Phishing Awareness Training

Learn how to identify, avoid, and respond to phishing attacks

Understanding Email Phishing

- Email phishing is a deceptive cyber attack where criminals pretend to be reputable sources to steal information.
- Attackers craft convincing emails that appear to come from trusted organizations like banks, online services, or colleagues.
- Common tactics include creating urgency, impersonating known contacts, and requesting sensitive data like passwords or payment details.
- Stay cautious and think before clicking links or sharing information.

Characteristics of Email Phishing

- Deceptive Sender Addresses: Attackers mimic legitimate email addresses with slight variations.
- Urgent Language: Scare tactics urging you to act immediately, such as threats of account suspension.
- Suspicious Links: Hidden URLs that redirect to fake websites. Always hover to preview the true destination.
- Lack of Contact Info: Many phishing emails provide generic or missing contact details.
- Too Good to Be True: Offers of unexpected prizes or windfalls are typical bait.
- Spoofed Websites: Fake sites mimicking real ones, often with small differences in the URL.

Understanding Spear Phishing

- Spear phishing is a highly targeted phishing attack focused on a specific person or organization.
- Unlike mass phishing, spear phishing emails are personalized using details about the target's role or contacts.
- These messages often appear to come from a known colleague or business partner, making them harder to detect.

Real-World Phishing Examples

- Netflix Scam (2020): Fake emails claiming account issues redirected users to a fraudulent login page to steal credentials.
- Microsoft Office 365 Attack (2019): Emails threatened account suspension, tricking users into revealing login details on a counterfeit Microsoft site.

Other Phishing Variants

- Spear Phishing: Personalized attacks aimed at individuals or specific groups.
- Whaling: Targets high-level executives and senior management.
- Vishing: Voice phishing conducted over phone calls to extract sensitive data.
- Smishing: SMS phishing using text messages to lure victims into clicking malicious links.

Recognizing Suspicious Sender Addresses

- Always verify the domain name in the sender’s address. Attackers often use domains that look similar but have minor changes.
- Look for subtle misspellings or added characters that may go unnoticed at first glance.

How to Check Links Safely

- Hover over hyperlinks without clicking to see the actual URL.
- Ensure that the displayed link text matches the real destination.
- Be wary of unfamiliar domains or links with excessive or random characters that don’t make sense.

Reporting Phishing Attempts

- Never reply to suspicious emails or click on any links or attachments.
- Document details: sender’s email, subject line, and any suspicious links.
- Use your company’s designated reporting tool or contact your IT/security team immediately.
- If you interacted with the email, change passwords and monitor accounts for unusual activity.

Steps to Take If You Suspect Phishing

- Do not interact with suspicious emails — avoid clicking links or downloading attachments.
- Verify the sender using a trusted communication method.
- Report the email to your IT or security team with all relevant details.
- Delete the phishing email after reporting to prevent accidental clicks.
- Monitor your accounts and watch for unauthorized transactions.

Why Reporting Matters

- Early reporting helps IT teams detect and stop threats quickly, reducing risk of data breaches.
- Consistent reporting allows security teams to analyze trends and strengthen defenses.
- Promotes a culture of security awareness throughout the organization.
- Protects sensitive information and supports compliance with industry regulations.
- Feedback from reported incidents improves training and security measures for everyone.

Conclusion

- Always stay alert and think critically when handling emails.
- Verify sender addresses and inspect links before clicking.
- Report any suspicious emails immediately.
- Keep up with security training and best practices.
- Together, we can create a safer digital workspace.