International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

A Comprehensive Study of Social Engineering - The Art of Mind Hacking

Pummy Dhiman*1, Sheikh Abdul Wajid 2, Farah Fayaz Quraishi3

*1 Assistant professor, College of Creative Studies, Vidya Jyoti Eduversity, Derabassi Punjab, India
2 Lecturer , PG Department of Computer Sciences, University of Kashmir, Srinagar, India
3 Research Scholar, PG Department of Computer Sciences, University of Kashmir, Srinagar, India

ABSTRACT

The objective of this research is to presents and demonstrates what social engineering is and how one can use this to hack the human mind for capturing useful information about organizations or individuals and how they can be prevented. A questionnaire has conducted accordingly to determine the awareness of social engineering. Since there is neither hardware nor software available to install in human being to protect against social engineering, it is essential that good practices be implemented. This work contains some current scientific, technical and psychological information on the topic of social engineering today.

Keywords : Social Engineering, Phishing, Information Security

I. INTRODUCTION

For any organization information act as a backbone, because it is the information on which decisions and actions are based. Therefore, information security aspects are very important, as it is the information and details of the organization that can help any hacker to have a complete control over the organization. Any organization that is using the best security technologies by spending as much money as it can is still totally vulnerable.[4]

If we ask any security professional and he will tell you that the weakest link in the security chain is the human who accepts a person or scenario at face value. Why bother developing and planning a sophisticated technical hack when you could just trick someone into giving you access to anything you want? This art is known as social engineering.

From technical aspect, Social engineering comes under access attack, in which an intruder can trick a member of an organization into giving over valuable information, such as locations of files, and servers, and passwords, the process of hacking is made much easier.

What is Social Engineering?

Social engineering is the art of manipulating people into performing actions or revealing confidential information. The term typically applies to trick the target for the purpose of information gathering, fraud, identity theft or gaining computer access. [2][8]

What is a social engineering attack?

In a social engineering attack, an attacker uses human interaction i.e. social skills to obtain information about an organization or its computer systems. An attacker may appear to be respectable, possibly pretend to be a new employee, repair person, or specialist and even offer credentials to support that identity.

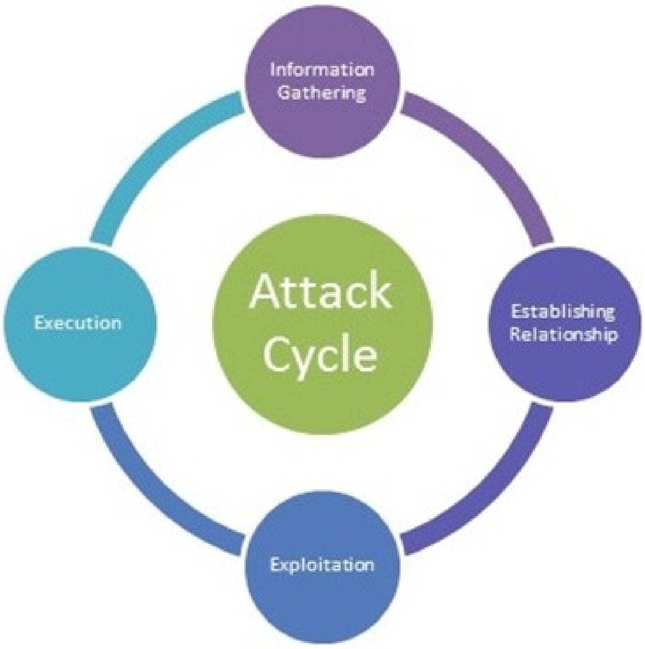
The Attack Cycle:

Social engineering only gives the information, which is up to the attacker whether he/she want to use that information to attack or not. We can say that, it is only the first step to the ladder.

There is a four-step sequence to attack to have a complete control over an organization, typically referred to as an attack cycle: information gathering, establishing relationship, exploitation, and execution.

CSEIT1726179 | Received : 15 Nov 2017 | Accepted : 04 Dec 2017 | November-December-2017 [(2)6: 543-548]

In technical attacks the targets are manipulated into believing that they are interacting with real application to provide confidential information.

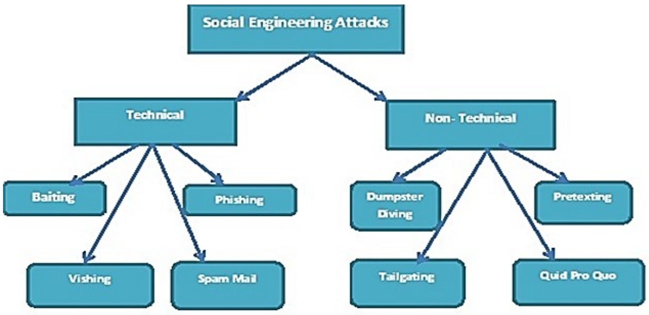


Depending on the nature of the attack and the target, the cycle can repeat several steps or even every step multiple times until the attacker gives up, or satisfies with the results. For example, an attacker may use a series of attacks to work their way to the target to achieve their goals because going straight to attack would likely fail.

