Computing, Information Systems, Development Informatics & Allied Research Journal
Vol. 7 No. 3 September, 2017 - www.cisdijournal.org

Social Engineering Techniques and Mitigating the Associated Security Risks

[1]Adenekan, O.A. & [2]Durosinmi, A.E
[1&2]Department of Computer Engineering
Moshood Abiola Polytechnic
Abeokuta, Ogun State. Nigeria.
E-mail: adenekanolujide@yahoo.com[1], cunlexie@hotmail.com[2]

ABSTRACT

Social engineering is an ancient tactic, exploiting human weakness, ignorance, fear, Uncertainty, and vanity, to manipulate victims for personal gain. Today, with users putting more of themselves online in the "social web world," social engineering scams have rapidly risen to become the most prevalent type of online security threat. Whether through email, IM, Facebook or dozens of other social media outlets, it's far too easy for scammers to con well-meaning individuals into providing access and information. Attackers increasingly employ social engineering tactics to exploit natural human predispositions with the goal of bypassing defences. Such approaches can persuade victims into clicking on malicious links, open exploit-laden attachments and install malicious software. In this paper we have studied Social Engineering Attack in detail (including attack process and classification of Social Engineering attack) and reviewed some of the existing techniques along with their advantages and disadvantages and also make recommendations on how both can be mitigated.

Keywords: Social Engineering, password, threat, firewalls, Attack

CISDI Journal Reference Format
Adenekan, O.A. & Durosinmi, A.E (2017): Internet of Things (IoT): I Social Engineering Techniques and Mitigating the Associated Security Risks. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 7 No 3. Pp 75-79
Available online at www.cisdijournal.org

1. INTRODUCTION

Simply, social engineering is psychological exploitation: the manipulation of reason, logic and relationships to get people to do something which presents a risk or a threat. It's all about capitalizing on relationships people have with those they know, their "circle of trust", manipulating them to divulge information, or outright posing as a trusted source to do the same. Social engineers appeal to authority, vanity, emotion or logic using verifiable facts and figures to gain access to money, information, anything of value. Social engineers also rely on the natural helpfulness of people [1]. It's human nature, for instance, to hold the door open for someone carrying an armload of packages; whether they're authorized to enter is another question. Over thousands of years, social engineering has not changed its methods, only its medium. One of the primary types of social engineering on the Internet is phishing. The schemes are varied and typically involve something like this [4].

The victim receives an email, IM, or text under the guise of a legitimate and respected source with alarming news that his bank account has been compromised. It then asks the victim to enter his ID and password or other sensitive information. It's a direct, upfront request from the criminal for the personal data, which is voluntarily disclosed by the victim before he realizes he's been tricked. No matter how tight your network security or well-considered your security policy, the human element at your business remains vulnerable to hackers. But there are steps you can take to tighten your security against social engineering attacks [3].

2. RELATED WORKS

To launch a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility [1]. A social engineering attack is usually conducted by an outsider who will use a variety of psychological tricks on a computer user to get the information they need in order to access a computer or network. Do not get confused with the concept "outsider." While the true outside hackers get the headlines, the far more prevalent form of social engineering in conducted by one employee on another employee.

They uses human error or weakness to gain access to any system despite the layers of defensive security controls that may have been implemented. A hacker may have to invest a lot of time & effort in breaking an access control system, but he or she will find it easier in persuading a person to allow admittance to secure area or even to disclose confidential information. Despite the automation of machines and networks today, there is not Computer system in the world that is not dependent on human operations at one point in time or another [3]. Human's interfaces will always be there to provide information and perform maintenance of the system. Social engineering has rapidly risen from 'one of the oldest tricks in the book' to a fundamental corporate threat that can't be ignored. In fact, security experts predict that as our culture becomes increasingly dependent on information, social engineering will remain the single biggest threat to any enterprise or government security system [1] [2]. Social engineering attacks, particularly through social media sites and services like Facebook and Twitter, are one of the newer and more rapidly increasing threats.

Fraudsters have a huge, always-on, target-rich (more than 500 million!) environment at their disposal, many of whom are maintaining a constant Facebook connection through a combination of their work computers, personal computers and smart phones. Social engineering is defined as a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures. A good social engineer is not only a good actor, but is also good at "reading" people to determine what type of ploy will work best with a particular person. When a hacker combines social engineering skills with technical expertise, it becomes easy to breach almost any network. Many common Internet scams, such as e-mails purporting to be from a user's bank or Credit Card Company and asking them to go to a Web site where they're directed to fill in account information, are forms of social engineering. Some social engineers base their success on research abilities [7]. Such activities as "dumpster diving" (going through discarded paperwork to find credentials and other useful information) can also be considered a form of social engineering.

