SOCIAL ENGINEERING- ATTACKS AND PREVENTIVE MEASURES

Dr. Nidhi Sriavstava

Assistant Professor
Amity Institute of Information Technology,
Amity University, Lucknow, India

Abstract : Security of data is an important concern for any organization or individual. People take various measures to protect their system and data from any type of breaches. As the hacker finds it difficult to access the system or confidential information of the individual they are now using social engineering as a way to gather secret information. Social engineering is a method in which the human psychology is used to gather confidential information about organization or individual from the user. The hackers portray in such a way that the people tend to unknowingly share their information. This paper describes about social engineering, the social engineering attack cycle and the numerous techniques used by attacker to lure victim. The paper also lists the various precautions which the individual can take to prevent such attacks.

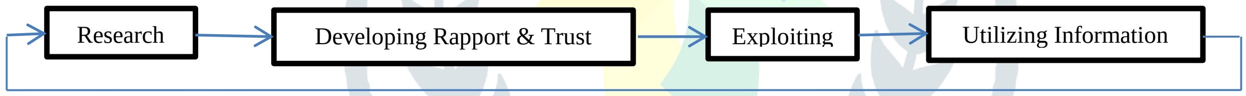
***IndexTerms* - social engineering, phishing, baiting, tailgating**

I. INTRODUCTION

Social engineering is a way or methods used so as to manipulate people so that they can reveal or expose their confidential information. Engebretson (2011) defines social engineering as “one of the simplest methods to gather information about a target through the process of exploiting human weakness that is inherit to every organization.” [1]

In short we can say that social engineering refers to deceitful techniques which are designed to influence humans in the way the owner wants to. In social engineering generally innocent humans are made as targets that are very vulnerable and tend to share their personal and confidential information with the attackers [2]. This paper is divided into V sections. Section I defines social engineering. Section II gives the four phases in Kevin Mitnick’s social engineering attack cycle. Section III describes the various techniques through which social engineering attack is carried out. Section IV lists the various preventive measures which can be taken to avert these attacks. Finally Section V gives the conclusion.

II. SOCIAL ENGINEERING ATTACK CYCLE



Kevin Mitnick has given a model on social engineering attack in his book, ‘The art of deception:controlling the human element of security’. Mitcnick has described four phases and the flow between these phases. The fig 1 shows these four phases. [3]

Figure 1: Kevin Mitnick’s Social Engineering Attack Cycle [3]

The description of each of these phases is as below:

a. Research: In this the attacker tries to gather as much information as it can about the victim so that it is easy for him/her to plan the attack.

b. Development of the rapport & trust: The attacker tries to develop an emotional bonding with the victim so that the victim trusts the attacker and shares the confidential data with the attacker. This can be done by attacker by various ways like playing an authoritative role, disclosing some of the confidential information to the victim so that they develop a trust also discloses their personal information to the attacker.

c. Exploits the trust: Based on the trust established with the victim, the attacker tends to exploit and manipulate the victim and extracts the information from him/her.

d. Utilised: This is the final stage which is reached by utilizing the previous phases and the attacker reaches the goal for which this trust was developed with the victim. [3]

III. TECHNIQUES OF SOCIAL ENGINEERING ATTACK

The various ways the attacker can exploit the vulnerabilities of the individual are described below [2, 4, 5, 6,7] :

a. Phishing: In this the phisher generally uses email as a tool to deceive people. In this email is sent asking for verification of information by clicking on the link given in the email. The email is shown to be very important and the information asked in it to be very urgent which if not furnished immediately will lead to deactivation of account or leaking of information, etc. The content in the email is shown as to be sent from legitimate individual or business like a card company, bank or colleague employee. The link given when clicked leads to a fraud company page with its logo and looks like the original website of the company and asks for private and confidential information of the individual like bank account no., password, credit/debit card number, pin, etc. Phishing strikes masses by reaching out to large audience.

b. Baiting: As the name in itself tells it is a trap used to deceive people. Bait can be physical or digital. In physical baiting the attacker purposefully leaves a flash drive on desk of people which contains a malicious file with good name. As soon as the USB is inserted the infected files gets stored on the storage medium of the user. The USBs are generally named in such a way that catches the attention of the user and they are forced to open it like “Summarized salary report of the employees” etc. In the digital baiting the user while downloading the music or the movie unknowingly downloads the malware onto the system and the attacker then has full control on the data stored in the user’s systems.

c. Pop-up windows: In this while the user is working on the system suddenly a pop up window will appear which prompts the user to reenter the username and password as the network connection had temporarily been interrupted and lost. This information of the user is then used by the attackers to connect to the user’s system and gain access to the user’s data.

d. E-mail attachments: The viruses, Trojans and worms are attached as programs hidden in the email attachments. The attachments are given attractive names so that the users are attracted towards them and they tend to open them and thus storing these malicious software on their system through which the attackers gain access to the system. The first example of this type was “I love you” worm. Another method used in this is by attaching a file which looks as if it is an image with extension like jpg, png, etc. Generally a long name is used like Virat kohli image.jpg.exe. In windows this will show as Virat kohli image.jpg. The exe is hidden from the user who unknowingly clicks on this thinking it to be jpg image and thus gives access to its system. The users are also tricked by placing the malicious software in the zip file which the user needs to unzip before they can access the contents of it.

e. Email Scans: In this the users are given attractive offers like they have won hundred dollars as prize and to transfer the amount in their bank their username and password is required. A not so aware user in this case tends to fall into the trap and disclose their confidential data to the attackers.

f. Interesting Software: The user is shown a CPU performance enhancer software, antivirus software, system utility software which will improve their system if it is downloaded and installed. The victim once does this a key logger generally gets installed in their system and all the usernames and passwords of the user are then recorded by the attacker.

g. Watering Holes: In this the attacker has to do a lot of research on the victim and list out the websites which he/she regularly visits. The attacker then infects these websites with malware and then just sits and wait for the victim to fall in the trap.

h. Tailgating: Also known as piggybacking. In this the attacker takes help of the authorized person to enter into the restricted area. Commonly the person who needs to get access follows the authorized person and holds a large box or item and shows as if he/she is unable to open the door. The authorized person then tries to help him/her by holding the door for that person. The person then easily gets access into the restricted premise through the genuine person. But this only works in businesses where swipe card is not required.

