The Threat of Social Engineering

Anise Ward
December 8, 2016

Abstract—Every individual and organization is spending thousands of dollars on protecting their system. But no matter how much money is spent, they are still vulnerable to social engineering attack. Thispaper will discuss the different attacks a social engineer use and how not only companies are being attacked but colleges to. Also how the malware the social engineers use in an attack works.

I. Introduction

As technical attacks have increased so have numerous based countermeasures to prevent them. Individuals and corporations spend thousands of dollars to protect their system from being hacked. But no matter how much money is spent they are still the target. In the book "*Art of Deception*" Kevin Mitnick says "You could spend a fortune purchasing technology and services….and your network infrastructure could still remain vulnerable to old-fashion manipulation [1]. Attackers are switching their focus and targeting people through the use of social engineering methods, often gaining access to individual's personal information.

According to many authors social engineering can be defined in many ways. One way to define social engineering is breaking an organization's or individual's security by interactions with people [2]. Kevin Mitnick defines it as "taking advantage of people's naivety through influence, persuasion and manipulation to obtain virtual information" [1]. Another way to define it as an act to manipulatean individual to gain personal information. This attack is associated with taking advantage of people who often considered the weakest link in the security system. It is also one of the hardest attacks to handle.

II. Social engineering

In this paper social engineering is defined as an act to manipulate an individual to gain personal information. It is a blend of technology, science, and art [3]. This term applies to the trickery of gathering information to an individual or organization. In business perspective it is one of the hardest risks for a company to secure. Social engineers are able to take advantage of individuals or organizations with or without the use of technology. The goal of social engineering is to gain unauthorized information in order to commit fraud or identity theft and financial gain. Social engineers abuse human emotions such as fear, curiosity, the natural desire to help, and the tendency to trust in order to bypass security systems [4]. Social engineers think it is much easier to abuse a person's trust then to use technical ways to hack into a secured computer. Figure 1 shows the four steps used by social engineersto attack individuals and organizations. The four steps are 1. Information Gathering 2. Development of Relationship 3. Exploitation of Relationship 4. Execution.

Information Gathering

In the information gathering the attacker uses different public sources such as the internet, social media posts, job portals and many other sources to collect information on their target [2]. The information from this step is used in the next step.

1) *Development of Relationship*

Development of relationship trust is formed between the attacker and the target using direct or indirect communication [5]. It is aimed at creating a

relationship with the target based on being helpful and trustful. When this step is successful, theattacker continues to the next step.

2) *Exploitation of Relationship*

Exploitation of relationship is when the attacker wants the target to reveal important information such as passwords, credit card numbers, and login details [2]. This can be the ultimate aim of the attack, or the beginning of the next step.

3) *Execution*

The last step execution is aimed at the achievement of the attacker trying to achieve their ultimate goal and the obtained information is put to work. This step might be the beginning of another social engineering attack [5].

Social engineers use these four steps with different techniques whether it is physical techniques (non-technology based) or psychological techniques (technology based).

III. Physical techniques (Non-technology based)

The physical techniques (non-technology based) relies on background research This is where the attacker gathers information on their target. Two of the most common physical techniques consist of the following:

A. Dumpster Diving

Dumpster Diving is information is collected on an individual or company by the attacker going through an individual or organization garbage or dumpster. These socialengineers look for possible security leaks in the trash such as company phone books, memos, letters, login information, company credit card statements, company letter headsand much more. These items are very helpful and useful to the social engineer see Figure 2. They collect confidential information that was not discarded correctly.

Item Retrieved	Why is it so useful?
Calendars	Can reveal which employee are of town at a particular time
USB flash drives or portable hard drives	These devices are often improperly disposed and may contain valuable information
Memos	Unimportant memos can often provide small bits of useful information for an attacker who is building an impersonation.

