Phishing Awareness Training

Protect Yourself. Protect Your Organization.

What is Phishing?

Phishing is a cyberattack technique where attackers pretend to be trustworthy entities (like banks, companies, or colleagues) in order to trick people into giving away sensitive information such as passwords, credit card numbers, or personal details.

Key Points:

- Usually comes through emails, text messages, fake websites, or phone calls.
- Attackers disguise themselves as banks, government agencies, companies, or colleagues.
- The main goal is to steal data or money.

How to Recognize Phishing Emails And Fake Websites

Phishing Emails

- **Urgent or Threatening Language:** "Your account will be suspended!" or "Immediate action required!"
- **Suspicious Sender Address:** The "From" address doesn't match the company's real domain (e.g., paypal@securesrvc.com instead of service@paypal.com).
- **Generic Salutations:** "Dear Customer" instead of your name.
- **Grammar and Spelling Errors:** Professional companies rarely make these mistakes.
- **Links that Don't Match:** The visible link text says one thing, but the actual URL (when you hover over it) goes somewhere else.
- **Unusual Attachments:** Unexpected files like .zip or .exe.

Fake Websites

- **Check the URL:** Look for misspellings (e.g., amaz0n.com instead of amazon.com).
- **Look for HTTPS:** A legitimate website will have a padlock icon and "https://" at the beginning of the URL.
- **Trust the Certificate:** Click the padlock to view the security certificate. Does it match the company's name?
- **Poor Design & Functionality:** Blurry logos, broken links, and bad grammar are often signs of a rushed fake site.

Social Engineering Tactics

1 **Urgency & Fear:** "Your account is locked!" or "You will be fined!"

2 **Greed & Opportunity:** "Claim your prize!" or "You've won a lottery!"

3 **Authority:** Impersonating a boss, a law enforcement officer, or a bank manager.

4 **Trust & Likability:** A fake email from a known colleague asking for a quick favor.

Real-World Example: Phishing for Passwords

- **Scenario:** You receive an email from a popular service like Google or Microsoft.
- **Subject:** "Security Alert: Your password has been changed."
- **Email Body:** "Someone in a different location just signed into your account. Click here to secure your account."
- **The Catch:** The link leads to a fake login page that looks identical to the real one. When you enter your credentials, they are stolen.

Best Practices: How to Protect Yourself

- **STOP. THINK. CLICK?:** Before clicking any link, pause and examine the email carefully.
- **Hover Over Links:** Don't click. Just hover your mouse cursor over the link to see the real URL.
- **Don't Use Email Links:** If you're unsure, go directly to the company's website by typing the address yourself.
- **Report Suspicious Emails:** Use your company's designated method to report phishing attempts.
- **Use Strong, Unique Passwords:** And enable two-factor authentication (2FA) whenever possible.
- **Keep Software Updated:** This includes your operating system, web browser, and antivirus software.

Interactive Quiz: Is This a Phish?

Q1. You receive an email from your bank asking to confirm your login details via a link. What should you do?

- ❑ A. Click the link and log in
- ❑ B. Delete the email
- ❑ C. Report it to IT/security team ✅

Q2. A site URL looks like www.netf1ix-support.com. Safe or phishing?

- ❑ Safe ❌
- ❑ Phishing ✅

Final Thoughts & Key Takeaways

- ❏ Phishing is a constant threat, but you are the first line of defense.
- ❏ **Trust your gut:** If an email feels "off," it probably is.
- ❏ **Think before you click.**
- ❏ **Report everything suspicious.**
- ❏ Your vigilance protects not just you, but the entire organization.


Thank You
“Stay alert, stay safe!”