Phishing Awareness Training

KURALOVIYAN P

Introduction to Phishing

Phishing is a cyberattack where attackers impersonate trusted entities to trick individuals into revealing sensitive information such as passwords, credit card details, or personal data. These attacks commonly occur through emails, fake websites, SMS (smishing), phone calls (vishing), or social media messages.

How to Recognize Phishing Emails

Key Indicators of Phishing Emails:

- Suspicious sender address: The email may look similar to a legitimate address but with minor changes.
- Urgent or threatening language: Phrases like “Your account will be locked” or “Immediate action required.”
- Unexpected attachments or links: These may contain malware or lead to malicious websites.
- Spelling/grammar mistakes: Legitimate companies rarely send poorly written emails.
- Requests for personal or financial information: Real organizations do not ask for sensitive data via email.

Identifying Fake or Malicious Websites

Signs a Website May Be Fake:

- URL mismatches: Slight spelling changes (e.g., g00gle.com instead of google.com)
- No HTTPS or broken padlock symbol
- Poor design or low-quality logos
- Pop-ups asking for credentials
- Unusual requests for personal information

Always verify:

- URL spelling
- SSL certificate (HTTPS)
- Contact information and legitimacy

Social Engineering Tactics Used by Attackers

Attackers manipulate human behavior using psychological techniques. Common tactics include:

- Pretexting: Creating a believable story to gain trust.
- Impersonation: Acting as a boss, IT staff, bank, or government agency.
- Baiting: Offering something attractive (free rewards, coupons).
- Urgency & fear: Forcing quick decisions under pressure.
- Authority pressure: “This is your manager… update this immediately.”

Best Practices to Avoid Phishing Attacks:

- Verify before clicking: Hover over links to check the destination.
- Do not open unknown attachments.
- Never share sensitive information via email or chat.
- Enable multi-factor authentication (MFA).
- Use strong, unique passwords and a password manager.
- Keep systems and antivirus software updated.
- Report suspicious emails to the IT/SOC team immediately.

Real-World Examples of Phishing:

Example 1: Fake Bank Notification:

An email claims your account is locked and asks you to log in through a link—this link leads to a fake login page designed to steal credentials.

Example 2: HR Payroll Update Scam:

Attackers impersonate HR departments asking employees to update payroll information, redirecting them to malicious forms.

Example 3: Delivery Service Scam:

A message claims a package couldn't be delivered and includes a link to "reschedule," which installs malware.

Conclusion:

Phishing remains one of the most common and effective cyberattack methods because it exploits human trust rather than technical vulnerabilities. By understanding how phishing works, recognizing the signs of fraudulent emails and websites, and practicing safe online behavior, individuals and organizations can significantly reduce the risk of falling victim. Continuous awareness, regular training, and proactive reporting are essential to building a strong security culture.

THANK YOU