Figure 2 Items social engineers use [6]

B. Tailgating

Attackers gain unauthorized information about a company by following behind an employee entering the company. Despite many companies having specialized doors that only permit access to authorized areas with a card or code, it is the human kindness of holding the door for the next person. Tailgating can happen in many forms such as a tailgater standing outside the door and waits until an employee exits the building. The tailgater then slips behind the person as they are walking and grabs the door before it closes [6]. Piggybacking is a form of tailgating, that allows an employee to conspire with an unauthorized person to allow them to walk in with them [5].

C. Shoulder Surfing

Shoulder surfing is looking over someone shoulder while they are using a computer or entering a code for a secured area. The attacker looks over the target individual shoulder to gain information such as passwordsand login information.

IV. Psychological Techniques (technology based)

Psychological techniques (human based) is based on developing a one-to-one communication between the attacker and the targetindividual [2]. It reliesheavily on technology to trick and manipulate the target individual into believing that they are interacting with a real application and to get them to provide confidential information. For example, the target individual gets a popup window informing the target individual that their network connection has been lost, and the target individual will need to re-authenticate in order to proceed. The information that the target individual entered is emailed back to the social engineer through an installed program on the target individual system [2]. Once the target individual provides their information on that popup window the damage is done. This method is carried out through the deception by taking advantage of the human's weakness to trust.Some of the reasons that make psychological social engineering effective is listed in Figure 3 [6]. The psychological techniques consist of the following:

A. Pretexting and Impersonation

Social engineers use pretexting and impersonation together in an attack. Pretexting is when a person lies to another person in order to gain confidential information. But it more than lying to someone, it is creating a new identity to manipulate the target individual.

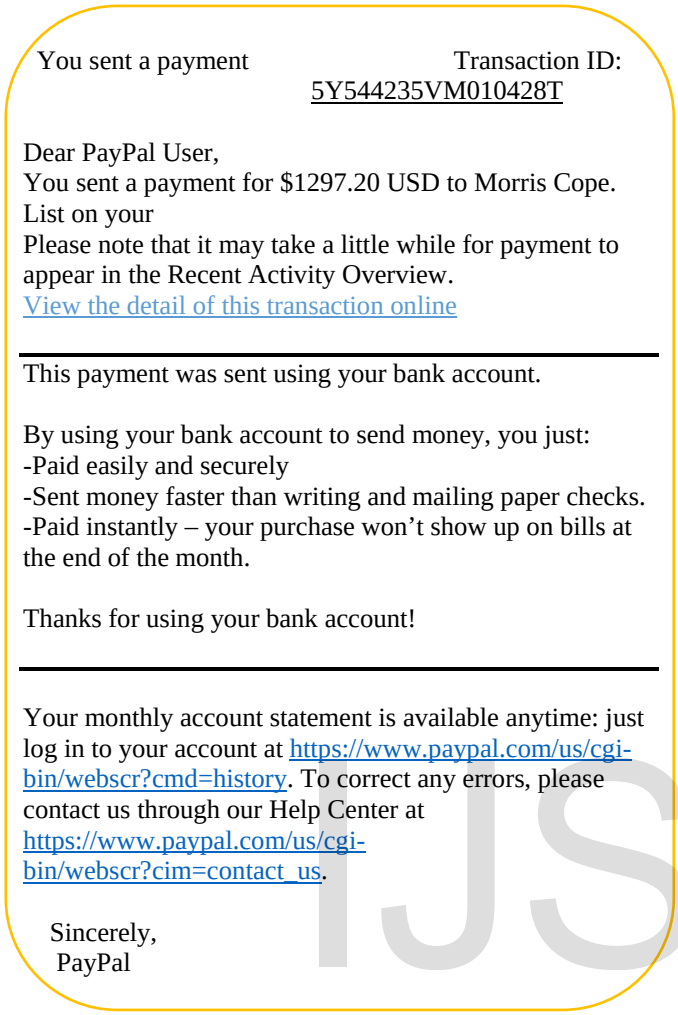
Impersonation is when a social engineer impersonates a network administrator, help desk, or a CEO and ask an employee for their username and password. They do this so can “fix the problem” in the target individual computer. The goal of impersonation is to obtain information or access to an individual computer.

