Social Engineering - The Dark Art of Manipulation

Prerit Shah[1], Siddharth Nanda[2], Rajeshwari Gundla[3]
[1]U.G. Student, [2]Faculty, [3]Senior Faculty
SOE, ADYPU, Lohegaon, Pune, Maharashtra, India[1]
IT, iNurture, Bengaluru, India[2,3]

Abstract **-** In 21st century, information is the very crucial asset of any individual or organizations. Humans are often trusted with crucial information rather than trusting a computer or electronic devices of any kind. But every human being contains a weak spot for something like a pet, family, a loved one probably even their first car. This information can be used to manipulate humans and blackmailing them to leak crucial information which may lead to cyber crimes and loss of valuable data. This is known as Social Engineering. In this paper, I've discussed about social engineering, the types of social engineering attacks and defense against various social engineering attacks.

Keywords **-** Information, Confidentiality, Manipulation, Human Hacking, Psychology

I. INTRODUCTION

Every organization respective private information and employees who have access to this information. It is crucial to maintain the confidentiality, integrity and availability of this information. This is achieved by following a simple triad IAA i.e. identification, authentication and authorization. Simple questions are asked like for identification, "Do I know You?", for authentication "May i check some kind of ID?" and for authorization "Do you belong here?". If this process is compromised, then the confidentiality of the system or information is compromised, and integrity and availability of the system or information are can be compromised [1]. The Social Engineers or the con-artists of the modern day attempt to bypass the IAA trial by impersonating a person who has access of the information by manipulating this person's psychology to leak passwords or other crucial information.

II. SOCIAL ENGINEERING

Social engineering is a variety of harmful activities that are the result of human interaction. It uses psychological management to mislead users into security errors or to provide sensitive information.

Social engineering attacks require multiple steps. Victims must first seek to collect the necessary basic information about the victim, including the vulnerability of the penetration and security protocols. Later, an attacker may encourage further action to breach security practices, such as building trust in the victim, disclosing confidential information, or using critical resources. The profile of a SE attack is much like the software development life cycle (SDLC) and Mitnick states 4 distinct stages of "The Social Engineering Cycle:" research, developing rapport and trust, exploiting trust, and utilizing information[2].

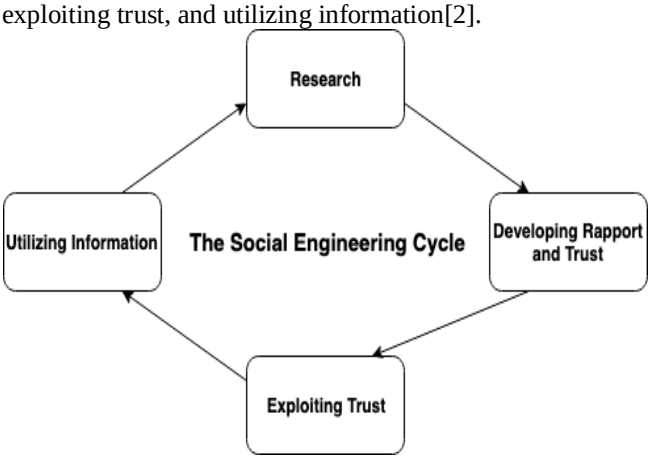

Figure 1: The Social Engineering Cycle

III. TYPES OF SOCIAL ENGINEERING ATTACKS

Individuals can be persuaded by studying their routines and analysing facts and hitting their deepest emotions Rusch refers to these paths as the "central route to persuasion" and "peripheral route to persuasion," respectively [3]. Various types of social engineering attacks are mentioned below.

A. Baiting - Cyber criminals can drop a USB drive full of malware on the target website. In addition, the agent can mark the device secretly - "confidential" or "price"[4]. The target of the bait will take the device and connect it to the computer to find out what it is. The malware will then automatically be inserted into your computer.

B. Phishing - A malicious user could send an email that appears from the source of the potential victim's trust. For example, a resource is a bank where email recipients need to click a link to access their account[5]. However, those who click the link will go to a fake website. When they enter the fake website, they actually qualify and let attackers access their bank account.

C. Email Hacking and Contact Spamming - When your friend sends an email with an link saying, "I think it's absolutely beautiful," you cannot think before opening[6]. When examining someone's email, you think you've got an email because they know what happened to your life which might easily be derived from your social media. The main objective is to distribute malware and to distinguish it from its data.

