MAT JOURNALS

Journal of Information Technology and Sciences
Volume 5 Issue 1

# Social Engineering: A Technique for Managing Human Behavior

***Neetu Bansla[1*], Swati Kunwar[2], Khushboo Gupta[1]***
*[1]Assistant Professor, Department of CSE, VCE, Meerut, UP, India*
*[2]Assistant Professor, Department of AS, VCE, Meerut, UP, India*
***Email:****neetu.bansla@vidya.edu.in*
***DOI:***

***Abstract***

*Social engineering uses human behavior instead of technical measures for exploring systems, differentdata, thingsthat are of any profitable use. This piece of research gives a briefing on how human mind is capable of invading into crucial systems or capturing useful information regarding people or organizations. Certain defense mechanisms and preventive measures are also covered in this paper. Social engineering is a human behavior based technique for hacking & luring people for sneaking into someone's security system. Since social engineering relies heavily on human behavior, no hardware or equipment can be made to stop the losses, which arise as a result of human interaction. Therefore, certain good practices are suggested.Moreover, the purpose is to create awareness and study the impact of social engineering on the society.*

***Keywords:****Social engineering, data, human, information*

## INTRODUCTION

A simple definition of social engineering says that it is a non-technical way of thrashing someone's security system & stealing the crucial stuff like any data or information. Sometimes social engineering can also be considered as a way of spoofing someone's identity thereby creating a bluff. Often people are mistaken for taking human interactions lightly & share their key information with other persons, who can be known or unknown. So far only some preventive measures are suggested like-use of strong passwords, two factor authentications, not sharing of passwords. [1][2].Social engineering is difficult to handle as it is an uncommon way of breaching into someone's system as it relies heavily on trickery & psychological manipulation rather than technical counter measures[1][3][16]. Moreover, a skeptical message or email should be avoided which asks for a person's personal details & bank account details. Legitimacy of a message can be often verified by checking the domain name of the source or the sender.

Social engineering is a multistep process. Firstly, the necessary information about the target is gathered such as weak security points, possible ways of entry, individualbackground. After that the attacker plans for the attack by gaining victims trust & provide stimuli for subsequent actions for breaking security measures thereby revealing sensitive information or giving access to restricted resources [2].Issues like social engineering attacks can be avoided by retaining high level of awareness and vigilance towards forgeries and identity spoofing in the name of social human interactions. Based on a specific type, the social engineering attacks are categorized in various classes discussed further in this paper.

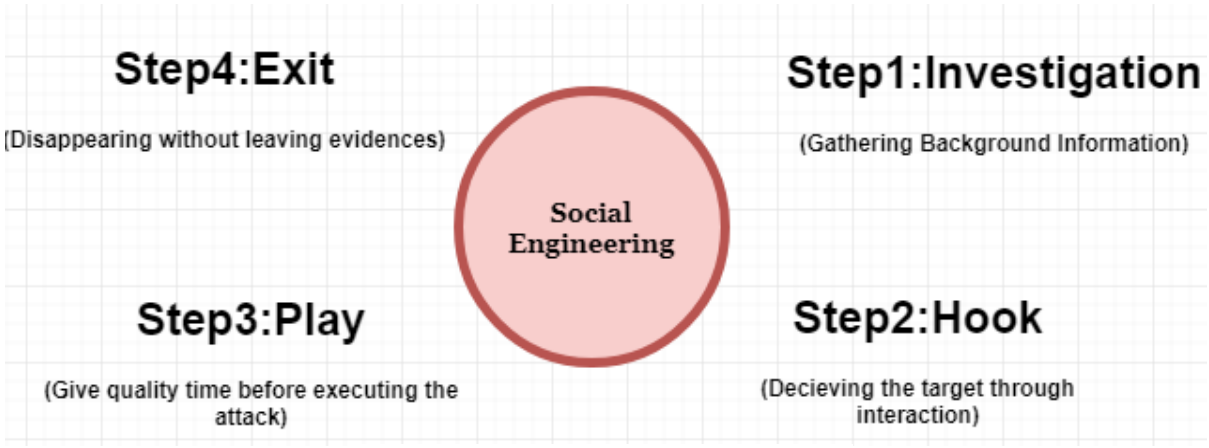


***Figure 1:*** *Social Engineering Life Cycle*

## SOCIAL ENGINEERING ATTACK TECHNIQUES

Social engineering attacks can be accomplished in any place which has human interaction involved as it has divergent or various forms. The five subsequent occurring of digital social engineering strikes are:

**Phishing-** These schemes are the emails and text messages whose main concern is to promote a sense of seriousness, necessity, strangeness or panic in the targeted person. It is famous social engineering strike. This scheme prompts them to disclose or release vital information by opening links to hostile websites or clicking attachments that accommodate malware. In Phishing technique the homogeneous messages are sent to all users. [4].