Principle	Description	Example
Authority	Directed by someone impersonating authority figure or falsely citing their authority	“I’m the CEO calling.”
Intimidation	To frighten and by threat	“If you don’t reset my password, I will call your supervisor.”
Consensus/Social Proof	Influenced by what others do	“I called last week and your colleague reset my password.”

Figure 3 Psychological social engineering [6]

B. Phishing

Phishing is one of the most dominant attacks seen today. Antti-Phishing Work Group (APWG) defines phishing as " a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account information [5]. Phishing attacks are successful because the emails, fake websites, and logos appear to look legitimate. Figure 4 show what an actual phishing looks like. There are three types of phishing general phishing, spear phishing, and vishing/Interactive Voice Response (IVR).



You sent a payment Transaction ID: 5Y544235VM010428T

Dear PayPal User,
You sent a payment for $1297.20 USD to Morris Cope.
List on your
Please note that it may take a little while for payment to appear in the Recent Activity Overview.
View the detail of this transaction online

This payment was sent using your bank account.

By using your bank account to send money, you just:
-Paid easily and securely
-Sent money faster than writing and mailing paper checks.
-Paid instantly – your purchase won't show up on bills at the end of the month.

Thanks for using your bank account!

Your monthly account statement is available anytime: just log in to your account at https://www.paypal.com/us/cgi-bin/webscr?cmd=history. To correct any errors, please contact us through our Help Center at https://www.paypal.com/us/cgi-bin/webscr?cim=contact_us.

Sincerely,
PayPal

Figure 4 Phishing email [6]

1) *General phishing*

General phishingis done through emails and phone calls. The email has an attachment which is malware and ask the target individual for personal information. The attacker sending the email appears to be from a legitimate bank, school or company. These messages explain that there is a problem with the target individual account that requires the target to verify information by clicking on the displayed link and providing information in their web link. The link location appears to look like the legitimate logo from a bank, school, or company and content is copied from the legitimate bank, school, or company making the website seem real. The fake website resembles the legitimate bank, school, or company which tricks the target individual in to entering their information, enabling the social engineer to implant malicious programs [5].

2) *Spear Phishing*

Spear phishing involves targeted e-mails. The e-mail message includes the target person personal information making it seem believable to the targetindividual and more difficult to be filtered by software [5].

3) *Vishing/Interactive Voice Response (IVR)*

Vishing also known as Interactive Voice Response (IVR) is a technique that involves using an IVR system to imitate a legitimate message that appears to come from a bank or company. The attacker directs the target individual to verify their confidential information through a specific number which has been set up by the attacker.

C.Baiting

The attacker leaves an infected malware such as a USB, CD, or DVD at a location where the target individual will find it. Once the target person finds and loads the USB, CD, or DVD on their computer the malware is installed.

Social engineers who use baiting offer a download of a movie or music, something that someone wants. Once the target individual takes the bait, the social engineer uses malicious software to corrupt their system and steal confidential information [5].

D. Hoax

Hoax is contained in an email message usually claiming to be from the IT department and used as a first step in an attack. The hoax implicates that is a "deadly virus" circulating the Internet and that the

user should erase specific files or change security configuration and then forward the message to others [6]. If the user changes the configurations they are allowing the attacker to attack their system. Also erasing the files and calling the number which is the hoax makes the computer more vulnerable for attacking.

V. Malware Attack

Malware is used for viruses, worms, and Trojan horses. Malware is used in a lot of social engineering attacks mostly phishing attacks. In order for social engineering malware to succeed they use technological attacks and tactics. The malware uses a variety of tactics such as websites, emails, mobile devices, etc. to infect someone system. Google tracks websites with potential malware and phishing. Since November 20, 2016 has decreased to 27, 503 while phishing websites have increased to 48, 306 on November 6, 2016 [7]. The steps that a social engineering malware attacker uses is shown in Figure 5 but not all social engineering malware attackers follow the steps. The steps show a successful attack by social engineering malware attacker and how the tactics trick the user into opening an attachment or clicking on a web link [8].