Information gathering is the most time-consuming phase of the attack cycle. A social engineer can combine many small pieces of information gathered from different sources into a useful picture of the weakness of a system.

Types of Attacks

There are two categories of social engineering attacks. One comes under technical attacks and second one is non-technical attacks.



Baiting:
When you find an unknown USB flash drive, and load the device, it begins installing malware and key loggers designed to collect your personal information such as passwords onto your laptop or computer.
Never trust a website offering free downloads in exchange for information. If you do visit websites that requite your email address, create a new email address dedicated for spam and not used as your primary email account shared with friends and family.

Phishing: Phishing emails are highly crafted replica fake emails designed to appear from trusted companies. Cyber criminals send these phishing emails in hopes that you will click on their links or gain your personal information. [9]

Vishing : This term is combination of voice and phishing. Voice phishing or vishing is when someone tries to pull the same kind of trick over the phone. It is the act of acquiring private personal and financial information from the target by means of the telephone. Some attackers may use voice changers to hide their identity. Typically attackers use a technique called caller ID spoofing to make it look like calls are coming from a legitimate or known phone number.[13] Then they either ask people to provide their credit card numbers, PIN codes etc to verify their account or they give another number where the target is to call to give account details.

SMiShing: SMiShing is defined as “the act of using mobile phone text messages (SMS) to attract victims into immediate action such as downloading mobile malware, visiting a malicious website or calling a fraudulent phone number.”

Spam Mail: Email that offer job offer and contains a link that you just have to check can take over your machine and collect your contacts info and trick them just like you were tricked. Email can also contain a download–pictures, music, movie, document, etc., that has malicious software embedded. If you download you become infected. Now, attacker have access to your machine, email account, social network accounts and contacts, and the attack spreads to everyone you know.

In non-technical category the attacker take advantage of the target’s human behaviour weakness to get confidential information.

Dumpster Diving: Digging out through your trash or your company’s trash an identity thief can find enough information about you to launch an attack.

Tailgating: When someone follows your to a restricted area and asks for you to hold the door open because they claim to have forgotten their RFID card. This situation is known as tailgating. It can take on other forms such as someone borrowing your laptop or phone and installing malware.

Quid Pro Quo: Quid Pro Quo is an offer such as a free T-shirt, pen, etc. in exchange for your login information

Shoulder Surfing: It includes simply looking over someone's shoulder while they are using a computer. The attacker or the shoulder surfer look's over someone's shoulder to gain information such as passwords and pin numbers.

Social Engineering in Social Networking Sites: Social networking sites (SNSs), with their large numbers of users and large information base, seem to be perfect breeding grounds for exploiting the vulnerabilities of people, the weakest link in security. Now a day everybody is using social networking sites and providing their personal information freely. The social engineer easily creates fake account or to impersonate any identity in order to gain trust from the victim. When the victim accepts the friendship invitation, the social engineer can establish a direct connection, engage in small talk, or act as if he/she has the same interests, problems, or experiences of the victim. Moreover, being in a "friend list" of a victim, allows the social engineer to spy on posts or activities that the victim makes. Moreover, some social network sites automatically recommend new friends for the users depending on some common elements, such as friends, schools, or groups in common. This feature can lead to another important other technique of social engineering called reverse attack. In this attack, the social engineer connects to the victim's friends first, so that the victim gets tricked into contacting the social engineer him/herself [5].

II. METHODS AND MATERIAL

Survey:

To fulfil this research, I conducted a questionnaire and collected insightful opinions of participants.

