Social Engineering Attacks

Social engineering is defined as the act of influencing and manipulating people to disclose information. Some perpetrators consider it much easier to abuse a person's trust than to use technical means to hack into a secured computer system. They have learned how to trick their targets into giving them information by exploiting certain qualities in human nature.

Fraudsters use a variety of modes of communications, such as email, internet, and telephone, to perpetrate their scheme of defrauding and manipulating customers to access their personal/ sensitive information.

Common Social Engineering Attack Techniques
Security experts recognize that most scams generally follow four stages:
a - Information Gathering
b - Relationship Development
c - Exploitation
d - Execution

This methodology, along with 'human tendency' being the weakest link in the security chain, creates a vulnerability that can have a serious operational impact.

The social engineering attack strategies fall into the following basic categories:

1. PHISHING
Phishing scams might be the most common type of social engineering attacks used today. Most phishing scams demonstrate the following characteristics:

- Seek to obtain personal information, such as names, addresses, email ID etc.
- Use link shorteners or embedded links that redirect users to suspicious websites with URLs that appear legitimate.
- Incorporates threats, fear and a sense of urgency in an attempt to manipulate the user into acting promptly.

Some phishing emails are more poorly crafted than others to the extent that their messages often exhibit spelling and grammatical errors, but these emails are no less focused on directing victims to a fake website or form where they can steal user login credentials and other personal information.

2. PRETEXTING
Pretexting is another form of social engineering attack where the attackers focus on creating a good pretext, or a fabricated scenario that they can use to try and steal their victims' personal information. These types of attacks commonly take the form of scammers who pretend that they need certain bits of information from their target in order to confirm their identity.

More advanced attackers will also try to manipulate their targets into performing an action by providing a pretext or scenario that requires disclosure of information or access to information. A good example of this would be an attacker who impersonates an external IT services auditor and manipulates a company's physical security staff into letting them into the building.

Unlike phishing emails, which use fear and urgency to their advantage, pretexting attacks rely on building a false sense of trust with the victim. This requires the attacker to build a credible story that leaves little room for doubt on the part of their target.

Pretexting attacks are commonly used to gain both sensitive and non-sensitive information.

3. BAITING

Attackers leave infected USB drives or optical disks at public places with a hope of someone picking it up out of curiosity and using it on their devices. A more modern example of baiting can be found on the web. Various download links, mostly containing malicious software, are thrown in front of random people hoping someone would click on them.

Baiting attacks are not only restricted to online schemes, and can also involve the exploitation of human curiosity via the use of physical media.

4. QUID PRO QUO

Another social engineering method Quid pro quo involves people posing as technical support. They make random calls to a company's employees claiming that they're contacting them regarding an issue. Sometimes, such people get the chance to make the victim do things they want. It can be used for normal people also.

Quid pro quo involves an exchange of something with the target, for instance, the attacker trying to solve a victim's genuine problem. The exchange can involve materialistic things such as some gift in return for the information.

5. TAILGATING

Another type of social engineering attack is known as 'tailgating' or 'piggybacking'. These types of attacks involve someone who lacks the proper authorization, following an employee into a restricted area.

In a common type of tailgating attack, a person impersonates a delivery driver and waits outside a building. When an employee gains security's approval and opens the door, the attacker asks that the employee hold the door, thereby gaining improper access through someone who is authorized to enter the company premises.

Tailgating does not work in all corporate settings. For example, in larger companies all persons entering a building are required to swipe an access card. However, in mid-sized enterprises, attackers can strike up conversations with employees and use this show of familiarity to successfully get past the front desk.

Best Practices to avoid Social Engineering Attacks:

- **Always use antivirus software on your personal devices:** There are several free and subscription based antivirus software's/ services which can be downloaded and used to keep your computer virus-free. Antivirus software's usually slows down the computer, but it is highly recommended that it is not turned off under any circumstance. Leave them on and stay protected. Upgrade your device if you think the antivirus program slows it down.

- **Always use a device firewall:** A personal or operating system firewall is an excellent line of defense against malicious software that attempts to connect out to its home server. You will receive a warning when an attempt is made, and you can optionally block the communication. Blocking the communication won't remove the infection, but it will render it mostly harmless, especially if it is one of the many "logger" infections that grabs your data as you type it into websites or client software's.

- **Keep your operating systems and software up to date:** Though it may take an extra step of system reboot, to update your apps and operating systems, and such updates may result in your device reacting slowly, it is better to ensure regular system and software updates, for your own good.

- **Never download pirated or cracked software:** Pirated or cracked software's will mostly include some type of malware. Additionally, it is illegal to steal software. If you are using a corporate computer and you download pirated software onto it, you are jeopardizing the security of your company's systems and your job because your company can get into big trouble for harboring pirated software.

- **Don't click on popup windows that tell you that your computer is infected with a virus:** Antivirus software's do not generally work that way. Those pop-ups install malware onto your computer, with your permission. Sometimes it's a scam that requires you to pay money to have the software removed by the software originator. Do not fall for it. Do not pay them to remove it if you've done it; instead look up online how to remove the malware yourself.

- **Be careful with email attachments:** Not all email attachments are harmful; but unless you are expecting an attachment from someone you know, don't download or open it until you are sure that it's okay to do so. If it is from someone you don't know, delete the email or identify it as spam and do not download or open the attachment.

- **Don't use public wifi hotspots without using a VPN (virtual private network) connection:** Do not connect to a public wifi unless you do so through a VPN. A VPN will encrypt your communications to and from the internet so that anyone who might be eavesdropping cannot steal your information.

- **Use passwords on everything and be sure that they are strong passwords:** Do not use the same password for everything. Do not use easy-to-guess passwords. Use strong passwords that are at least eight characters in length and include capitals, numbers, and special characters. Passwords protect everything: devices, email, VPN, anything that you don't want to share with others. Be paranoid and change your passwords often.

Beware of what kind of information you share on social media sites: Everyone loves social networking sites and you probably post photos on it, have conversations on it, play games on it and attach all kinds of other apps to it. By doing so, you may be putting your privacy at risk. There are companies that scan these sites and collect your data. They collect your data from public records, social media sites and from other sites that deliver malicious payloads to your devices. Keep private information private.