Social Engineering Effects on Human

Janvi Sanjay Manohar

Researcher Student, Department of Information Technology,
B.K.Birla College of Arts, Science & Commerce Kalyan(Autonomous), Maharashtra, India.

---***---

Abstract - *Social engineering has become a remarkable threat to the security of business government or any institutions. Common examples of social engineering contains spearfishing attacks, pretexting, baiting, phishing, etc. These attacks contains a social engineer feed on the trust of the user to give information that will allow the social engineer to penetrate a secured system. The user may not be aware of the attack. The user is one of the most major factors which is influencing the security of the system, and these users frequently do not understand the importance of their role in information security. Culprit use social engineering tactile because it is normally easier to use our naturally tendency to trust, that it is to discover ways to hack our software. But by taking some precautions, user can reduce the risk of being a victim to social engineering frauds. While social engineering has no set recipe for success and may be tough to picture in writing, the concepts and practice of social engineering have been adapted to scenes in television and movies.*

Key Words: Phishing, Spear Phishing, Reverse Social Engineering, etc.

1. INTRODUCTION

Social engineering is the psychological manipulation of people into executing actions or revealing personal information. Employee behaviour can have a big impact on information security in organizations. Author advice that to control information security culture, following five steps should be taken i.e., pre-evaluation, strategic planning, operative planning, implementation, and post-evaluation. In conventional way, culprits commit crimes either by killing the victim and make be-leave to be the legal person or purloin confidential information from garbage, where culprit access information from scrap letters, financial records, electricity bills, and many others bills which are dumped without shredding properly. In a social engineering attack, an attacker uses human interaction (social skills) to gain or compromise information about an organization or its computer systems. An attacker may seem unassuming and honourable, feasibly claiming to be a new employee, a repair person, or researcher and even offering credentials to carry that identity. However, by asking questions, he or she may be able to piece together sufficient information to penetrate an organization's network. If an attacker is not able to collect sufficient information from one source, he or she may contact another source within the same organization and plan on the information from the first source to add to his or her credibility.

1.1 Pretexting

Pretexting is the act of generating and using an developed scenario to catch a targeted victim in a way that increases the possibility that the victim will reveal information or perform actions that would be unlikely in ordinary conditions. In detailed, this is a more choosed version of the phishing scam whereby an attacker chooses specific isolated or enterprises. They then outfitter their messages based on characteristics, job positions, and contacts belonging to their victims to make their attack less noticeable. Spear phishing needs much more attempt on behalf of the culprit and may take weeks and months to pull off. They're much difficult to detect and have better success rates if done skillfully.

A spear phishing scheme might contains an attacker who, in imitating an organization's IT consultant, sends an email to one or more employees. It's worded and signed exactly as the consultant commonly does, thereby deluding recipients into thinking it's an genuine message. The message induce recipients to change their password and gives them with a link that redirects them to a hostile page where the attacker now captures their credentials. It most frequently involves some previous research or setup and the use of this information for imitation(*e.g.*, date of birth, Social Security number, last bill amount) to set up legality in the mind of the target. As a background, pretexting can be explain as the first evolution of social engineering, and continued to develop as social engineering included current-day technologies. Current and past examples of pretexting demonstrate this development.

This attack can be used to fool a business into revealing customer details as well as by private investigators to gain telephone records, utility records, banking records and other details right from company service officers. The details can then be used to create even greater legitimacy under strong questioning with a manager, *e.g.*, to make account changes, get specific balances, etc.

1.2 Vishing

Phone phishing/vishing uses a rogue interactive voice response (IVR) system to play a legal-sounding copy of a bank or other institution's IVR system. The victim is prompted (generally via a phishing e-mail) to call in to the "bank" via a (ideally toll free) number provided in order to "verify" details. A typical "vishing" system will reject log-ins frequently, making sure the victim enters PINs or passwords multiple times, often revealing several different passwords. More modern systems transfer the victim to the attacker/defrauder, who poses as a customer service agent or security expert for further questioning of the victim.