**Spear Phishing-**This is the more focused version of the phishing scheme as in this the striker selects certain people or companies. Spear phishing technique needs more attempts on part of the striker and it may take a considerate time as to pull this scheme off. These schemes are done expertly therefore making them mostly undetectable. In this the striker customizes the messages established on features, job positions and contact possession of the targeted person as to make the attack less noticeable or observable [4].

**Baiting**Baiting involves a faulty assurance to stimulate provoke the targeted person's material or curiosity. This scheme persuades the users in such a way that they confine them and steal all their vital data or impose a malware in their system. Physical Media is the savage form of Baiting which is used to diffuse the malicious malware in the system. The targeted person clicks the bait because of his/her curiosity and then places it in work or home computer evolving it in automatic installation of malware. Tempting and Attractive advertisements which guides to harmful sites or urges the users to download a malware- infected application are the online form of Baiting Scheme.

**Scareware**This scheme includes the victims who are flooded with flawed panic and counterfeit ultimatum. Scareware is also mentioned as deceitful software or fraudware. It is diffused through spam emails which doles out fraudulent threats or create offers for users to buy harmful services. Users are mislead to believe that their system is damaged by the malware, persuading them to instate software that has no benefit to the person but the striker or it is a malicious malware itself**.**

**Pretexting**The scheme is initiated by a person pretending to need crucial information from a sufferer as to carry out an evaluative task. The striker obtains data through ingenious crafted lies. He/she

interrogates in such a way that sufferer's identity is confirmed and through this they assemble the crucial data. The striker begins by developing as a co-worker, police, tax officials who have the authority to know things. [4].

## TYPES OF SOCIAL ENGINEERING SKILLS

Following are the few Skills to exploits user to get access to your system.

**Impersonating Staff:** This is an art of discovering situation to convince a target, which can be a person or a computer to release information or perform an action. This is conducted mostly via telephone or emails. Most influential and danger hoax for attainment of physical access to any system is to pretend to be somebody from inside the corporation. Some users may gave their password to a "unfamiliar person" on a phone call, thinking him to be the member of IT staff. This is specifically true if the caller indicates that their account may be restricted/disabled and that they might not be able to access important e-mails or access needed network shares if they do not cooperate. It is the most time consuming attack as it requires investigation and research to get data and information regarding target to establish the legality in the mind of target[8][9].

**Intimidation Strategies:** In this case, the social engineer tries to pretend as somebody important like a big boss from headquarters, an inspector from the government, a top client of the company, or someone else who can assault fear into the heart of regular employees. He or she comes storming/raid in, or calls the victim up, already screaming, yelling, angry, irritated or annoyed. They may also threaten the employee to fire if they do not get the information they need [9] [14] [17].

**Hoaxing:** A hoax is an effort or attempt to trick and pretend the individuals into trusting somewhat "false" are "real". It also may lead to sudden decisions being taken due to fear of an untoward incident.

**Playing on user's Sympathy:** The social engineer may make-believe to be an employee from outside, perhaps from the phone company or the company's ISP-Internet service provider. Nature of people is to help a person who is in trouble [9].

**Creating Confusion:** Another trick involves first creating a problem and then taking advantage of it. It can be as simple as setting off a fire alarm so that everyone will vacate the area quickly, without locking down his or her computers. Social engineers can then use a logged-on session to do their dirty work [10] [14].

**Reverse Social Engineering:** An even trickier practice of social engineering take place when a social engineer gets and makes others to ask him or her questions instead of questioning them. These social engineers usually have to do a lot of planning, preparation, scheduling, forecasting, research and investigation to pull it off, placing themselves in a position of seeming authority or expertise [11].

**Mail:** The use of an interesting subject line triggers and activates an emotion that may leads to accidental participation from the social engineer. There are two common forms. The first involves malicious code; this code is usually hidden within a file attached to an email. The intention is explained in an International journal of computer [5] [12] for improving QoS of routing protocols in Mobile ad hoc networks.

**Dumpster Diving:** Someone from the company throwing away junk mail or routine mail / letter of the company without ripping the document. If the mail contained personal information, or credit card offers, that dumpster diver could use to carry out identity theft. Dumpster diver also searches for information like company

organization chart, who reports to whom, especially management level employee who can be impersonated to hack important detail. Dumpster diving information can be used in impersonation attack [10] [11].

## SOCIAL ENGINEERING PREVENTION

Social engineers influence human emotions such as peculiarity or panic to proceed the schemes and lure the victims in their confines. Hence always be cautious whenever you sense distress by an email, tempting to an offer which is exhibited on a website or when we come over random digital media lying about. Our attentive existence can assist us in shielding our self in case of social engineering attacks in digital world. Subsequent points assist us to enhance our surveillance in relation to social engineering hacks. [5].

