3.1.8 Phishing and Internet-Based Technique Facts

Users interfacing with the internet either through email or browsing websites can pose substantial security threats to an organization. Attacks that entice users to provide sensitive information or click a link that installs malware are called social engineering attacks. Increasing user awareness of the types of threats and how to successfully avoid them is critical to an organization's overall security.

This lesson covers the following topics:

- Phishing
- Other social engineering attacks

Phishing

One of the most successful social engineering attacks is called a phishing attack. In a phishing attack, the social engineer masquerades as a trustworthy entity in an electronic communication. The following table describes a few variations of phishing attacks.

Attack	Description
Spear phishing	In spear phishing, an attacker gathers information about the victim, such as their online bank. The attacker then sends a phishing email to the victim that appears to be from that bank. Usually, the email contains a link that sends the user to a site that looks legitimate, but is intended to capture the victim's personal information.
Whaling	Whaling is another form of phishing that targets senior executives and high-profile victims.
Vishing	Vishing is like phishing, but instead of an email, the attacker uses Voice over IP (VoIP) to gain sensitive information. The term is a combination of voice and phishing.
SMS phishing	In SMS phishing (smishing), the attacker sends a text message with a supposedly urgent topic to trick the victim into taking immediate action. The message usually contains a link that will either install malware on the victim's phone or extract personal information.

Other Social Engineering Attacks

The table below describes other common social engineering attacks.

Attack	Description
Pharming	Pharming involves the attacker executing malicious programs on the target's computer so that any URL traffic redirects to the attacker's malicious website. This attack is also called phishing without a lure. The attacker is then privy to the user's sensitive data, like IDs, passwords, and banking details. Pharming attacks frequently come in the form of malware such as Trojan horses, worms, and similar programs. Pharming is commonly implemented using DNS cache poisoning or host file modification. ▪ In DNS cache poisoning, the attacker launches the attack on the chosen DNS server. Then, in the DNS table, the attacker changes the IP address of a legitimate website to a fake website. When the user enters a legitimate URL, the DNS redirects the user to the fake website controlled by the attacker. ▪ In host file modification, the attacker sends malicious code as an email attachment. When the user opens the attachment, the malicious code executes and modifies the local host file on the user's computer. When the user enters a legitimate URL in the browser, the compromised host file redirects the user to the fraudulent website controlled by the attacker.
Social networking	Many attackers are turning to applications such as Facebook, Twitter, Instagram, to steal identities and information. Also, many attackers use social media to scam users. These scams are designed to entice the user to click a link that brings up a malicious site the attacker controls. Usually, the site requests personal information and sensitive data, such as an email address or credit card number.