D. Pretexting - Let's say you received an email with a favorable name. The email states that you've won a cash prize and requires your private and sensitive information to prove that you are the actual recipient and to speed up the transfer[7]. Instead, there is a risk that your depositors can

access and restore your money, instead of adding it to your bank account.

E. Quid Pro Quo - A scammer may call a target, pretending to be an IT support technician. The victim can transfer his user name to the computer and think about technical support[8]. Instead, the attacker can control the victim's computer, download this malware, or steal personal information from the computer for identity theft.

F. Vishing -Vishing is a voice version of phishing. "V" means voice, but otherwise the scam is similar. Criminals use the phone to deceive victims to provide them with valuable information[9].

Table 1: Comparison of threats between types of social engineering attacks

Type	Threat Level	Advantage	Disadvantage	Environment
Baiting	Low	Complete control of the victim's system	Hardware Required	Physical
Phishing	High	Access to user credentials	Interaction with the user	Virtual
Email Hacking and Contact Spamming	High	Access to company's confidential information	Accurate prior information about the victim or organization	Virtual
Pretexting	Medium	Access to banking details	Latency in user interaction	Virtual
Quid Pro Quo	Medium	Physical Access to victims system	Risk of being identified and confronted	Physical
Vishing	High	Gaining more trust through voice	Phone number and voice can be identified	Virtual

IV. TIPS TO DEFEND YOURSELF FROM SOCIAL ENGINEERING

Social users use human behavior, such as curiosity or fear, to implement plans and to retrieve those who are trapped. So whenever you are on the email, you are attracted to a web site or when you face digital media br wary. Staying cautious can help you gaurd yourself from most engineering threats worldwide [10].

A. Consider the source - It is not advisable to direct attach a USB drive that you found in the park. It can be loaded with malwares and you might lose your valuable data. Also, don't open emails and attachments from unknown sources.

B. Use Multifactor Authentication - In case your login details have already been compromised, multi factor authentication can protect the confidentiality of your information.

C. Keep your defense softwares updated - Out of all, 83% users becomes targets of cyber-attacks because their antivirus softwares or firewalls are not up-to-date. Don't be that guy.

D. Slow Down - Attackers usually count on their victims to act fast. If you find anything odd, slow down, analyze the situation and act accordingly.

V. CONCLUSION

Social Engineering has been used for ages and will be used for a long time because it depends on curious human psychology. Organizations and individuals must equip themselves with the techniques used by social engineers to understand the risk better and have a better chance of defending such attacks. Good practices will keep most cyber crimes away.

VI. REFERENCES

[1]. Tim Thornburgh, Social Engineering: The "Dark Art", Kennesaw State University

[2]. Mitnick, K. & Simon, W. (2002) The art of deception: Controlling the human element of security. Indianapolis, Indiana: Wiley Publishing, Inc.

[3]. Rusch, J. (1999, June 24) The "social engineering" of Internet fraud. Paper presented at the 1999 Internet Society's INET'99 conference. Retrieved June 6, 2004 from http://www.isoc.org/isoc/ conferences/inet/99/ proceedings/3g/3g_2.html

[4]. Daan Wagenaar, Yannick Scheelen, Dimitar Pavlov: USB Baiting,Universiteit van Amsterdam

[5]. Tom Jagatic, Nathaniel Johnson, Markus Jakobsson, and Filippo Menczer:Social Phishing, School of Informatics, Indiana University, Bloomington, December 12, 2005

[6]. Garrett Brown, Travis Howe, Micheal Ihbe, Atul Prakash, and Kevin Borders:Social Networks and Context-Aware Spam, University of Michigan, Department of Electrical Engineering and Computer Science

[7]. Ivaturi, Koteswara and Janczewski, Lech, "A Taxonomy for Social Engineering attacks" (2011).CONF-IRM 2011 Proceedings. 15.http://aisel.aisnet.org/confirm2011/15

[8]. F. Mouton, M. M. Malan, L. Leenen and H. S. Venter, "Social engineering attack framework," 2014 Information Security for South Africa, Johannesburg, 2014, pp. 1-9.doi: 10.1109/ISSA.2014.6950510

[9]. https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html (Accessed on 08/04/2019)

[10]. https://www.imperva.com/learn/application-security/social-engineering-attack/?utm_campaign=Incapsula-moved (Accessed on 08/04/2019)