Social Engineering : An Inevitable Attack System

Bharath Chandra Nimmala

Computer Science and Engineering, Kakatiya Institute of Technology and Science

---

Abstract - Social engineering is the term used for a variety of malicious acts performed by people. It uses psychological deception to make security errors or to include classified information. In one or more stages, social engineering attacks occur. First, an attacker examines the target to provide details required for the assault, including possible entry points and weak safety precautions. The intruder then trusts and encourages further activities, such as the disclosure of classified information or access to essential infrastructure, that break security practices.

***Key Words*:** attacks, passwords, email, network, links.

1. INTRODUCTION

Social engineering is the way people are manipulated to give away sensitive details. The types of information these criminals seek can differ, but when targeting people, the criminals normally manipulate us to send them their passwords or bank data, or to illegally access your computer to install malware, so they can have access to and control of your passwords and banking records. Criminals employ psychological psychology techniques, and it is always better to use your innate desire to believe than to find means of hacking your apps. For example, someone is way easier to trick you than you are to try cracking your password. Safety involves learning who and what to believe.

2. WORKING OF SOCIAL ENGINEERING

Social engineers employ a wide range of attacking strategies. The first move in the majority of social engineering attacks is to investigate and investigate the target for the intruder. For example, if the objective is a company, the hacker could collect information on the structure of employees, internal activities, popular lingoes used in the industry and potential business associates, among other things. Social engineers are commonly known for concentrating on low-level, but initially accessible habits and trends such as a safety guard or receptionist; hackers can look up information on the social media accounts and examine their behavior, whether online or in person. From there, the hacker will plan and exploit the vulnerability that is found during the recovery process, based on the collected information. When the assault is complete, hackers have access to confidential data such as credit card and banking information and make money off the targets.

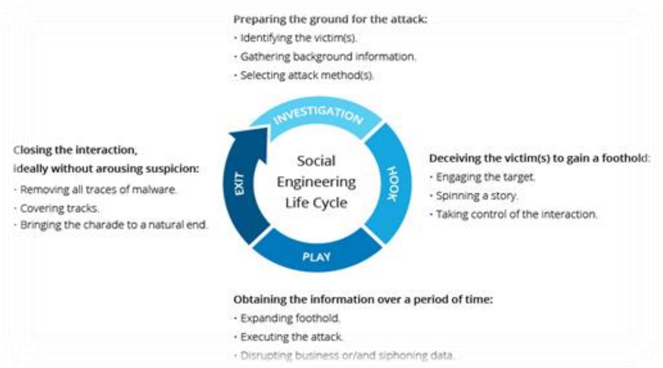
Preparing the ground for the attack:
· Identifying the victim(s).
· Gathering background information.
· Selecting attack method(s).
INVESTIGATION
Closing the interaction, ideally without arousing suspicion:
· Removing all traces of malware.
· Covering tracks.
· Bringing the charade to a natural end.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

Fig -1: Life Cycle of Social Engineering

3. SCENARIOS OF ATTACKS

3.1 Email from a friend:

If a hacker tries to crack the email password of an individual or to socially engineer it is given access to the contact list of that person–and since most people have a password anywhere, they probably have access to social network contacts of that individual too. Since the suspect has controlled this email address, he sends emails to all his associates or leaving comments on all social media of his friend or maybe on his friend's pages.

These communications will take advantage of your trust and curiosity to:

- Contain a link you really need to find out – because as you're concerned about a friend, you'll trust the link and click, then the criminals can take over your computer and gather information and mislead them, just as they're taught.
- Contains an image, audio, film, documentary, etc. download with embedded malicious software. If you download – like you presume

your buddy is probably – you get poisoned. Now the perpetrator has access and attacks to your machine, email address and social networking sites and connections.