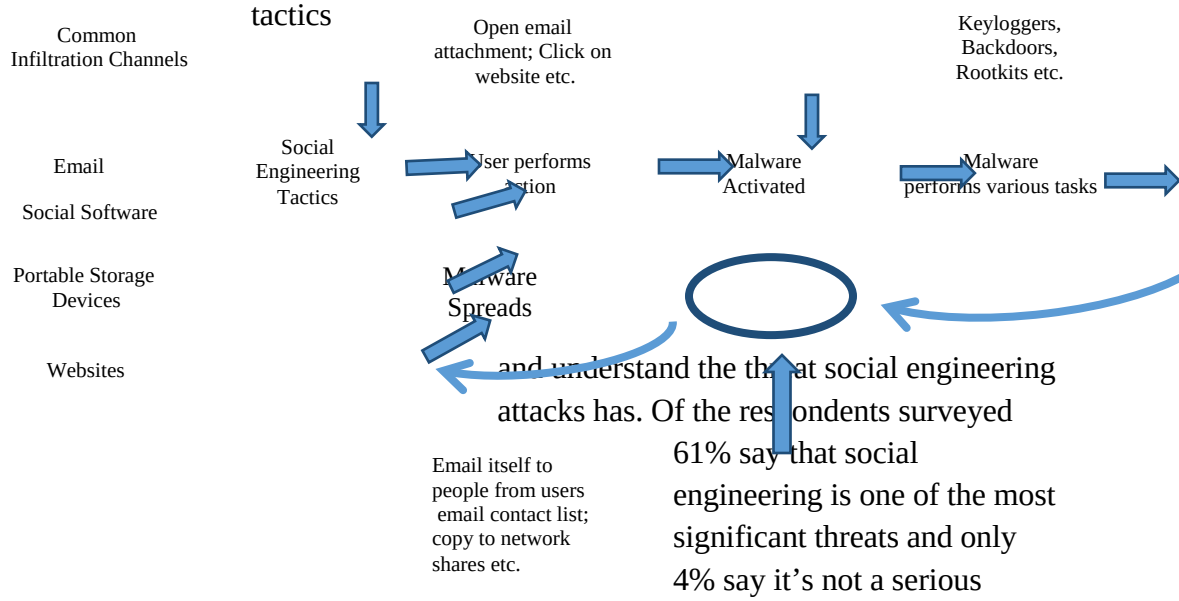


Figure 5 Malware attack [8]

VI. Attack on Companies

Social engineering attacks companies of all sizes and types. They attack for financial gain and fraud. Many companies think that as long as their computer systems are protected their company is protected. But what they don't realize it is there employees they need to secure against attacks. Agari, a company that offers data-driven security solutions, released a survey called "Email Security: Social Engineering Report." The survey was done in 2016 on 200 organization primary Healthcare, Government, Financial Services, and Education. The purpose of the survey was to see the prevalence of social engineering attacks on companies, how social engineering attacks are hurting companies, and how to defend them. In the survey 46% percent of security leaders know their company was a victim of at least one social engineering attack, and 5% rate their company defense against social engineering as superior." Security leaders know and understand the threat that social engineering attacks has. Of the respondents surveyed 61% say that social engineering is one of the most significant threats and only 4% say it's not a serious business problem. The 4% is a small number but can still can affect a company, they are probably not aware of

what social engineering can do. Employees being aware of what social engineering can do, what is it and how to stop plays an important in a company. In the survey 22% of the respondents do not know what percentage of email delivered to end users could be considered untrustworthy [9]. Just as computers have a pop –up blocker to block bad websites, employees need to be to trained to stop social engineering attacks.

A. It's Phishing Time for GoDaddy

GoDaddy customers was attacked by a phishing scam discovered by Comodo Threat Research Lab (CTRL). CTRL is an IT professional computer scientists and engineers that analyze and filter spam, phishing and malware around the world. The phishing scam targeted GoDaddy users by sending emails to the users from support@gadaddy.com. The email told the users that they no longer have any email storage and incoming emails are being rejected. The email also tells the user to upgrade their account in 24 hours or their account will be suspended. If the users click on the link in their email they can upgrade to 2 GB for free. The link in the email was http instead of https which is not a secure website [10].

