Social Engineering – Threats & Prevention

Amanpreet Kaur Sara*
Nidhi Srivastava**

Abstract

The term "social engineering" (SE) has gained wide acceptance in the Information Technology (IT) and Information Systems (IS) communities as a social/psychological process by which an individual (called attacker) can gain information from an individual (called victim) about a sensitive subject. This information can be used immediately to by-pass the existing Identification-Authentication-Authorization (IAA) process or as part of a further SE event. Social engineering methods are numerous and people using it are extremely ingenious and adaptable. Nonetheless, the field is new but the tactics of the attackers remain same. Therefore, this paper provides an overview of the current scenario in social engineering and the security issues associated with it.

Keywords: Cyber security; risks; hacking; social engineering

I. Introduction

A typical misunderstanding regarding cyber-attacks/ hacks is that a very high end tools and technologies are used to retrieve sensitive information from someone's account, machines or mobile phones. This is essentially false. Hackers have discovered very old and simple method to steal your data by just conversing with you and misguiding you.[1] In this paper we will figure out how these sorts of human assaults (called social engineering assaults) work and what you can do to ensure yourself.

II. Types of Social Engineering Attacks

Here are some of the techniques that are commonly used to retrieve sensitive information.

A. Phishing

Phishing is the main type of social engg assaults that are commonly conveyed as an chat, email, web promotion or site that has been intended to imitate a real system and organisation. Phishing messages are created to convey a feeling of earnestness or dread with the objective of catching an end client's sensitive information. A phishing message may originate from a bank, the govt or a noteworthy organizations. The conversation or content of the call may vary. Some request that the customer to verify their login details, and incorporate a taunted up login page finish with logos and marking to look honest to goodness. Some claim the customer is the winner of a great prize or draw and demand access to a bank account in which to send the rewards. Some request altruistic gifts after a natural calamity or disaster.[2]

B. Baiting

Baiting, like phishing, includes offering something very attractive to a customer at the cost of their login details or private information. The "Bait" is available in both forms digital and physical. Digital say for example some music or movie file download. While downloading you get the infected files and caught into trap. Physical say for example some flash drive with a name "Annual Appraisal Report" is intentionally left on someone's desk. As its name is so attractive anybody who will come and see it will definitely insert this drive to the system and he/she will be trapped. [2, 3]

C. Quid Pro Quo

This type of Assault happens when assailants ask for private or sensitive data from somebody in return for something attractive or some kind of pay. Say for eg a customer may get a telephone call from the assailants

Amanpreet Kaur Sara*
IT Department,
Institute of Information Technology and Management

Nidhi Srivastava**
IT Department,
Institute of Information Technology and Management

who, acted like a technology expert, offers free IT help or innovation enhancements in return for login accreditations. [1,4] Another regular case is a assailants, acted like a specialist, requests access to the organization's system as a major aspect of an analysis or experiment in return for Rs.1000/- . On the off chance that an offer seems to be very genuine. Then is defiantly it is a quid pro quo.

D. Pretexting

In pretexting preplanned situation is created (pretext) to trap a targeted customer in order to reveal some sensitive information. In these type of situations customer perform actions that are expected by a hacker and he caught into the trap and reveal his/her sensitive information. [4] An elaborate lie, it most often involves some prior research or setup and the use of this information for impersonation (e.g., date of birth, Social Security number, last bill amount) to establish legitimacy in the mind of the target. [5]

E. Piggybacking

Other name for piggybacking is tailing. When a unauthorized person physically follows an authorized person into an organization's private area or system. Say for example sometimes a person request another person to hold the gate as he has forgotten his access card. Another example is to borrow someone's laptop or system for some times and installing malicious software by entering into his restricted information zone.

F. Hoaxing

Hoaxing is an endeavor to trap the people into thinking something false is genuine. It likewise may prompt to sudden choices being taken because of fear of an unfortunate incident.

III. Preventions

By educating self, user can prevent itself from the problem of social engineering to large extent. Extremely common and easy way is not to give the password to anyone and by taking regular backup of the data. There has to be strict action. Application of authentication system like smart cards or biometrics is a key. By doing this, you can prevent a high percentage of social engineering attempts. There has to be good policies for successful defense against the social engineering and all personnel should ensure to follow them. It is not about typical software system for Social engineering attacks but the people which in themselves are quite fickle. There are certain counter measures which we can help in reduction of these attacks.[18]

Below mentioned are the prevention techniques for individual defense.

A. We should always be vigilant of any email which asks for personal financial information or warns of termination of online accounts instantly.