3.2 Email from another trusted source:

These messages can use a story or pretext to:

- Request your assistance urgently
- Use attempted phishing
- Ask for donations or some other reason for a charity fundraiser
- Notifying about a lottery

Fig -2: Pictorial representation of a phisher

4. TYPES OF ATTACKS

4.1 Baiting:

Baiting is when an attacker leaves a malware-infected physical device, such as a USB flash drive, in a place it is sure to be found. The finder then picks up the device and loads it onto his or her computer, unintentionally installing the malware.

4.2 Phishing:

Phishing is where a malicious party sends fake emails, which are often said to be from a reputable source and are disguised as a genuine email. The communication is intended to deceive the user to share or click on a connection that will install malware.

4.3 Spear Phishing:

Spear Phishing is similar to phishing but suitable for a particular person or organization.

4.4 Vishing:

The use of social technology over the telephone is also known as Voice Phishing to collect confidential and financial information from the target.

4.5 Pretexting:

Pretexting is when one party lies to another to gain access to privileged data. For example, a pretexting scam could involve an attacker who pretends to need personal or financial data in order to confirm the identity of the recipient.

4.6 Honey Trap:

An attempt in which the social engineer claims to be an appealing individual for online interaction, falsifications of online relationships and the collection of classified information.

4.7 Tailgating:

Tailgating is where a hacker enters the locked building behind someone who has an approved access card, also called piggybacking. This assault presumes that a person with legal access to the building is courteous enough, provided they are required to be there, to open the door for the person behind them.

5. PREVENTION

Social engineers exploit human sentiments such as interest or anxiety to implement strategies and lure victims. Therefore, be careful anytime you feel alarmed by an email, drawn by a website offers, or come across streamlined digital media. You can defend yourself from most social engineering threats in the digital realm by being alert.

These tips will contribute to more awareness with regard to social engineering hacks:

- You don't need to reply to an e-mail if you don't know the sender in question. Even if you know them and suspect their post, search the news from other outlets, such as telephone or directly from the website of a service provider and validate them. Note that e-mail addresses are still spoofed; an intruder might have also initiated an e-mail from a trustworthy source.

- User accounts are among the most useful knowledge attackers. The use of authentication multifactor helps to secure your account if the device is compromised.
- Thinking twice before you consider an offer as a reality is too exciting. Googling will help you easily decide whether the bid is genuine or whether you're playing with a trap.
- Making sure automated upgrades are implemented or make it popular every day to import the most recent signatures. Regularly search the machine for new pathogens to verify that the patches have been applied.

SOCIAL ENGINEERING TACTICS
YOUR DATA IS AT RISK EVERYDAY THROUGH SOCIAL ENGINEERING ATTACKS.
WHY SOCIAL ENGINEERING ?
HACKING A HUMAN IS MUCH EASIER THAN HACKING A BUSINESS.
laziness
ignorance
haste
fear
attitude
trust
ATTACKERS PREY ON YOUR HUMAN WEAKNESS
carelessness
sympathy
ego
ability
greed
desire
28%
Likelihood your business will experience a data breach in the next 2 years
$3.8 M
The average cost of a single data breach in 2015

Fig -3: Image describing scenario caused by social attacks

6. CONCLUSION

Social engineering attacks are very successful because people are the most vulnerable and exploitable link in a secure network. From 2017 to 2018, attacks on social engineering doubled from 2.4 million on telephone theft, and the rate continued to rise until now. Developing policies and procedures to defend us against this type of widespread intrusion is absolutely important.

REFERENCES

1. Jessica C Flack and Raissa M D'souza, The Digital Age and the Future of Social Network Science and Engineering, Proceedings of the IEEE, 2014, 102 (12), 1873 – 1877.

2. A Karakasiliotis, M Papadaki and SM Furnell, Assessing End-User Awareness of Social Engineering and Phishing, Proceedings of the 7th Australian Information Warfare and Security Conference, 2006.

3. Thomas R Peltier, Social Engineering: Concepts and Solutions, Information Systems Security, 2006.

4. Anubhav Chitrey, Dharmendra Singh and Vrijendra Singh, A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model, International Journal of Information and Network Security, 2012, 1(2), 45 – 53.