**Don't open emails and attachments from suspicious sources** – The email addresses are bluffed all the time, an email supposedly approaching from a reliable source may have actually been commenced by an attacker. Never reply an email whose sender you don't know and if you are acquainted but are doubtful about their messages, verify and authenticate the news from other sources like telephones or service provider's site, etc.[5].

**Use Multifactor Authentication**: One of the possessions attackers pursues isuser's credentials. Therefore use multiple verifications which guarantee the account's insurance in the case of system compromise.

**Be Wary of Tempting Offers**: if you get an offer which is too tempting or attractive you need to think many times before welcoming it. To verify whether you are dealing with a valid or credible offer or a trap, just GOOGLE it, it might help.

**Keep your antivirus/ antimalware software updated** – Be certain that your automatic updations are active or make sure to download the updated signatures first every day. Regular verification should be checked to ensure the application of updates is done then scan to find the possible infections. [6].

**Anti-Phishing Tools**-The use of this tool attach to a database of blacklisted phishing websites is suggested. These tools are unable to give full security as the phishing sites are cheap, simple to construct and lifetime is of few days. The examples are: Web sense, McAfee's anti–phishing filter, Netcraft anti-phishing system and Microsoft Phishing Filter.

**Strong Passwords**- Maintaining a strong password and changing periodically should be ensured by individuals themselves. Same passwords for all accounts are not recommended at all as the security is at risk. Some crucial data is kept in phones by some people so make sure they have passwords in them. Compliance on office network should be assured by the organization.

**Education and Training**- This includes progressing security awareness and training programs to develop employees in approaches to resist social engineering. It should involve periodic prompting about the essentials of security consciousness.

## CONCLUSION

Information security is very significant in present-day scenario. Moreover, the safety about information is continuously improving, the one fragile fact is that the human being who is susceptible to use such methods and techniques. The social engineering attacks concentrations on attacking the human behavior with the purpose to achieve a specified goal; in this case, it is to gain privileged and confidential information. Social engineering used different methods for

avoiding performed security attack. Psychosomatic attack and physical attack are type social engineering attack technique [13]. This paper has highlighted most fundamental social engineering attacks and has stated the general counter-measures for social engineering and further more alleviation schemes can be in motivation.

**REFERENCES**

1. Francois Mouton, Mercia M. Malany, Louise Leenen and H.S. Venterz, "Social Engineering Attack Framework", IEEE/2014.
2. Aisha SuliamanAlazri, "The Awareness of Social engineering in Information Revolution: Techniques and Challenges", IEEE/2015.
3. Osuagwu E. U. and Chukwudebe G. A, Salihu T., Chukwudebe V. N., "Mitigating Social Engineering for Improved Cyber security", IEEE/2015.
4. M. NazreenBanu et al, "A Comprehensive Study of Phishing Attacks"/ (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 , 2013, 783-786.
5. Chirillo, John. "Hack Attacks Denied" A Complete Guide to Network Lockdowns for UNIX, Windows, and Linux, Second Edition". Second Edition". John Wiley & Sons, Inc. 2002.
6. Heur, Richard. "Theft and Dumpster diving". Defense Security Service Academy. March 1996. URL: http://www.mbay.net/~heuer/T3method/Theft.htm
7. Hillary, Bob. "SANs Security Essentials". SANS Conference. July 2003.
8. Robinson, Jarvis. "Internal Threat-Risks and Countermeasures". Version 1.0. November 15, 2001. URL: http://www.sans.org/rr/papers/60/475.pdf
9. Hu, Jim. "AOL boosts email security after attack." CNET News. September 21, 2000. URL: http://news.com.com/2102-1023_3-242092.html?tag=st_util_print
10. CERT Coordination Center. "CERT Advisory CA=1991-04 Social Engineering". September 18, 1997. URL: http://www.cert.org/advisories/CA-1991-04.html
11. Granger, Sarah. "Social Engineering Fundamentals, Part II: Combat Strategies". Security Focus. January 9,2002. URL: http://www.securityfocus.com/printable/infocus/1533
12. Granger, Sarah. "Social Engineering Fundamentals, Part I: Hacker Tactics". December 18, 2001.
13. National Cooperative Education Statistics Task Force. "Protecting Your System Physical Security" 2002. URL: http://nces.ed.gov/pubs98/safetech/chapter5.asp (4 April 2003).
14. Mitnick, Kevin. The Art of Deception – Controlling "The Human Element Security". Indianapolis: Wiley Publishing Inc., 2002.
15. Gaudin, Sharon. "How To Thwart The Social Engineers" 10 May 2002. URL: http://itmanagement.earthweb.com/secu/article.php/1041161 (11 March 2003).
16. Burton, Graeme. "Companies exposed to 'social engineers' — Mitnick" 4 September 2002. URL: http://www.infoconomy.com/pages/news-andgossip/group66338.adp (11 March 2003)

***Cite this article as:***