Social engineering

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

Social Engineering is the act of manipulating people into doing something bad. This usually happens by getting someone to do something without knowing what they're doing. In this case, an attacker gets someone to reveal sensitive information or grant access to critical resources.Social engineering attacks rely on human errors. This means that mistakes made by legitimate users are more likely to be successful than those made by malicious actors.

Social Engineering Attacks - Five Most Common Types

Phishing Attack: This attack involves sending email messages or text messages to people who may be interested in your organization. These emails often appear to be legitimate requests for information or instructions, but instead contain malicious links or attachments that download malware onto users' computers.

Baiting attacks use a false offer to trick people into downloading malicious software. Physical media containing malware are left around places where people congregate, including elevators, restrooms, and parking lots.Victims pick up the bait out curiosity and insert it into their work or home computers, resulting in automatic malware infection on the system. Baited scams don't necessarily have to be carried on in the physical world. In online forms of baiting, enticing ads lead to malicious sites or encourage users to download a virus-infected application.

Scareware is a type of malware that tricks users into thinking their computers are infected by viruses, when in fact they're not. This type of malware is often used to trick people into installing other types of malware.

Scareware is also distributed via email. Spam emails distribute scareware. Users are warned about fake products and scams.

Social engineering attacks are very common nowadays. Be aware of emails, offers, and other digital media lying around. Don't fall for them!Don't open emails and attachments from unknown senders. Cross-check and confirm news from other sources. Remember that email addresses may be spoofed.Multifactor authentication is a great way to protect your accounts. Don't accept any offers that sound too good to be true. Google the topic to see if there are other ways to do what the offer says.