LESSON NOTES

CYBERSECURITY

Domain 5.0 - Security Program Management and Oversight

5.6.1 - Phishing Awareness

Lesson Overview:

Students will:

- Investigate how to determine phishing attacks.

Guiding Question: How can users recognize phishing attempts?

Suggested Grade Levels: 10 - 12

CompTIA Security+ SYO-701 Objective:

5.6 - Given a scenario, implement security awareness practices

- Phishing
  - Campaigns
  - Recognizing a phishing attempt
  - Responding to reported suspicious messages

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Phishing Awareness

Phishing

Phishing is a cybercrime tactic used by malicious actors to deceive individuals into providing sensitive information such as usernames, passwords, credit card details, or other personal information. ***Phishing campaigns*** typically involve mass emails, text messages, or phone calls that appear to be from legitimate sources but are designed to trick recipients into divulging confidential information or downloading malicious software.

Recognizing a Phishing Attempt

Phishing emails often use deceptive email addresses that may closely resemble legitimate ones. Look for misspellings or unusual domain names. Phishing emails often create a sense of urgency or use threats to prompt immediate action. Be cautious of messages demanding urgent responses or threatening consequences. Hover over links to reveal the actual URL. Avoid clicking on links in suspicious emails, especially those directing you to provide sensitive information. Be cautious of unexpected attachments, as they may contain malware. Many phishing emails contain grammatical errors or awkward language. Legitimate organizations usually have professional communication standards. Be wary of emails requesting sensitive information such as passwords, social security numbers, or financial details. Legitimate organizations typically do not request this information via email.

Responding to Reported Suspicious Messages

If you receive a suspicious email, do not click on any links or download any attachments. Instead, forward the email to your organization's IT or security team for analysis. If you believe you've been targeted by a phishing attempt, report it to the appropriate authorities. This could include your company's IT department, your email provider, or relevant law enforcement agencies. Share information about phishing tactics with colleagues, friends, and family to raise awareness and prevent others from falling victim to similar scams. Ensure your antivirus and anti-malware software is up to date to detect and prevent potential threats from phishing emails and malicious attachments. If you've inadvertently provided sensitive information in response to a phishing email, immediately change your passwords for affected accounts and enable two-factor authentication where possible.

Phishing campaigns continue to be a prevalent threat in the digital landscape. Recognizing the signs of a phishing attempt and knowing how to respond effectively are crucial steps in protecting yourself and your organization from cyber threats. Stay vigilant, educate yourself and others, and always verify the legitimacy of any requests for sensitive information.