B. If an email is not digitally signed, you cannot ensure if the same isn't forged or spoofed. It is highly recommendable to check the full headers as anyone can mail by any mail.

C. Generally fraudulent person would ask for information such as usernames, passwords, credit card numbers, social security numbers, etc. This kind of information is not asked normally by even the authorized company representative. Hence one should be careful.

D. You may find Phisher emails are generally not personalized you may find something like this "Dear Customer". This is majorly because of the fact that these are intended to trap innocent people by sending mass mailers. Authorized mails will have personalized beginning. However one should be vigilant as phisher could send specific email intending to trap an individual. It could well then be like our case study.

E. One should very careful while contacting financial institutions. It has to be thoroughly checked while entering your critical information like bank card, hard-copy correspondence, or monthly account statement. Always keep in mind that the e-mails/ links could look very authentic however it could be spurious.

F. One should always ensure that one is using a secure website while submitting credit card or other sensitive information via your Web browser.

G. You should log on and change the password on regular basis.[15]

H. Every bank, credit and debit card statements should be properly checked and one should ensure that all transactions are legitimate

I. You should not assume that website is legitimate just by looking at the appearance of the same.

J. One should avoid filling forms in email messages or pop-up windows that ask for personal financial information. These are generally used by spammers as well as phisher for attack in future.[10]

IV. Conclusion

In today's world, perhaps we could have most secured and sophisticated network or clear policies however we humans are highly unpredictable due to sheer curiosity and never ending greed without concern for the consequences. We could very well face our own version of a Trojan tragedy [11]. Biggest irony of social engineering attacks is that humans are not only the biggest problem and security risk, but also the best tool to defend against these attacks. Organizations should definitely fight social engineering attacks by forming policies and framework that has clear sets of roles and responsibilities for all users and not just security personnel. Also organization should make sure that, these policies and procedures are executed by users properly and without doubt regular training needs to be imparted given such incidents' regular occurrence.

References

1. "Ouch" The monthly security newsletter for computer users issue(November 2014)
2. "Mosin Hasan, Nilesh Prajapati and Safvan Vohara" on "CASE STUDY ON SOCIAL ENGINEERING TECHNIQUES FOR PERSUASION" in International journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC) Vol.2, No.2, June 2010
3. "Christopher Hadnagy " -A book on "Social Engineering -The Art of Human Hacking "Published by Wiley Publishing, Inc. in 2011
4. The story of HP pretexting scandal with discussion is available at Davani, Faraz (14 August 2011). "HP Pretexting Scandal by Faraz Davani". Scribed. Retrieved 15 August 2011.
5. "Pretexting: Your Personal Information Revealed", Federal Trade Commission
6. "Tim Thornburgh" on "Social Engineering: The Dark Art" published in ACM digital library Proceeding New York in infoSecCD '04 Proceedings of the 1st annual conference on Information security curriculum development page 133-135.
7. "Valericã GREAVU-ªERBAN, Oana ªERBAN" on " Social Engineering a General Approach" in Informatica Economicã vol. 18, no. 2/2014
8. Malware : Threat to the Economy, Survey Study by Mosin Hasan, National Conference IT and Business Intelligence (ITBI - 08)
9. White paper: Avoiding Social Engineering and Phishing Attacks,Cyber Security Tip ST04-014, by Mindi McDowell,Carnegie Mellon University, June 2007.
10. Book of 'People Hacking' by Harl
11. FCAC Cautions Consumers About New "Vishing" Scam, Financial Consumer Agency of Canada, July 25, 2006.
12. Schulman, Jay. Voice-over-IP Scams Set to Grow, VoIP News, July 21, 2006.
13. Spying Linux: Consequences, Technique and Prevention by Mosin Hasan, IEEE International Advance Computing Conference (IACC'09)

14. Redmon,- audit and policy Social Engineering manipulating source , Author: Jared Kee,SANS institute.
15. White paper 'Management Update: How Businesses Can Defend against Social Engineering Attacks' published on March 16, 2005 by Gartner.
16. White paper, Social Engineering:An attack vector most intricate to tackle by Ashish Thapar.
17. The Origin of Social Engineering Bt Heip Dand MacAFEE Security Journal, Fall 2008.
18. Psychology: A Precious Security Tool by Yves Lafrance,SANS Institute,2004.
19. SOCIAL ENGINEERING: A MEANS TO VIOLATE A COMPUTER SYSTEM, By Malcolm Allen, SANS Institute, 2007
20. Inside Spyware – Techniques, Remedies and Cure by Mosin hasan Emerging Trends in Computer Technology National Conference