The basic purpose of this survey is to collect data from targeted users. We have conducted survey among 20 users to know about the awareness of social engineering attacks in our around world. Following questionnaire is putted against users:

1. Do you know about Social Engineering?
2. Do you provide your all personal details on social networking sites?
3. Do you know what an email scam is and how to identify one?
4. My computer has no value to hackers, they do not target me.
5. Do you ever reply/click/like against any unknown friend request/post/message/video received?
6. Do you ever reply against any received unwanted email?
7. Do you read the terms and condition whenever you registering on any server/website?
8. Are your all login ID and password are totally different?
9. If you receive a phone call or email with notification that you have won the lottery prize in their organization. All that is a processing fee in order to obtain the huge amount of money that they have won. What will you do in that case?
10. Has anyone you know asked for your password?
11. Do you know who to contact in case you are hacked or if your computer is infected? How secure do you feel your computer is?
12. Is the firewall on your computer enabled?
13. If you received a call and they introduce themselves that they are part of the Bank where your Bank Account is there. They asked you to answer some questions such as your (Bank Account Number, ATM Number, ATM Password etc.).Then what will you do in that case?
14. Do you use the same passwords for your work accounts as you do for your personal accounts at home, such as Facebook, Twitter or your personal email accounts?
15. A stranger calls your house and says there is some technical support of your ISP. He/ She says that there is some problem in their Internet connection and needs your password to fix it. Is it safe to provide your password?
16. Do any unknown person or individual asks you to donate some money by showing some type of receipt of any organization, orphanage?
17. How careful are you when you open an attachment in email?
18. Is anti-virus currently installed, updated and enabled on your computer?
19. Do you know what a phishing attack is?
20. Have you ever had you email account hacked or stolen?

III. RESULTS AND DISCUSSION

Analysis of Data Collected Through Survey: We make a questionnaire and record users' response.

1. Knowledge about Social Engineering

Sample Size	Users who know about Social Engineering	User who know Little bit, but probably not all	Users who do not know about Social Engineering
20	3	9	8

2. All personal details on social networking sites

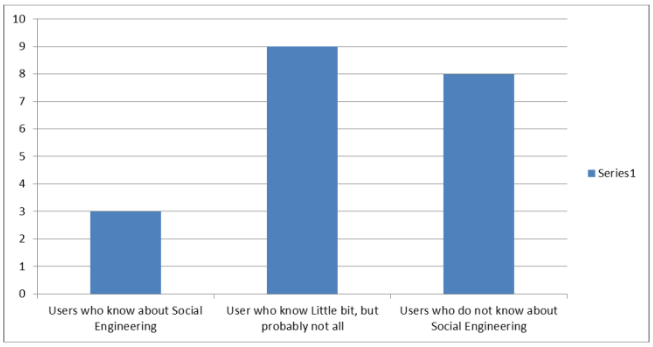
Sample Size	Users who provide all personal details	Users who do not provide all personal details
20	7	13

3. Same password for all social networking sites

Sample Size	Users who use same password	Users who do not use same password
20	8	12

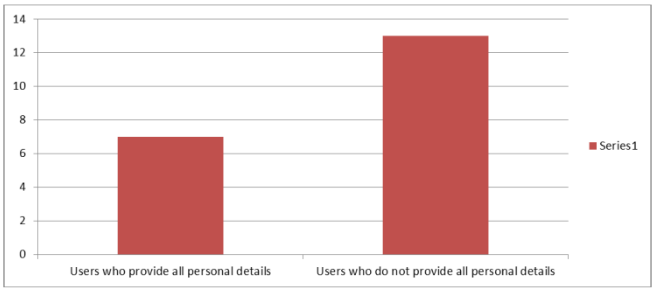
4. Users Alertness about opening an attachment in email

Sample Size	Users who make sure to know sender before opening it	Users who feel nothing wrong in it
20	8	12

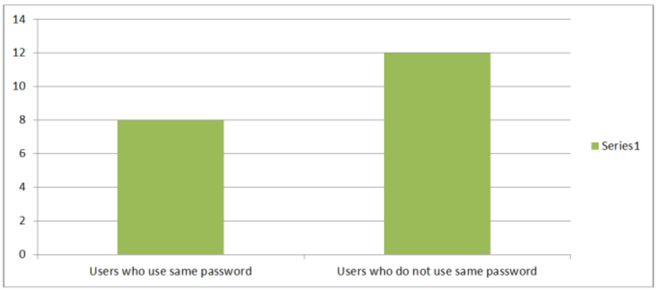


Graphs 1. Knowledge about Social Engineering

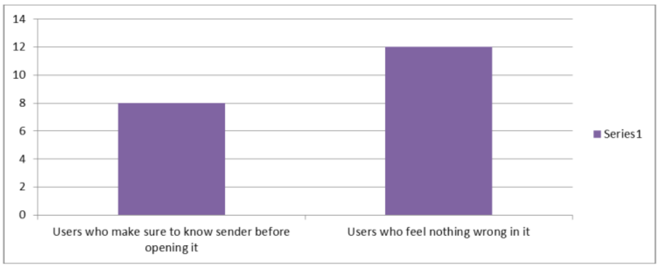
All personal details on social networking sites



Same password for all social networking sites



Users Alertness about opening an attachment in email



PREVENTION:

• Human being is the weakest link in social engineering attack, he needs to be educated about the dangers of social engineering. He needs to be trained on what social engineering is and how it can manifest itself in an organization.