B. Phishing on Campus

St. John's University was attacked by a phishing email and baiting attack. The email was sent to students asking for their email and password through e-mail correspondence. It was also sent to the employees of the school. But the employees were sent a bait social engineering attack. According to the Torch employees were baited with "performance and compensation review information."The Torch is the award-winning independent student newspaper of St. John's University [11].

1) As employees and students be aware of what a phishing emails look like.
2) Always double check the emails that are being sent to you.
3) Call the company that sent the email, if you are unsure.
4) Be careful what you post on your social media account.

Conclusion

In conclusion, there are many social engineering attacks that can occur. Social engineering are the most common attacks that a hacker uses for fraud and financial gain. These attacks aren't only limited to companies they can happen to anyone, anywhere. Be aware of social engineering attacks and remember only you can prevent them from happening.

References

[1] K. D. Mitnick, W. L. Simon, and S. Wozniak, *The art of deception: Controlling the human element of security*. Indianapolis, IN: Wiley, John & Sons, 2002.

[2]I. Ghafir, V. Prenosil, A. Alhejailan and M. Hammoudeh, "Social Engineering Attack Strategies and Defence Approaches," *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, Vienna, 2016, pp. 145-149.

[3] Z. L. Švehla, I. Sedinić and L. Pauk, "Going white hat: Security check by hacking employees using social engineering techniques," *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija, 2016, pp. 1419-1422.xxx

[4] S. Schmookler, and L. A. Block, *AXIS Insurance*, 2015. [Online]. Available: http://www.axiscapital.com/en-us/insurance-site/Documents/AXIS-Social-Engineering-Whitepaper-2-10-2015.pdf.

[5] K. Y. Abeywardana, E. Pfluegel and M. J. Tunnicliffe, "A layered defense mechanism for a social engineering aware perimeter," *2016 SAI Computing Conference (SAI)*, London, 2016, pp. 1054-1062.

[6] M. D. Ciampa, *Comptia Security+ guide to network security fundamentals*, 5th ed. Boston, MA, United States: CENGAGE Learning Custom Publishing, 2014.

[7] "Safe browsing – transparency report – Google,". [Online]. Available: https://www.google.com/transparencyreport/safebrowsing/. Accessed: Dec. 01, 2016.

[8] Sherly Abraham, InduShobha Chengalur-Smith, An overview of social engineering malware: Trends, tactics, and implications, Technology in Society, Volume 32, Issue 3, August 2010, Pages 183-196, ISSN 0160-791X, http://dx.doi.org/10.1016/j.techsoc.2010.07.001.

[9] J. Wilson, "Agari," 2016. [Online]. Available: https://www.agari.com/wp-content/uploads/2016/09/Social-Engineering-Report-ISMG.pdf. Accessed: Nov. 01, 2016.

[10] "GoDaddy users targeted with Phishing attack," DEFEND, 2016. [Online]. Available: http://defendmagazine.org/2016/08/26/godaddy-users-targed-with-phishing-attack/. Accessed: Nov. 30, 2016.

[11] B. Danquah, "Phishing attacks on campus," in *Home Scroll*, The Torch, 2016. [Online]. Available: http://www.torchonline.com/news/2016/12/03/phishing-attacks-on-campus/. Accessed: Dec. 8, 2016.

[12] Chubb Group of Insurance Companies "Guide to preventing social engineering fraud" 1st ed. 2016. Print http://www.chubb.com/businesses/csi/chubb19441.pdf

[13]M. Gupta and S. Agrawal, "A SURVEY ON SOCIAL ENGINEERING AND THE ART OF DECEPTION," *nternational Journal of Innovations in Engineering and Technology (IJIET)*, vol. 1, no. 1, Jun. 2012.