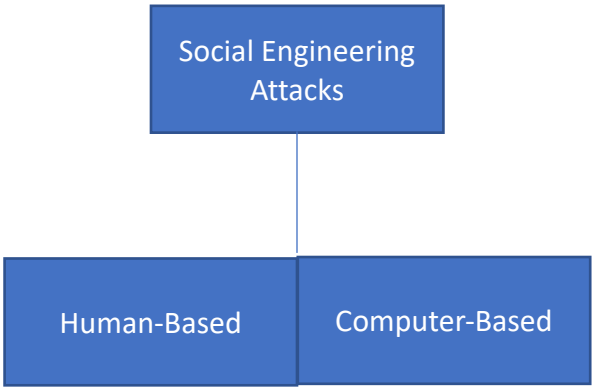

Figure 3. Classification of Social Engineering Attacks (Salahdine, & Kaabouch, N. 2019).

Human-Based attacks take place when the attackers interact with the target to gather the required information. Some human-based attacks include, but not limited to, the direct approach, the helpless user, the important user, the technical support personnel, and reverse engineering (Allen, M.,2006).

Figure 4: Human-Based Attacks (Tarallo, H. M., 2015).

Direct Approach: With the direct approach, the attacker will ask the individual target to complete a task. This task could be something as simple as using the telephone and querying the target for their username/password. Another example of a direct approach would be someone sliding in behind an employee coming into work. What if they had a delivery uniform on and asked you to hold the door as they have a box in their hand? These approaches directly involve a person to gather confidential company information (Allen, M.,2006).

The Helpless User: This type of social engineering is where the attacker pretends they are part of the organization and are helpless. One prime example of this would be someone calling the help desk pretending to be a new user. The attacker could route the phone call through the internal organization phone system as they call the service desk. The attacker displays confusion in what they are attempting to do. For instance, the caller could communicate to the help desk that they are having trouble finding a particular file. The help desk might go on to explain the layout of the file structure. The attacker could use this information later in an attack (Tarrallo H. M. 2015).

The Important User: With this type of attack, it sometimes will involve two types of concepts. One concept is an impersonation, and the other is pulling rank. Impersonation would mean pretending to be someone to gather valuable, confidential information from an unknown individual target. During the impersonation process, the attacker could easily pretend they are essential to make the target comply easier with the request. An example would be pretending to be a new admin assistant for a VP, where they call the service desk asking for specific information. The attacker comes across as really wanting to help their superior (Tarrallo H. M. 2015).

Technical Service Personel: This is a prevalent concept used in social engineering. Everyone has had an IT support person call them trying to help fix a problem. This type of attack is not an uncommon occurrence that happens in an organization. An example would be the attacker calling the user pretending to be a system administrator. The attacker goes on to tell the user they will need their credentials (username/password) to help them with the specific issue they are having with the application. Most of the time, the user will pass along their credentials without hesitation to the attacker. The attacker now has the credentials to access the application (Allen M.,2006).

Reverse Engineering: This approach is different than the others that have been discussed. In this social engineering attack, the target is enticed to asked the attacker questions to gain information. This type of attack is more common in a home setting or small business where no IT services are available to the user. Reverse Engineering involves three phases: Sabotage, Marketing, and Support.

- **Sabotage:** When the attacker gains access, they corrupt the computer, or it appears to the user the equipment needs fixing to continue the use of the machine. The user calls the unknown attacker for help, not knowing what is about to happen.
- **Marketing:** The attacker will leave their contact information around the user's business through business cards. When the user has a computer problem, they will call the number on the business card for assistance. Another way the attacker advertises in on the computer. When the error occurs on the computer, the attacker could undoubtedly have their contact number on the computer screen. The user would see this number and call for assistance.

- **Support:** Support concepts were mentioned in the last phase discussion, but the final step in the reverse engineering cycle is the actual support assistance by the attacker. The support would be the user calling for aid from the unknown attacker from their advertised information discussed above. When the attacker has the user on the phone, the attacker would then elicit confidential information while fixing the problem (Tarrallo H. M. 2015).