IV. METHODS TO PREVENT SOCIAL ENGINEERING ATTACK

With the rampant increase in the social engineering attack various tools and techniques have been designed to reduce and prevent these attacks. Most important is that the user should be vigilant and aware of the possible ways he/she could be lured and trapped. Some of the important preventive measures which can be taken are explained below [1,8,9,10]:

a. Anti-phishing tool: These contain a database of the phishing sites which are blacklisted. But the average lifespan of a phishing site is only few days and as it is easy to build such cheap websites more such phishing sites keeps on coming up. Some examples of these are McAfee’s anti-phishing filter, Microsoft phishing filter, etc.

b. Strong passwords: Care should be taken that a long and strong password is used. Also the passwords should be changed from time to time. Also same password should not be used for all the sites and accounts so that if user gains access to one account he/she must not be able to access all the sites.

c. Training: Training should be given to the organization’s employees and individuals so that they do not fall into the trap and disclose important and confidential information of the organization or themselves.

d. Auditing and testing: Besides training, from time to time the person’s vulnerability should also be checked. Audits are necessary to check if everyone in the organization is following the policies laid down by the company.

e. Protection from social network: Individuals should be careful while adding people to their networks and should make sure that they are adding only genuine friends. Also privacy settings of the social networking sites should be such that full protection and privacy is guaranteed.

f. Emails from untrusted sources: Emails received from untrusted sources should not be opened by the individual or employee. Especially attachments with the emails should be verified before being opened. Also, all emails which ask for personal information like bank account no., passwords, credit card details, pin, etc. should be deleted at once.

g. Organizational policies: Proper guidelines/policies should be made and circulated among the employees of the organization on way of handling the sensitive and confidential data. Mainly Do’s and Don’ts should be clearly specified.

h. Proper disposal of data: The individual's confidential data in hard copy should be properly disposed of. Also the organization's confidential hard copies should be properly put into shredders or incinerators so that it does not land in wrong hands. Also digital data should be properly deleted.

i. Personal details should not be disclosed on public information database: The users should not disclose their personal information like date of birth, anniversary dates and other details on the public domain database as anyone can view it and use it to their benefit.

j. Secure website: User should always use a secure connection to connect to a website, especially where money transaction is being done.

k. Card statements should be checked: Transaction statement of all banks and debit/credit card should be cross checked to make sure that legitimate transactions have been done.

l. Secure SSL: Companies who are mainly based on online transactions must make sure that their SSL (Secure Socket Layer) certificates are updated and robust and are from trustable parties. Through this they can protect their company and the customers from any fraudulent attacks.

m. Lock your laptop: Whenever an employee is not at his/her workstation the laptop should be locked so that no one can access it without permission.

n. Cyber security professionals: With increase in cyber-attack, need for more cyber security professionals have gone up.

o. Two-factor authentication: In case if the attacker gets hold of the username and password, it will make it difficult to get access to the system.

V. CONCLUSION

Social Engineering is the art of taking advantage of the human flaws to achieve a malicious objective. The hacker uses non-technical methods to gather secret information. This paper highlights the ways in which the attacker acts to get the information. There is no stringent way to deal with these attacks, but there are guidelines/precautions which a user can follow to prevent them from falling into the trap. These precautions are highlighted in the paper. The above steps do not guarantee full security but definitely will reduce the chance of getting compromised

REFERENCES

[1] Nabie Y Conteh, Paul J Schmick, “Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks”, International Journal of Advanced Computer Research, Volume 6(23) pp.23-31, 2016.

[2] Breda F., Barbosa H., Morais T.” Social Engineering and Cyber Security”, Conference: International Technology, Education and Development Conference, March 2017.

[3] Francois Mouton, Mercia M. Malany, Louise Leenen and H.S. Venterz, “Social Engineering Attack Framework”, IEEE/2014.

[4] Anshul Kumar, Mansi Chaudhary and Nagresh Kumar, “Social Engineering Threats and Awareness: A Survey”, European Journal of Advances in Engineering and Technology, 2015, 2(11) pp. 15-19.

[5] Tejasvini A. Kher Swati L. Kariya, “A Survey on Social Engineering: Techniques and Countermeasures”, IJSRD, Volume 4, Issue 07, 2016, pp. 258-260.

[6] Ashish Thapar, white paper on “Social Engineering –An attack vector most intricate to tackle”.

[7] Shivam Lohani, “Social Engineering: Hacking into Humans”, Special Issue based on proceedings of 4th International Conference on Cyber Security (ICCS) 2018.

[8] Islam Abdalla Mohamed Abass, “Social Engineering Threat and Defense: A Literature Survey”, Journal of Information Security, 2018, 9, pp.257-264.

[9] Fatima Salahdine, Naima Kaabouch, “Social Engineering Attacks: A Survey”, Future Internet 2019, 11, 89

[10] Anshul Kumar1, Nagresh Kumar, “Social Engineering: Attack, Prevention and Framework”, IJRASET, Volume 4 Issue II, February 2016.