1.3 Spear Phishing

Phone phishing (or "vishing") uses a rogue interactive voice response (IVR) system to recreate a legitimate-sounding copy of a bank or other institution's IVR system. The victim is prompted (typically via a phishing e-mail) to call in to the "bank" via a (ideally toll free) number provided in order to "verify" information. A typical "vishing" system will reject log-ins continually, ensuring the victim enters PINs or passwords multiple times, often disclosing several different passwords. More advanced systems transfer the victim to the attacker/defrauder, who poses as a customer service agent or security expert for further questioning of the victim.

1.4 Water Holing

Water holing is a selected social engineering scheme that capitalizes on the trust users have in websites they frequently visit. The victim feels safe to do things they would not do in a different situation. A careful person might, for example, purposefully avoid clicking a link in an unsolicited email, but the same person would not hesitate to follow a link on a website they often visit. So, the attacker arranges a trap for the unaware prey at a supported watering hole. This strategy has been successfully used to gain access to some supposedly very secure systems.

The attacker may set out by recognizing a group or individuals to target. The preparation contains convocation details about websites the targets often visit from the secure system. The details gathering confirms that the targets visit the websites and that the system allows such visits. The attacker then tests these websites for vulnerabilities to introduce code that may infect a visitor's system with malware. The injected code trap and malware may be customized to the specific target group and the specific systems they use. In time, one or more members of the target group will get infected and the attacker can gain access to the secure system.

1.5 Baiting

Baiting is like the real-world Trojan horse that uses corporeal media and relies on the curiosity or greed of the victim. In this attack, attackers leave malware-infected floppy disks, CD-ROMs, or USB flash drives in locations people will find them (bathrooms, elevators, sidewalks, parking lots, etc.), give them legal and curiosity-piquing labels, and waits for victims.

For example, an attacker may make a disk presenting a corporate logo, available from the target's website, and label it "Executive Salary Summary Q2 2012". The attacker then leaves the disk on the floor of an elevator or somewhere in the lobby of the target company/organisation. An unaware employee may find it and insert the disk into a computer to satisfy their curiosity, or a good aware employee may find it and return it to the company. In any case, just inserting the disk into a computer installs malware, giving attackers access to the victim's PC and, perhaps, the target company's internal computer network.

One study done in 2016 had researchers drop 297 USB drives around the campus of the University of Illinois. The drives includes files on them that linked to web pages owned by the researchers. The researchers is able to see how many of the drives had files on them opened, but not how many were put into a computer without having a file opened. Of the 297 drives that were dropped, 290 (98%) of them were picked up and 135 (45%) of them "called home".

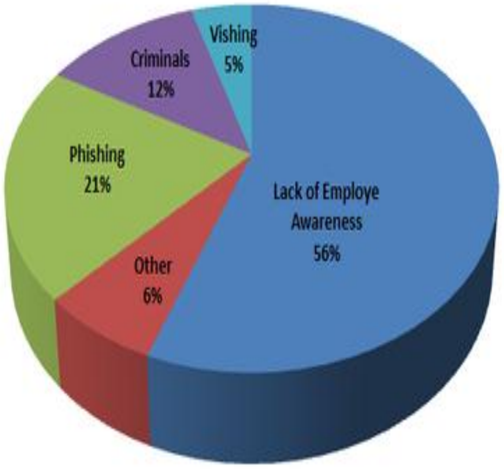

Fig-2: What's the most dangerous social engineering threat to organizations?

2. EVOLUTION OF SOCIAL ENGINEERING

In the context of information security, social engineering is emotionally controlling of people into executing actions or revealing private details. This vary from social engineering within the social sciences, which does not concern the revealing of private details. A type of confidence trick for information gathering, fraud, or system access, it vary from a regular"con" in that it is often one of many steps in a more compounded fraud scheme.

It has also been described as "any act that effects a person to take an effort that may or may not be in their best interests. "Possibly the earliest recorded account of social engineering is from the book of Genesis where it is written that the Devil, in the form of a snake played to Eve's greed by convincing her God was keeping specific powers to himself by forbidding her and Adam from eating fruit from the Tree of Life. One of the strategy in social engineer is gaining the trust of the target by positioning themselves as an ally. This can be done by using 'distrust' tactics – a strategy in which the attacker casts negative defamation on another character and then steps in as the hero. Following are steps or way how social engineering works.