Computer-Based attacks include but certainly not limited to email, phishing, and websites. There are many computer-based attacks in social engineering, but for this paper, we will discuss some of the more common techniques used. These attacks do not require the presence of a user to launch the attack.

Figure 5: Computer-Based Attacks (Tarrallo H. M. 2015)

- **Email:** For this type of attack, the attacker contacts the victim by email, promising them a prize, money, or free merchandise. The attacker wants the victim to break all of their security rules to provide personal information back to the attacker. Phishing in which we will talk about later in the paper is sent through emails. Emails also

provide a way for an attacker to introduce malicious code into an organization. The malicious code could be a virus that entered into the network that causes so much havoc. This type of malicious code is generally in an attachment that has been delivered with the email (Salahdine, & Kaabouch, N. 2019).

- **Phishing:** This is one of the most common attacks in social engineering. Attackers frequently aim at gaining private and confidential information from the victims. These phishing scams are typically seen in emails sent to the victims. The emails contain fake websites, ads, PayPal sites, phony lottery wins, awards, and free offers. Phishing scams frequently request the user to input their personal information, banking information, username/passwords, and other personal information. Some phishing scams can even launch keyloggers to record keystroke information without the user ever knowing(Salahdine, & Kaabouch, N. 2019).
- **Websites:** The attacker creates these social engineering attacks in hopes of attracting the victim to visit their fake website. The same tricks are used as the other methods, such as promises of free merchandise or awards that have been won. Once the user visits the website, they are asked to input personal information. This personal information can then be used to gain access to confidential information. Some of these fake websites also ask for specific passwords that need to be entered. It could be the same password that is used at work (Tarrallo H. M. 2015).

Human Behavior:

Attackers that use social engineering attacks are looking for specific human traits in their targets. These traits allow human beings to be taken advantage of by social engineer attacks. The traits include but not limited to, the following:

- **Excitement:** Most everyone has felt the excitement in some form. Have you ever received an email stating that you had won a prize? Maybe it was asking for you to click on a specific link and fill out the information to obtain a new Ipad. To someone who untrained, excitement sets in, and the user complies with the email to receive that new Ipad. The email could have contained an attachment that the user opened as well. Once an attachment has been opened, the computer has been comprised with a possible virus. The attacker gains remote access to the machine and network(Thapar, A., 2007).
- **Fear of Authority:** Most humans have some apprehensive in the presence of authority figures. Authority figures could be law enforcement, but most times, with social engineering, the attacker impersonates a higher-ranked authority figure in the organization. When the attackers take on the role of a higher-ranked authority, the users tend to pass on confidential or sensitive information to the attacker (Shetty, D.).
- **Desire to be helpful:** Many, if not all, humans want to be useful in their personal lives and at their place of employment. Being kind is a common trait that the attackers take advantage of social engineering attacks. Most employees are taught from orientation to be helpful to others and to be a team player. People with the desire to be useful and to solve other people's queries tend to give out a lot of information. This information could contain sensitive and confidential information. The attacker could use this data to gain access to a system or network.
- **Laziness:** Some workers do the same set of activities around their jobs every day. People don’t always look for other ways to do these activities and become bored. Workers over time may create shortcuts to do the tasks but are still able to meet their

goals. People will tend to get lazy doing this every day and could be taken advantage of by a social engineering attacker. Attackers would be able to obtain information with ease due to the laid back attitude of these workers (Thapar, A., 2007).

- **Ego:** Many times, the attackers make the person feel very confident and secure in giving out the information. The attacker removes the logical awareness of the security breach that is happing in front of their eyes. The employee enjoys displaying how much knowledge of the information they have.
- **Insufficient Knowledge:** Many times, the employee, due to lack of training or education, are not sure they have enough knowledge about a specific system or product. The attacker takes advantage of the lack of knowledge by creating urgency and not allowing the employee a lot of time to think. The employee never realizes they are actually under attack (Shetty, D.).

