13.2.2 Social Engineering Facts

Social engineering is an attack that exploits human nature by convincing someone to reveal information or perform an activity. There are two forms of social engineering.

- *Passive* social engineering takes advantage of the unintentional actions of others to gather information or gain access to a secure facility.
- *Active* social engineering involves direct interaction with users, asking them to reveal information or take actions. Attackers use the following methods:
  - Assuming a position of authority (boss or network administrator)
  - Bribery
  - Forgery
  - Flattery
  - Using a disguise
  - Placing a critical timeframe on an action

Social Engineering Attack Types

There are seven main types of social engineering attacks.

- *Persuasive* social engineering entails an attacker convincing a person to give them restricted information or access.
- *Reciprocity* social engineering entails an attacker giving something of lesser or equal value to what they expect in return to the person who helps them gain access or information.
- *Social validation* entails an attacker using peer pressure to coerce someone else to bend rules or give information that they should not.
- *Commitment* social engineering entails convincing someone to buy into an overall idea, then demanding or including further specifics that were not presented up front.
- *Scarcity* social engineering entails an attacker presenting an item as a limited-time or scarce quantity offer to increase sales.
- *Friendship* social engineering entails an attacker using the premise of a friendship as a reason the victim should take unauthorized actions that benefit the attacker.
- *Authority* social engineering entails an attacker either lying about having authority or using their high status in a company to force victims to perform actions or give information that exceeds their authorization level.

Social Engineering Attack Characteristics

The following table describes common social engineering attacks.

Attack	Description
Shoulder Surfing	*Shoulder surfing* involves looking over the shoulder of someone working on a computer.
Eavesdropping	*Eavesdropping* refers to an unauthorized person listening to employees or other authorized personnel as they discuss sensitive topics.
Dumpster Diving	*Dumpster diving* is the process of looking in the trash for sensitive information that has not been properly disposed of.
Tailgating and Piggybacking	*Piggybacking* and *tailgating* refer to an attacker entering a secured building by following an authorized employee through a secure door without providing identification. Piggybacking usually implies consent from the authorized employee, whereas tailgating implies no consent from the authorized employee.
Masquerading	*Masquerading* refers to convincing personnel to grant access to sensitive information or protected systems by pretending to be someone who is authorized and/or requires that access. Masquerading is more passive than impersonating.
Phishing	A *phishing* scam is an email pretending to be from a trusted organization, asking to verify personal information or send money. In a phishing attack: - A fraudulent message (that appears to be legitimate) is sent to a target. - The message requests that the target visit a fraudulent website (which also appears to be legitimate). Graphics, links, and websites look almost identical to legitimate requests and websites they are trying to represent. - The fraudulent website requests that the victim provide sensitive information such as the account number and password. Common phishing scams include the following features: - A Rock Phish kit is a fake website that imitates a real website (such as banks, PayPal®, eBay®, and Amazon®). Phishing emails direct you to the fake website to enter account information. A single server can host multiple fake sites using multiple registered DNS names. These sites can be set up and taken down rapidly to avoid detection. - A *Nigerian scam*, also known as a *419 scam*, involves emails that request a small amount of money to help transfer funds from a foreign country. For your assistance, you are to receive a reward for a much larger amount of money

	that will be sent to you at a later date. ▪ In *spear phishing*, attackers gather information about the victim, such as identifying which online banks they use. They then send phishing emails that appear to be from the user's bank. ▪ *Whaling* is another form of phishing that targets senior executives and high-profile victims. ▪ *Vishing* is similar to phishing. Instead of an email, the attacker uses Voice over IP (VoIP) to gain sensitive information. The term is a combination of *voice* and *phishing*. To protect against phishing: ▪ Check the actual link destination within emails to verify that they go to the correct URL, not a spoofed one. ▪ Do not click on links in emails. Instead, type the real bank URL into the browser. ▪ Verify that HTTPS is used on e-commerce sites. HTTPS requires a certificate that matches the server name in the URL that is verified by a trusted CA. You can also look for the lock icon to verify that HTTPS is used. ▪ Implement phishing protections within your browser.
Caller ID Spoofing	*Caller ID spoofing* causes the telephone network to display a number on the recipient's caller ID display that implies that a call is coming from a legitimate source.
Hoax Emails	*Hoax emails* prey on email recipients who are fearful and believe most information if it is presented in a professional manner. Usually these hoax messages instruct the reader to delete key system files or download Trojan horse viruses.
Spyware/Adware	*Spyware* and *adware* are pop-up advertisements that can have malicious objectives, such as tricking users into unknowingly downloading malware or gathering information about the user and sending it to a third party for commercial gain.
Pretexting	*Pretexting* is the use of a fictitious scenario to persuade someone to perform an action or give information for which they are not authorized. Pretexting usually requires the attacker to perform research to create a believable scenario.

Social Engineering Awareness Training

The most effective countermeasure for social engineering is employee awareness training on how to recognize social engineering schemes and how to respond appropriately. There are several countermeasures you should take.

- Train employees to:
  - Protect information by:
    - Securely disposing of sensitive documents, disks, and devices.
    - Protecting sensitive information on a computer from prying eyes.
    - Protecting sensitive information from prying ears.
  - Implement online security by:
    - Verifying the validity of websites.
    - Verifying that requests for privileged information are authorized.
    - Using bookmarked links instead of links in emails to go to websites.
    - Double-checking email information or instructions with a reputable third party antivirus software vendor before implementing recommendations.
    - Never opening a suspicious email attachment.
  - Determine the value for types of information, such as dial-in numbers, usernames, passwords, network addresses, etc. The greater the value, the higher the security around those items should be maintained.
  - Not allow others to use the employee's identification to enter a secure facility.
  - Demand proof of identity over the phone and in person.
- Implement strong identity verification methods to gain access to a secure building.