Skillmine
Technology • Consulting • Services

infosec
Miners

SOCIAL ENGINEERING

Social engineering is not a cyber-attack. It is the skill of persuading others to disclose sensitive information, exploiting vulnerabilities in people to obtain access to private data and secure systems. In order to access a target's account, social engineering uses manipulation of people rather than computer hacking.

HOW SOCIAL ENGINEERING WORKS.

Preparation: The social engineer obtains details on their victims, including how and where they can access them, such as via email, text message, social media and other such mediums.

Infiltration: The social engineer approaches their victims, usually impersonating a trustworthy source and using the information gathered about the victim to validate themselves.

Exploitation: Social engineers request things like account logins, financial information and contact information to gather data from their targets and use that to carry cyberattacks.

Disengagement: The social engineer stops communication with their victim, commits their attack and swiftly departs.

WHAT IS THE CYCLE OF SOCIAL ENGINEERING

01 Gathering Information
In- person tactics that can be used to collect information about the targeted systems to help identify attacks vectors and targets.

02 Relationship Development
Develop a relationship with the target.

03 Exploitation
Utilizing the collected information and relationships to breakdown the target.

04 Execution
Identifying social engineering strategies that can be utilized in cybersecurity.

Source: https://twitter.com/eccouncil/status/1311191588165607424?lang=zh-Hant

SOCIAL ENGINEERING ATTACK TYPES

Scareware:
Scareware is malware that, as its name suggests, tries to scare you into acting quickly. It frequently appears as pop-up windows or emails urging you to "act now" in order to remove malware or viruses from your computer. In fact, if you do act, you might be downloading a computer virus or malware.

Email hacking and contact spamming:
It's in our nature to pay attention to messages from people we know. Social engineers are all too aware of this, taking control of email accounts and flooding contact lists with phishing messages and frauds.

Access tailgating:
Access tailgating, also known as piggybacking, is when a social engineer physically pursues or follows an authorised person into a location to which they do not have access. This can be as easy as holding the door open for another person. Once inside, they have full reign to access devices containing important information.

Phishing:
A well-known method of obtaining information from an unwary victim is phishing. What is their modus operandi? A cybercriminal, or phisher, sends a message to a target asking for information or taking a specific action that could aid in committing a more serious crime. The request might be as straightforward as asking you to open an attachment or confirm your mailing address.

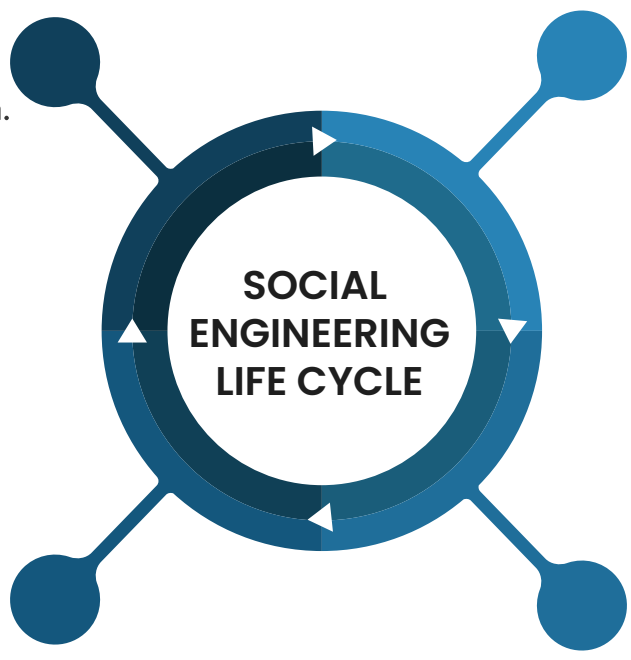
DNS spoofing:
DNS spoofing, also known as cache poisoning, occurs when a browser is tricked to route internet visitors to nefarious websites intent on obtaining critical information.

Baiting:
Baiting is based on the idea that someone will take the bait, which refers to holding out a tempting offer in front of a victim and expecting they will bite. Someone might persuade you to download a piece of music or a film on peer-to-peer platforms like social media, only for you to find out it is contaminated with malware later on.

Investigation

Preparing the ground for the attack:

- Identifying the victims.
- Gathering background information.
- Selecting attack methods.



Hook

Deceiving the victims 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.

Exit

Closing the interaction, ideally without arousing suspicion:

- Removing all traces of malware.
- Covering tracks.
- Brining the charade to a natural end.

Source: https://www.imperva.com/learn/application-security/social-engineering-attack/

COUNTERMEASURE FOR SOCIAL ENGINEERING

- Take your time and do your research.
- Don't allow a link to determine where you arrive.
- Don't share your personal information or images.
- Don't divulge important information (such passwords).
- Don't disobey regulations and procedures.
- Report any ominous behaviour.

IMPACT ON ORGANIZATION

01 Financial losses

02 Harm to reputation

03 Invasion of privacy

04 Threats from terrorism

05 Lawsuits

06 Temporary or permanent closure

07 Data theft

TECHNIQUES

Phishing involves sending out bait to trick people into divulging their information.

Pretexting (creating a false situation).

Fake websites are created to look authentic. Log in using previously-compromised actual credentials.

Malware Spread.

Fake Pop-up – Pops Appearance.

CONCLUSION

We gave a summary of social engineering assaults, current methods for detection, and available countermeasure methods through our Infosec Newsletter. These attacks can be prevented not only through the help of technology, robust security systems, cyber security experts but with the help of vigilant system users who can avoid putting their data for easy access to the preys.

SKILLMINE CYBER SECURITY TEAM

Skillmine
Technology • Consulting • Services

#46/4, Novel Tech park,
Kudlu Gate, Bangalore
Karnataka-560 068

+91 9920663515
www.Skill-mine.com
info@Skill-mine.com

India | KSA | UK | USA

Stay connected