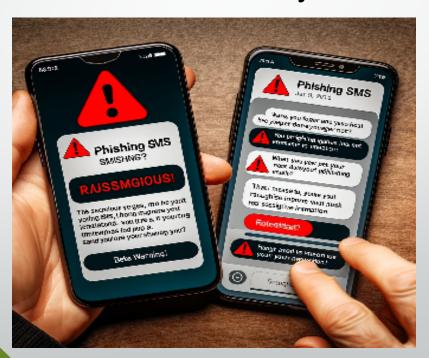
AWARENESS TRAINING

Protect Yourself from Cyber Threats



Introduction to Phishing

- What is Phishing?
 - **Definition:** Phishing is a cyberattack in which attackers attempt to deceive individuals into sharing sensitive information, often via email, websites, or text messages.
 - Goal: Steal personal information like usernames, passwords, or credit card details.
 - Types of Phishing: Email phishing, website phishing, spear-phishing, and social engineering tactics.

Types of Phishing Attacks:

- •Email Phishing: Sending fraudulent emails that appear legitimate.
- •Website Phishing: Creating fake websites that mimic real ones to capture sensitive data.
- •Spear Phishing: Targeting specific individuals with tailored content to increase success rates.
- •Smishing and Vishing: Phishing through SMS (Smishing) or voice calls (Vishing).

How Phishing Works:

• The Process:

- Attacker sends a deceptive message.
- Victim clicks a malicious link or downloads an attachment.
- The victim enters personal information on a fraudulent website.
- The attacker gains access to sensitive data.

Common Phishing Tactics:

- Urgency or fear (e.g., "Your account will be locked if you don't act now!")
- Posing as trusted entities (e.g., bank, social media platform, government agency).

Recognizing Phishing Emails:

- Key Indicators:
 - Suspicious Sender: Unknown email addresses, slight variations in domain names.
 - Unfamiliar Links: Hover over links to check the URL before clicking.
 - Grammatical Errors: Legitimate organizations tend to have professional communication.
 - Urgent Language: Claims that your account is compromised or requires immediate action.
 - Unexpected Attachments: Especially ZIP files or EXE files.

Phishing Websites:

- How to Spot a Fake Website:
 - Check the URL: Look for slight variations in the spelling or domain.
 - SSL Certificate: Legitimate sites use HTTPS.
 Be cautious of sites without the padlock symbol.
 - Visual Clues: Low-quality logos or images, spelling errors, odd formatting.
 - Real Website:
 URL: https:
 //www.bankofexample.e.com

Fake Website: URL: http: //www.bankofexam mple.com



Social Engineering Tactics:

- What is Social Engineering?
 - Definition: Manipulating people into divulging confidential information.
 - Tactics:
 - Pretexting: Pretending to be someone trustworthy (e.g., tech support).
 - Baiting: Offering something enticing to make a victim act (e.g., free downloads).
 - Tailgating: Physically following someone into a restricted area.
 - Real-World Example: In 2016, a phishing attack on the Democratic National Committee (DNC) used social engineering to trick staff into revealing their credentials, leading to a major email leak during the U.S. Presidential election.

Best Practices to Avoid Phishing Attacks:

•Email Hygiene:

- ✓ Do not click on suspicious links or open unexpected attachments.
- ✓ Verify the sender's email address.
- ✓ Avoid sharing personal information via email.
- •Website Safety:
- ✓ Double-check URLs, especially for login pages.
- ✓ Never enter personal information on sites that don't have HTTPS.
- Additional Precautions:
- ✓ Use Two-Factor Authentication (2FA).
- ✓ Keep your software and antivirus updated.
- ✓ Report phishing attempts to your IT or security department.

Case Study: Famous Phishing Attack:

- Example: The 2016 DNC Email Phishing Incident
 - What Happened: Hackers sent fraudulent emails to members of the Democratic National Committee.
 - Outcome: Sensitive data was stolen, leading to political repercussions.
 - Lessons Learned: Highlight the importance of vigilance and verification.

Conclusion and Call to Action:

- •Summary: Phishing attacks are common but avoidable. Stay vigilant, educate others, and protect your sensitive information.
- •Call to Action: Share this training with colleagues and report any suspicious messages or websites to your security team.

