13.4.2 Social Engineering Facts

Social engineering exploits human nature by convincing someone to reveal information or perform an activity. Examples of social engineering 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 tasks to be performed (such as delete a file or go to a website and enter sensitive information).
- Looking on desks for usernames and passwords.

This lesson covers the following topics:

- Social engineering attacks
- Social engineering countermeasures

Social Engineering Attacks

Specific social engineering attacks include:

Attack	Description
Dumpster Diving	*Dumpster diving* is the process of looking in the trash for sensitive information that has not been properly disposed of.
Shoulder Surfing	*Shoulder surfing* is looking over the shoulder of someone working on a computer.
Piggybacking	*Piggybacking* refers to an attacker entering a secured building by following an authorized employee. This is also called *tailgating*.
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. - The attacker usually poses as a member of senior management. - A scenario of distress is fabricated to the user to convince them that the actions are necessary.
Eavesdropping	*Eavesdropping* refers to an unauthorized person listening to conversations of employees or other authorized personnel discussing sensitive topics.
Phishing	*Phishing* uses an email and 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 the victim to provide sensitive information such as the account number and password. Hoax virus information email are a form of a phishing attack. This type of attack preys on email recipients who are fearful and will believe most information if it is presented in a professional manner. All too often, the 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 horses.

Social Engineering Countermeasures

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 demand proof of identity over the phone and in person.
- Define values for types of information, such as dial-in numbers, user names, passwords, network addresses, etc. The greater the value, the higher the security around those items should be maintained.
- Keep employees up-to-date on local regulations applicable to your industry, such as PCI data security standards,

General Data Protection Regulation (GDPR), and Protected Health Information (PHI).

- If someone requests privileged information, have employees find out why the person wants it and whether the person is authorized to obtain it.
- Verify information contained in emails and use bookmarked links instead of links in emails to go to company web sites.
- Dispose of sensitive documents securely, such as shredding or incinerating.
- Dispose of discs and devices securely by shredding floppy discs or overwriting discs with all 1's, all 0's, then all random characters.
- Verify information from suspicious emails by visiting two or more well-known malicious code threat management websites. These sites can be 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
