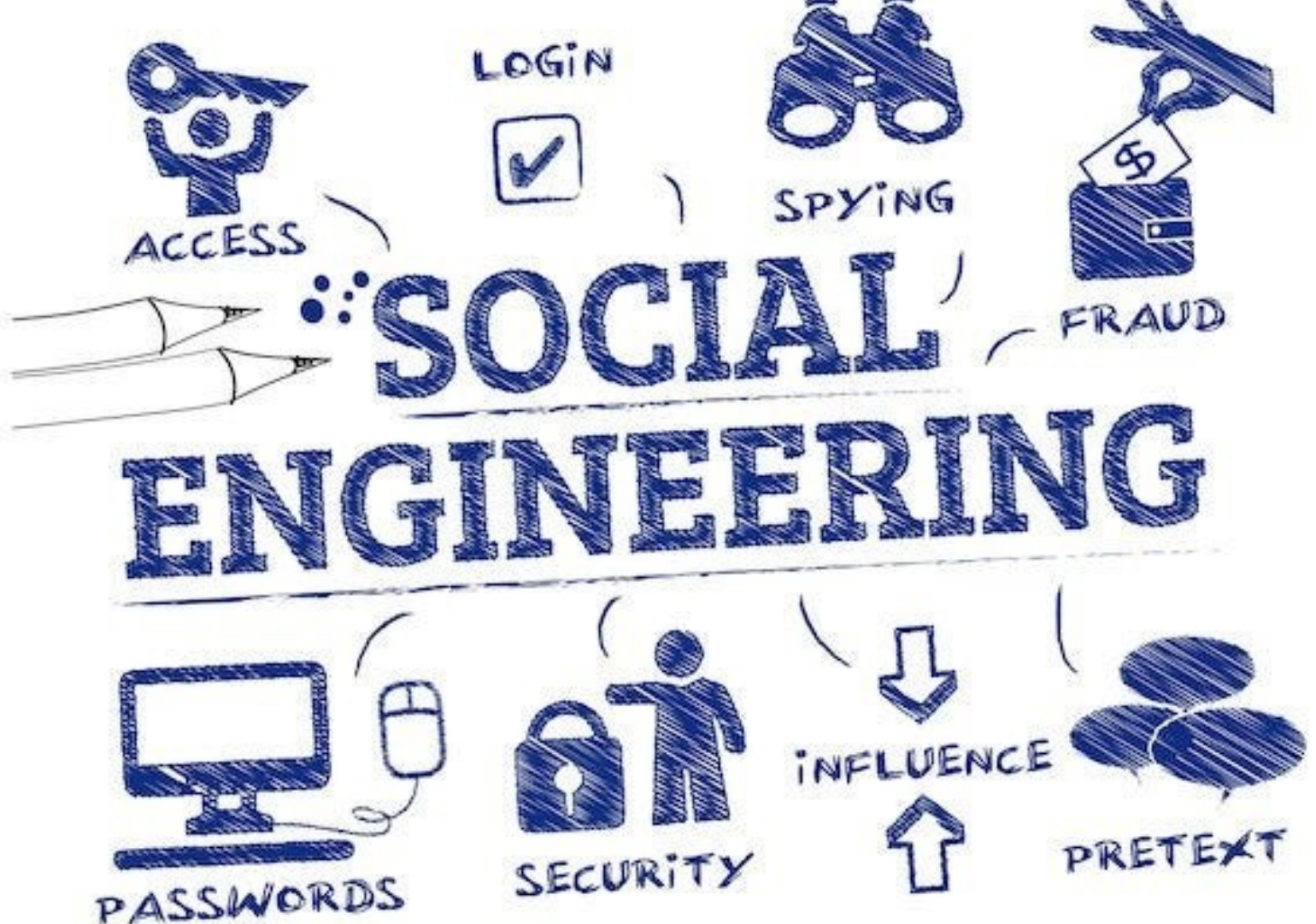
Phishing Awareness Training


LOGIN
ACCESS
SPYING
FRAUD
SOCIAL
ENGINEERING
PASSWORDS
SECURITY
INFLUENCE
PRETEXT

What is Social Engineering?

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information. The attacker moves to gain the victim’s trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.

MOST COMMON SOCIAL ENGINEERING ATTACKS

Phishing

Piggybacking

Baiting

Pretexting

Scareware

Quid Pro Quo

Impersonation

Social engineering attack techniques

- Baiting: As its name implies, baiting attacks use a false promise to pique a victim’s greed or curiosity. They lure users into a trap that steals their personal information or inflicts their systems with malware

- Scareware: involves victims being bombarded with false alarms and fictitious threats. Users are deceived to think their system is infected with malware, prompting them to install software that has no real benefit or is malware itself. Scareware is also referred to as deception software, rogue scanner software and fraudware.

- Pretexting: Here an attacker obtains information through a series of cleverly crafted lies. The scam is often initiated by a perpetrator pretending to need sensitive information from a victim so as to perform a critical task.

- Phishing: As one of the most popular social engineering attack types, phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.

How to Prevent

Social Engineering Attacks

- Don’t open emails and attachments from suspicious sources – If you don’t know the sender in question, you don’t need to answer an email. Even if you do know them and are suspicious about their message, cross-check and confirm the news from other sources, such as via telephone or directly from a service provider’s site.

- Use multifactor authentication – One of the most valuable pieces of information attackers seek are user credentials. Using multifactor authentication helps ensure your account’s protection in the event of system compromise.

- Be wary of tempting offers – If an offer sounds too enticing, think twice before accepting it as fact. Googling the topic can help you quickly determine whether you’re dealing with a legitimate offer or a trap.

- Keep your antivirus/antimalware software updated – Make sure automatic updates are engaged, or make it a habit to download the latest signatures first thing each day. Periodically check to make sure that the updates have been applied, and scan your system for possible infections.

Phisihing Prevention:

- Verify Sender Addresses: One of the simplest yet most effective ways to guard against phishing scams is to scrutinize the sender's email address. Cybercriminals often create email addresses that mimic legitimate ones, with slight alterations that can be easily missed at a glance. These alterations might include subtle misspellings, additional characters

- Beware of Urgent Requests: Another common tactic employed by cybercriminals is to inject a sense of urgency or panic into their emails. These emails often claim immediate action is required to resolve a problem, update an account, or prevent an account disruption. The goal is to rush the recipient into acting without taking the time to critically evaluate the request or verify the email's legitimacy

- Check for Suspicious Links: Hyperlinks embedded in emails are a common vehicle for phishing attacks. These links may appear legitimate at first glance, claiming to direct the user to a familiar website or service. However, they often lead to malicious sites designed to steal personal information or infect devices with malware.

- Be Wary of Email Attachments: Email attachments are another common tool used by cybercriminals to execute phishing attacks. These attachments can contain malware or viruses that, once opened, can compromise the recipient's device or the entire organization's network.
-


THANK YOU