2.3.8 Phishing and Internet-Based Techniques 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 to 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

Phishing is one of the most successful social engineering attacks. 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 the 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. It 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 either installs malware on the victim's phone or extracts personal information.

Other Social Engineering Attacks

The following tables 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 hosts file on the user's computer. When the user enters a legitimate URL in the browser, the compromised hosts file redirects the user to the fraudulent website controlled by the attacker.
Social media	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.
Typo squatting	Typo squatting, also called URL hijacking, relies on mistakes, such as typos made by users inputting a website address into a web browser. When a user enters an incorrect website address, the squatter may lead them to any URL. The typo squatter's URL may be one of several types, but all are similar to the victim site address: ▪ Common misspelling of the intended site, such as symantic.com instead of symantec.com. ▪ Misspelling based on a typographical error, such oreintaltrading.com instead of orientaltrading.com. ▪ A plural of a singular domain name, such as viking.com instead of vikings.com. ▪ A different top-level domain, such as tampicoil.org instead of tampicoil.com. ▪ An abuse of the Country Code Top-Level Domain, such as cocoskeelingislands.com instead of cocoskeelingislands.com.au.
Hybrid warfare	As it refers to technology, hybrid warfare employs political warfare and blends conventional warfare with cyberwarfare. Its goal is to influence others with things such as fake news, diplomacy, lawfare, and foreign electoral intervention. Examples include: ▪ Meddling in elections ▪ Misinformation ▪ Meddling in the security of foreign countries In 2015, the US Department of Defense Cyber Strategy, developed five pillars to combat hybrid and cyber warfare: 1. Build and maintain ready forces and capabilities to conduct cyberspace operations. 2. Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions. 3. Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyber attacks of significant consequence. 4. Build and maintain viable cyber options and plan to use those options to control conflict escalation and shape the conflict environment at all stages. 5. Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.
Watering hole attack	The term "watering hole attack" is derived from predators in the natural world who wait for an opportunity to attack their prey near watering holes. A watering hole is a passive computer attack technique in which an attacker anticipates or observes the websites an organization uses often and infects them with malware. Members of the targeted group can then become

	infected. Hackers could be looking for specific information to narrow their attacks from users that come from a specific IP address. A watering hole attack has five main steps: 1. The attacker identifies the sites visited by a victim and then infects the sites with malicious code. 2. The attacker identifies the vulnerabilities with the sites and injects it with malicious code. This could be JavaScript or code into the ads and banners used on the website. 3. The malicious code redirects the victims to a phishing site where there is malware. 4. When the victims visit these websites, the script containing malware is automatically downloaded to the victim's machines without their knowledge. 5. The malware then collects personal information from the victims and sends it back to the server operated by the attacker. There are several countermeasures against a watering hole attack: ▪ Update all your software to the latest versions and keep your operating system up to date. ▪ Configure firewalls, intrusions detection and prevention, and other network security products. ▪ Maintain your company's own website so it is free from malware. ▪ Use a VPN and the private browsing feature web browser's . ▪ Be aware of the popular websites that employees visit and ensure that those sites are free from malware. ▪ Train users on the dangers of potential watering hole attacks.
Credential harvesting	Credential harvesting, also known as password harvesting, is the process of gathering the usernames, passwords, email addresses, and other information through breaches and other activities. Hackers can then sell personal and financial data on the dark web, use the information to gain access to a company network for illegal purposes. Hackers might use cloned websites, such as Google, Amazon, eBay, and so on. When a user attempts to log in, they inadvertently send their credentials to the hackers. Hackers will also use phishing emails. Users must stay vigilant when receiving emails and be sure not to click on any unknown or unusual links. This could cause infected programs to download and install that you did not intend. To prevent credential harvesting, users must update their security software and be aware of the links they click on and sites they visit.