1. **Information gathering**-Information gathering is the first and for the most step that requires much patience and attentively watching habits of the victim. This step is gathering data about the victim's interests, personal details. It determines the success rate of the overall attack.

2. **Engaging with victim**-After information gathering required amount of information, the attacker opens a conversation with the victim smoothly without the victim knowing anything unprofessional.

3. **Attacking**-This step usually occurs after a long period of engaging with the target and during this details from the target is taken by using social engineering. In this phase, the attacker gets the results from the target.

4. **Closing interaction**-This is the last step which includes slowly shutting down the communication by the attacker without appearing any suspicion in the victim. In this way, the motive is fulfilled as well as the victim rarely comes to know the attack even happened.

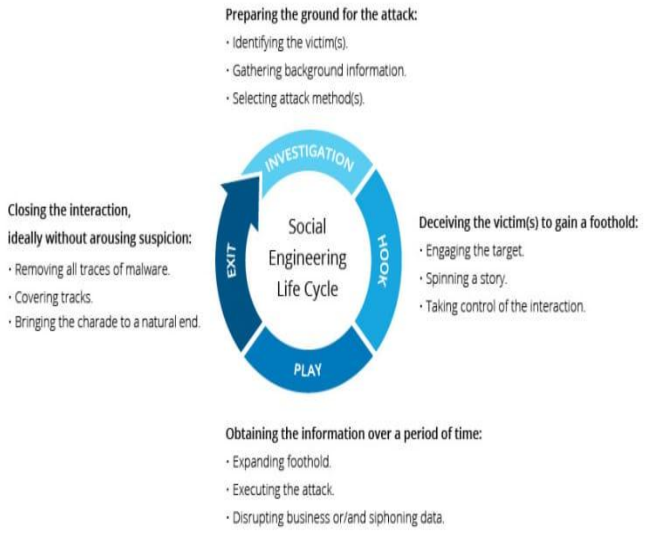
Preparing the ground for the attack:
· Identifying the victim(s).
· Gathering background information.
· Selecting attack method(s).
INVESTIGATION
HOOK
PLAY
EXIT
Social Engineering Life Cycle
Deceiving the victim(s) to gain a foothold:
· Engaging the target.
· Spinning a story.
· Taking control of the interaction.
Obtaining the information over a period of time:
· Expanding foothold.
· Executing the attack.
· Disrupting business or/and siphoning data.
Closing the interaction, ideally without arousing suspicion:
· Removing all traces of malware.
· Covering tracks.
· Bringing the charade to a natural end.

Fig-2: social engineering attack Life cycle.

3. CONCLUSIONS

Social engineering attack assumes on the tendency of the human nature to wish to be helpful, to trust people and to fear getting into trouble. It can be as good as well as bad purpose:

a) Implement an information security awareness program.

b) Needs proper recognition for everyone who performs a service.

c) Create a security alert system.

d) Implement caller ID technology for help desk and other support functions.

Educating people about the social engineering and its adverse effect can certainly decrease this type of attacks but cannot be fully prevented.

ACKNOWLEDGEMENT

I would like to thank the Department of Information Technology, B.K. Birla College of Arts, Science & Commerce (Autonomous), Kalyan and Prof. Swapna Nikale for their support in this research paper.

REFERENCES

1. 2011 Trends in Phishing Attacks: Suggestions for Future. Research Ryan M. Schuetzler University of Nebraska at Omaha, rschuetzler@unomaha.edu

2. Seidenberger, S. (2016). A new role for human resource managers: Social engineering attacks. Cornell University, 1. https://digitalcommons.ilr.cornell.edu/cgi/viewcontent.cgi?article=1091&context=chrr.

3. Mataracioglu, T., Ozkan, S., & Hackney, R. (2015). Towards a Security Lifecycle Model against Social Engineering Attacks: SLM-SEA. Cornell University, 1. https://arxiv.org/ftp/arxiv/papers/1507/1507.02458.pdf.

4. Abreu, J. V. F., Fernandes, J. H. C., Gondim, J. J. C., & Ralha, C. G. (2020). Bot Development for Social Engineering Attacks on Twitter. Cornell University, 1. https://arxiv.org/ftp/arxiv/papers/2007/2007.11778.pdf.