Some hackers may develop elaborate schemes to pose as building repair personnel or even temporarily take jobs as janitors to gain initial access, while others do all of their work from afar and never set foot near the physical site. A determined hacker may put days or weeks of effort into gaining the trust of a target employee [4]. This may be done in person, over the telephone or via e-mail or IM. "Reverse social engineering" is a term used to refer to hackers who create some sort of problem on the network or the user's computer and then come to the rescue (like the cases we occasionally read about where a person sets a fire and then rushes in to put it out, becoming an instant hero to the victims). This helps the social engineer gain trust quickly, and makes it easier for him/her to get desired information out of the victim. For example, the social engineer might then send an e-mailed attachment that contains malicious code through which he can gain control of the victim's computer. Because the victim now "knows" (and trusts) the engineer, the victim doesn't exercise the same caution about opening the attachment as would be the case if the attachment were from someone else[3].

3. TYPES OF SOCIAL ENGINEERING

Social engineering can be broken into two types: human-based and technology-based. Human-based refers to a person-to-person interaction to obtain the desired action. Technology-based refers to having an electronic interface that attempts to retrieve the desired outcome.

3.1 Impersonation and Important User

Of the human-based forms of social engineering, the first two are categorized as Impersonation and Important User. These two are often used in combination with one another. In the 1991 book Cyberpunk by Katie Hafner and John Markoff, they describe the actions of one Susan Hadley (aka Susan Thunder). Using an easily accessible military computer directory she was able to obtain the name of the individual in charge. She used her basic knowledge of military systems and terminology as she called a military base to find out the commanding officer of the secret compartmentalized information facility. She sweet-talked her way into obtaining the name of the Major's secretary and then hung up. Using this information, she changed tactics.

She switched from being nonchalant to authoritative. Her "boss," the Major, was having problems accessing the system and she wanted to know why. Using threats, she got the access and, according to her, was in the system within 20 minutes. Pretending to be someone you are not, or schmooze your way to the information you need [5]. cThese are typical examples of how social engineers work to obtain the information they need. They will often contact the help desk and drop names of other employees. Once they have what they need to gain further access, they will attack a more vulnerable person. Someone who has information, but not necessarily the clout to challenge anyone of "authority".

3.2 Third-party Authorization

The typical third-party authorization is when the social engineer drops the name of a higher-up who has the authority to grant access. It is usually something like "Ms. Shooter says its OK" or "Before she went on vacation, Ms. Shooter said I should call you to get this information." The social engineer may well have called the authorizing office to establish if they would be unavailable to corroborate the request. Remember, most social engineers are internal to the organization and can find this out very easy.

3.3 In Person

The social engineer may enter the building and pretend to be an employee, visitor or service personnel. They may be dressed in a uniform or become part of the contract cleaning crew. A few years ago in New York, the cleaning crew arrived just before lunch and began to go into the offices and empty the trash containers and dust. Most employees offered to get out of the way and left their office for a few minutes. Later in the afternoon the employees noticed that the trash cart was still in the hallway. The "cleaning crew" had cleaned the offices of wallets, purses and briefcases.

3.4 Dumpster Diving and Shoulder Surfing

Perhaps two of the oldest forms of social engineering are dumpster diving and shoulder surfing. The dumpster diver (now called trash trawler or garbagolist) is willing to get dirty to get the information they need. Too often companies throw out important information. Sensitive information, manuals and phone books should be shredded before disposing. In Detroit and bottled oxygen salesman bragged that he got his competitor's price list by accessing the competitor's dumpster and "rooting around like a pig." The shoulder surfer will look over someone's shoulder to gain passwords or pin numbers. A few years ago, one of the news magazine shows did a session on phone card fraud. During one sequence, the reporter was given a new phone calling card and told to use it a Grand Central Station in New York. While she made the call, the undercover police counted at least five people surfing her pin number. One even turned to the cameraman to make sure he got the number too. Within minutes the stolen card numbers were being used to make international phone calls.

3.5 Pop-up Windows

A window will appear on the screen informing the user that the host connection has been interrupted and that the network connection needs to be re-authenticated. The pop up program will then e-mail the intruder with the access information. In another scam a message saying from eBay asks the victim to submit his password and other personal information to a Web site. The e-mail typically arrives shortly after the victim's credit card had expired, so they didn't suspect the site was phony. These are called phishing scams and have been around for years but have in recent months become more numerous and sophisticated.

3.6 Mail Attachments

Programs and executable can be hidden in e-mail attachments. Vince Gallo was the first to show the vulnerability of governments and corporations to information warfare via email through his simulated Bun ratty attack. The first step to exploiting this vulnerability is to write a program that could be the "inside agent" to which the social engineer would send the covert messages. This program could be written to do anything, from sending copies of documents on the user's computer to spying on other computers on the network. It could be placed in the machine either with human assistance; for example, a collaborator inside the company, or by placing it on a Web site for download, hidden within innocent looking software: a Trojan horse. Once this Trojan software is inside the target machine, the malicious software does nothing until the attacker contacts it by sending an e-mail message to the compromised machine; the special message class allows it to be forwarded directly to the hidden folders without ever being seen by the user.

3.7 Websites

The newer trend in spam and identity theft is called brand spoofing. "Phishing" or "brand spoofing" is the process of sending an e-mail to a user falsely claiming to be a legitimate enterprise in an attempt to scam the user into disclosing private information. Government, financial institutions and online auctions/pay services are common targets of brand spoofing. The attacker sends an HTML e-mail input form within an email or an e-mail providing a link to a deceptive replica of an existing web page.