Defense Against Social Engineering Attacks:

There is no 100% way of protecting against social engineering attacks no matter what controls are in place at the organizations. The human factor plays a crucial role in social engineering attacks. Social engineering attacks can be reduced by taking certain precautions. This paper will mention a few of the precautions that are a must for any organization.

- **Security Policies:** This is the first step that should be done in any organization. Clear and readily available policies should be in a place where all employees can access at any time. A security policy sets the standards and levels of security that are in place. The set of security policies should address identification, shredding, hardware life cycle, password changes, and account access (Tarrallo H. M. 2015).

- **Security Awareness Training:** An organization can have excellent policies in place, but the users need to be aware of the security polices. Awareness training should address the policies, the risks, and potential losses, and also on social engineering techniques to be mindful. The education can be presented by an expert in the field, training videos, exercises, banners, or newsletters.
- **Physical Security:** Access to any hardware or offices should be strictly controlled and reviewed. Identification should always be visible or shown if asked to see. Visitors should have a process that is followed and have ID on their person. Data Center access should be given sparingly and strictly enforced. There should never be many people that have access to an organization's data center (Tarrallo H. M. 2015).

Conclusion:

Social Engineering attacks have been part of most major cyber events that occurred over the years. Many of these events have been against a large corporation in the United States. These types of attacks are ballooning as one of the main threats to individuals and businesses across the nation. Social Engineering is hard to defend because it manipulates human nature, not technology. Technology controls have been able to limit the number of regular attacks over the years, but technology controls can't prevent social engineering attacks that target individuals (Campbell C. 2019). It is essential as security professionals that employees are made aware of the basic knowledge needed to prevent social engineering attacks. Employees must attend security awareness programs, where they should be taught to recognize such attacks. It is crucial to make the topic of social engineering engaging and relevant as the employees are the first line of defense in social engineering attacks.

References

Allen, M. (2006). Social Engineering: A Means to Violate a Computer System. Retrieved November 24, 2019, from http://www.sans.org/readingroom/whitepapers/engineering/social-engineering-means-violate-computer-system-529

*Campbell C. (2019). Solutions for counteracting human deception in social engineering attacks. *Information Technology & People, 32*(5), 1130-1152. doi:10.1108/itp-12-2017-0422

Evans, N. (2009). Information technology social engineering: An academic definition and study of social engineering - analyzing the human firewall. Retrieved November 25, 2019, from https://lib.dr.iastate.edu/etd/10709?utm_source=lib.dr.iastate.edu%2Fetd%2F10709&utm_medium=PDF&utm_campaign=PDFCoverPages

*Krombholz, Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications, 22*, 113-122. doi:10.1016/j.jisa.2014.09.005

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. Indianapolis, IN, IN: Wiley.

*Mouton, F., Malan, M. M., Leenen, L., & Venter, H. (2014). Social engineering attack framework. *2014 Information Security for South Africa*. doi:10.1109/issa.2014.6950510

*Power, R., & Forte, D. (2006). Social engineering: Attacks have evolved, but countermeasures have not. *Computer Fraud & Security, 2006*(10), 17-20. doi:10.1016/s1361-3723(06)70433-x

*Salahdine, & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet, 11*(4), 89. doi:10.3390/fi11040089

Shetty, D. (n.d.). Social Engineering: The Human Factor. Retrieved November 23, 2019, from https://www.exploit-db.com/docs/english/18135-social-engineering---the-human-factor.pdf

Social engineering (security). (2019, November 13). Retrieved November 17, 2019, from https://en.wikipedia.org/wiki/Social_engineering_(security)

Social engineering. (2017). Retrieved November 17, 2019, from https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering

Tarallo, H. M. (2015). Social engineering—countermeasures, and controls to mitigate hacking. Retrieved November 24, 2019, from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1689458229?accountid=10639

Thapar, A.: Social Engineering : An Attack Vector Most Intricate to Tackle, Infosec Writers (2007), www.infosecwriters.com/text_resources/pdf/Social_Engineering_AThapar.pdf