• The security policy should be well-documented with sets of standards that form a strong foundation of a good security strategy. It should clearly document in simple terms, its scope and contents in each area that it applies to. The users should be following these guidelines for the policies to be effective.

✓ Audits must be conducted in order to ensure that the employees of the organization are following the policies and procedures.

✓ Slow down. Spammers want you to act first and think later. If the message conveys a sense of urgency, never let their urgency influence your careful review.

✓ The best way to protect against phishing attack is to not open anything that seems suspicious to you. Technical support will NEVER ask for your username and password since they can access this information if they need to (which they shouldn't).

- ✓ Delete any request for financial information or passwords. If you get asked to reply to a message with personal information, it’s a scam.
- ✓ Beware of any download. If you don’t know the sender personally and expect a file from them, downloading anything is a mistake.
- ✓ When a social engineering attack occurs, the victims should report the incident to the relevant personnel before any active attack is made. For example if a user gives his password to anyone, it is advisable to change the password immediately. This can reduce the impact of an attack.
- ✓ Foreign offers are fake. If you receive email from a foreign lottery, money from an unknown relative, or requests to transfer funds from a foreign country for a share of the money it is guaranteed to be a scam.
- ✓ Set your spam filters to high. Every email program has spam filters. To find yours, look under your settings options, and set these high– just remember to check your spam folder periodically to see if legitimate email has been accidentally trapped there. You can also search for a step-by-step guide to setting your spam filters by searching on the name of your email provider plus the phrase ’spam filters’.
- ✓ Secure your computing devices. Install anti-virus software, firewalls, email filters and keep these up-to-date. Set your operating system to automatically update, and if your Smartphone doesn’t automatically update, manually update it whenever you receive a notice to do so. Use an anti-phishing tool offered by your web browser or third party to alert you to risks. [10]
- ✓ Organizations should be careful about what they are posting on their company’s website. Company’s details like names of people on authority and contact numbers should be avoided.

IV.CONCLUSION

With traditional defensive security you can throw money into intrusion detection systems, firewalls, antivirus programs, and other solutions to maintain perimeter security. With social engineering no software systems exist that you can attach to your employees or yourself to remain secure. It means it is very easy for a good attacker to gather information about that organization just by gaining trust and being friendly with the user. To protect the Social Engineering, employee training & awareness is the key. Policies, procedures and standards are an important part of an overall anti-social engineering campaign. If people know what forms social engineering attacks are likely to take, they will be less likely to become victims.

V. REFERENCES

[1]. T. Bakhshi, M.Papadaki and S.M.Furnell," A Practical Assessment of Social Engineering Vulnerabilities", Human Aspects of Information Security & Assurance (HAISA 2008)

[2]. Anshul Kumar, MansiChaudhary and Nagresh Kumar," Social Engineering Threats and Awareness: A Survey", European Journal of Advances in Engineering and Technology, 2015

[3]. Anshul Kumar1, Nagresh Kumar,"Social Engineering: Attack, Prevention and Framework", International Journal for Research in Applied Science & Engineering Technology (IJRASET), February 2016

[4]. Megha Gupta and Sameer Agrawal." A SURVEY ON SOCIAL ENGINEERING AND THE ART OF DECEPTION", International Journal of Innovations in Engineering and Technology (IJIET), June 2012

[5]. Abdullah Algarni and YueXu," Social Engineering in Social Networking Sites: Phase-Based and Source-Based Models", International Journal of e-Education, e-Business, e-Management and e-Learning, December 2013

[6]. A.Karakasiliotis, S.M.Furnell and M.Papadaki," Assessing end-user awareness of social engineering and phishing",Australian Information Warfare and SecurityConference, 2006

[7]. www.us-cert.gov/ncas/tips/ST04-014

[8]. Christopher Hadnagy," Social Engineering- The art of Human Hacking",Wiley Publishing Inc.

[9]. www.hyphenet.com/what-is-social-engineering/

[10]. www.webroot.com/in/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering

[11]. www.social-engineer.org

[12]. www.social-engineer.org/wiki/archives/CommonAttacks/CommonAttacks-ClassicSE.html

[13]. www.cnet.com/news/protecting-yourself-from-vishing-attacks/

[14]. Peltier, T., “Social Engineering: Concepts and Solutions" Information Systems Security, publish 2006.

[15]. C. Anubhav, S. Dharmendra,B. Monark,S. Vrijendra ," A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model", International Journal of Information & Network Security (IJINS), June 2012ss