4. MITIGATING SOCIAL ENGINEERING

1. **Password Management**: Guidelines such as the number and type of characters that each password must include, how often a password must be changed, and even a simple declaration that employees should not disclose passwords to anyone (even if they believe they are speaking with someone at the corporate help desk) will help secure information assets.
2. **Two-Factor Authentication**: Authentication for high-risk network services such as modem pools and VPNs should use two-factor authentication rather than fixed passwords.
3. **Anti-Virus/Anti-Phishing Defenses**: Multiple layers of anti-virus defenses, such as at mail gateways and end-user desktops, can minimize the threat of phishing and other social-engineering attacks.
4. **Change Management**: A documented change-management process is more secure than an ad-hoc process, which is more easily exploited by an attacker who claims to be in a crisis.
5. **Information Classification**: A classification policy should clearly describe what information is considered sensitive and how to label and handle it.
6. **Document Handling and Destruction**: Sensitive documents and media must be securely disposed of and not simply thrown out with the regular office trash.
7. **Physical Security**: The organization should have effective physical security controls such as visitor logs, escort requirements, and background checks.

In addition to the items mentioned above, here are some other techniques to follow:

1. Establish security protocols, policies, and procedures for handling sensitive information. Make sure ALL employees are made aware of them. Regularly reiterate their importance.
2. Train employees in security protocols relevant to their position.
3. Identify information that is considered sensitive and evaluate its overall exposure to social engineering risk. Specify to trained personnel when, where and how this information should be securely handled and stored.
4. Identify information categories that may not be considered sensitive but could still be targeted by social engineers for the purpose of advancing their attacks.
5. Implement effective physical security controls such as visitor logs, escort requirements, and background checks for new employees or temporary workers.
6. Establish a system where sensitive documents and media are securely disposed of and not simply thrown out with the regular office trash. If not already in place, insist on the use of dumpsters with locks on them, with keys to them limited only to the waste management company and the cleaning staff.
7. Consider banning the use of non-corporate storage media such as flash drives.
8. Institute the use of a web content filtering system that allows you to block employee access to questionable and potentially malicious web sites that can lead to system compromise.

5. CONCLUDING REMARKS

Social networking websites have become a hotbed for online criminals, making literally hundreds of millions of people from all walks of life prime targets. With the emergence of interactive online communication tools such as social networks, blogs, microblogs and more, every employee and any organization can be targeted for a social engineering attack. Today's savvy social engineer scammers want to infiltrate your personal correspondence, making targets like Facebook far more interesting and profitable to them. Social engineering scams will continue to evolve and become even more convincing, more international, and more professional. Prevention begins with education about the value of information, increasing awareness of how social engineers operate, and having the right services in place to protect against attacks in real time. Today every organization, small and large, has the data and information easily monetized by criminals. Now more than ever, cyber security is everyone's business. The best way to mitigate the risk posed by rapidly evolving social-engineering methods is through an organizational commitment to a security-aware culture. Ongoing training will provide employees with the tools they need to recognize and respond to social-engineering threats, and support from the executive staff will create an attitude of ownership and accountability that encourages active participation in the security culture.

REFERENCES

1. Methods for Understanding and Reducing Social Engineering Attacks. Available online at http://www.esecurityplanet.com/views/article.php/3908881/9-Best-Defenses-Against-Social-Engineering-Attacks.htm
2. Network Attack and Defence. Available online at http://www.dummies.com/how-to/content/common-network-attack-strategies-password-attacks.html
3. Social Engineers. Available at http://www.windowsecurity.com/articles tutorials/misc_network_security/Social_Engineers.html
4. Social Engineering: Concepts and Solutions. Thomas R. Peltier Available at: http://www.infosectoday.com/Norwich/GI532/Social_Engineering.htm
5. http://security.tamu.edu/Security_for_Students/Staying_Safe/Social_Engineering_and_Phishing_ Attacks.php
6. The Risks of Social Networking. Available at http://www.symantec.com/connect/blogs/its-not-so-much-social-networking-it-social-engineering
7. The Threat of Social Engineering and Your Defense Against It. Available at http://www.sans.org/reading_room/whitepapers/engineering/threat-social-engineering-defense_1232
8. www.infosecwriters.com/text.../Social_Engineering_RMorgan.pdf
9. The New Face of Social Engineering Attacks on the Web Available at: http://www.cuiaa.org/WP_SocialEngineering.pdf
10. Social Engineering - Exploitation of Human Behavior - White paper Available at http://www.infosecwriters.com/text_resources/pdf/Social_Engineering_AThapar.pdf
11. Introduction-to-social-engineering.pdf Available at: https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/Introduction-to- - engineering.pdf
12. Social Engineering – Risks, Techniques and Safeguards Available at https://www.itegria.com/wp-content/uploads/2014/03/ItegriaSocialEngineering.pdf