3.5.3 Social Engineering Facts

Social engineering is an attack that exploits human nature by convincing someone to reveal information or perform an activity. Examples include:

- Impersonating support staff or management, either in person or over the phone.
- Asking for someone to hold open a door rather than using a key for entrance.
- Spoofed emails that ask for information or for tasks to be performed (such as deleting a file or going to a website and entering sensitive information).
- Looking on desks for usernames and passwords.

Social engineering techniques used against employees are as follows:

- Authority: an attacker either lies about having authority or uses their high status in a company to force victims to perform actions or give information that exceeds their authorization level.
- Intimidation: an attacker uses peer pressure to coerce someone else to bend rules or reveal confidential information.
- Consensus or social proof: a psychological phenomenon that occurs in social situations when people are unfamiliar with a situation and unable to determine the appropriate mode of behavior, so they mirror their behavior off of others that they assume are more familiar and better informed. Social engineers can take the lead in these situations to influence others' actions.
- Scarcity: social engineering entails an attacker presenting an item as a limited-time or scarce-quantity offer to increase sales.
- Familiarity: social engineering entails an attacker using the premise of a friendship as a reason for the victim to help them or do something unauthorized.
- Trust: social engineering entails an attacker convincing a person to give them information or access that they shouldn't.
- Urgency: an attacker fabricates a scenario of distress to convince an individual that their actions are necessary.

Specific social engineering attacks include:

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 a conversation between employees discussing 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	*Tailgating* refers to an attacker entering a secured building by following an authorized employee. With tailgating, the authorized employee does not consent to being followed.
Piggybacking	*Piggybacking* refers to an attacker entering a secured building by following an authorized employee. With piggybacking, the authorized employee does consent to being followed.
Impersonation	*Impersonation* 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. The attacker usually poses as a member of senior management.
Phishing	*Phishing* is an email attack that uses a spoofed website to gain sensitive information. In a phishing attack: ▪ A fraudulent message that appears to be legitimate is sent to a target. ▪ The message requests the target to visit a website, which also appears to be legitimate. ▪ The fraudulent website requests that the victim provide sensitive information, such as their account number and password. 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 when you visit 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.
Spear Phishing	*Spear phishing* is an attack targeted at specific individuals within a company to gain access to information that will allow the attacker to gain commercial advantage or commit fraud. Spear phishing frequently involves sending seemingly genuine emails to all employees or members of specific teams.
Whaling	*Whaling* targets senior executives and high-profile victims. It is like spear phishing, but only targets upper-level management.
Vishing	Vishing exploits voice-over-IP telephone services to gain access to an individual's personal and financial information, including their government ID number, bank account numbers, or credit card numbers.
Email Hoax	*Email hoaxes* prey on email recipients who are fearful and will believe most information if it is presented in a professional

	manner. Victims of these attacks fail to double-check the information or instructions with a reputable third-party antivirus software vendor before implementing the recommendations. Usually, these hoax messages instruct the reader to delete key system files or download Trojan viruses.
Virus Hoax	*Virus hoaxes* are false reports about non-existent viruses that often claim to do impossible things. Unfortunately, some recipients believe these hoaxes are a true virus warning and take drastic action, like shutting down their network.
Watering Hole	A *watering hole attack* is a targeted attack where the victim is a group like an organization, an industry, or a region. In this attack, the attacker guesses or observes which websites the group uses and infects one or more of them with malware. Eventually, a member of the targeted group becomes infected with the malware.

The most effective countermeasure for social engineering is employee awareness training on how to recognize social engineering schemes and how to respond appropriately. Specific countermeasures include:

- Train employees to secure 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 websites' validity
  - 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.
- Do not allow others to use employees' identification to enter a secure facility.
- Implement strong identity verification methods to gain access to a secure building.
- Require proof of identity over the phone and in person.
- If someone requests privileged information, have employees find out why she wants it and whether she is authorized to obtain it.
- Verify information contained in emails and use bookmarked links instead of links in emails to go to company websites.
- Verify information from suspicious emails by visiting two or more well-known malicious code threat management websites. You might reference your antivirus vendor or a well-known and well-regarded internet security watch group.
- Train employees to protect personally identifiable information (PII). An organization is legally obligated to ensure that employee and customer PII within its possession is protected. PII includes any information that can be used to exclusively identify an individual from others. Examples of information that could be considered PII include an individual's:
  - Full name
  - Address
  - Telephone number
  - Driver's license number
  - Email address
  - National identification number (such as a Social Security Number in the USA)
  - Credit card number
  - Bank account number
  - Fingerprints
  - Facial image
  - Handwriting sample
