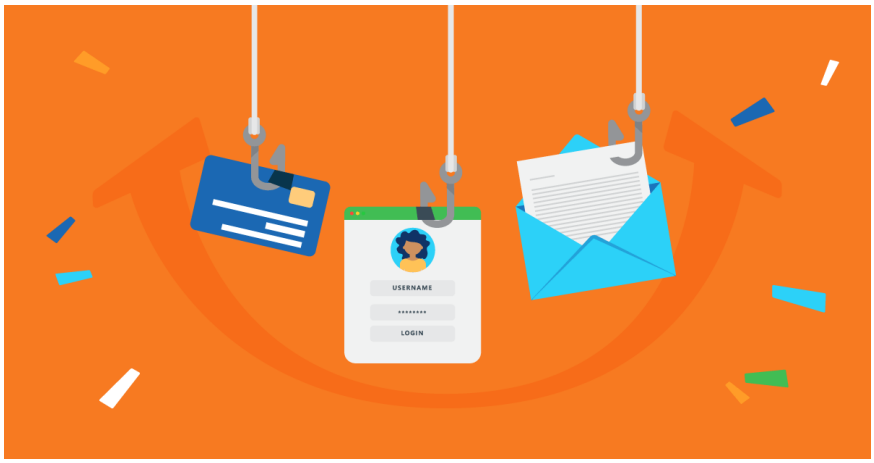
Phishing Awareness Training



[Graphic source: TalentLMS]

Table of Contents:

1. What is Phishing and Why is it Important?

[Graphic source: MSCVU]

What is Phishing?

Phishing is a fraudulent attempt to obtain sensitive information by pretending to be a trustworthy source. These scams often target personal details such as passwords, financial information, or other confidential data. Phishing can occur through various channels, including emails, phone calls, and text messages.

Why is Phishing Important?

Understanding phishing is crucial for protecting yourself and your organization from potential cyber threats. Recognizing these scams helps you avoid falling victim to them, thus safeguarding your personal and company information. Awareness of phishing techniques and their impact is essential for maintaining digital security and preventing data breaches.

[Graphic source: EC-Council]

2. Common Phishing Tactics

2.1: Email Phishing

Description: Email phishing involves fraudulent emails that appear to come from legitimate sources, such as well-known companies, banks, or colleagues. These emails typically ask for sensitive information, such as login credentials or financial details, or prompt you to click on malicious links or download attachments.

Red Flags:

- **Poor Grammar and Spelling:** Many phishing emails contain grammatical errors or awkward phrasing.
- **Urgent or Threatening Language**: Messages that create a sense of urgency or fear, such as threats of account suspension or immediate action required.
- **Unfamiliar Sender Addresses:** Emails from unexpected or unfamiliar addresses, especially those that mimic official domains.

[Graphic source: UTSA]

2.2: Spear Phishing

Description: Spear phishing is a targeted form of phishing where attackers focus on specific individuals or organizations. The messages are often personalized to seem more legitimate, leveraging information about the target's role, interests, or recent activities.

Red Flags:

- **Personalization:** Emails that use your name, job title, or details specific to your role or organization.
- **Contextual Relevance:** Messages that reference recent company events or personal interests to gain trust.

[Graphic source: Nucleo Consulting]

2.3: **Vishing** (Voice Phishing)

Description: Vishing involves phone calls where attackers pose as legitimate entities to extract sensitive information. This could be a call from someone pretending to be from your bank, IT department, or another trusted organization.

Red Flags:

- **Unsolicited Calls:** Receiving unexpected calls asking for confidential information.
- **Pressure Tactics:** High-pressure tactics or requests for immediate action or sensitive information.

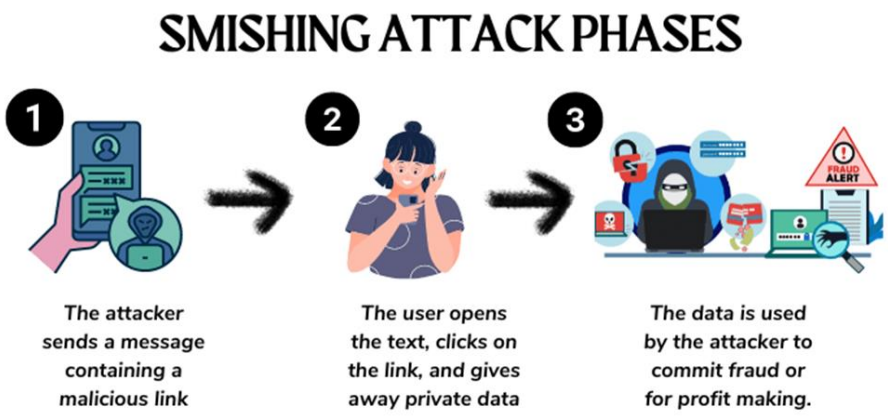
[Graphic source: Textmagic]

2.4: **Smishing (**SMS Phishing**)**

Description: Smishing involves phishing attempts through text messages. These messages often contain links that lead to fake websites or prompt you to reveal personal information.

Red Flags:

- **Unexpected Texts:** Receiving texts from unknown numbers or unexpected sources.
- **Suspicious Links:** Messages that include URLs leading to unfamiliar or suspicious websites.



[Graphic source: Terranova Security]

3. How to Recognize Phishing Attempts

Check the Sender

- ✓ **Tip:** Verify email addresses and phone numbers carefully. Official communication should come from trusted sources.
- ✓ **Tip:** Watch out for slight misspellings or variations in the sender's domain.
  (e.g., "@company.com" vs. "@compamy.com")
- ✓ **Tip:** Be cautious of emails that claim to be from a known contact but seem out of character or unexpected.

Look for Suspicious Links

- ✓ **Tip:** Hover over links to see their destination before clicking. Be wary of URLs that look strange or misspelled.
- ✓ **Tip:** Avoid clicking on shortened URLs unless you trust the source completely.

Be Cautious with Attachments

- ✓ **Tip:** Avoid opening attachments from unknown or unexpected sources.
- ✓ **Tip:** Double-check with the sender if you receive an unexpected attachment, even from a familiar contact.

Watch for Unusual Requests

- ✓ **Tip:** Be skeptical of unsolicited requests for sensitive information or urgent actions.
- ✓ **Tip:** Verify any unusual requests through a separate, trusted communication channel before taking action.

[Graphic source: dia.govt.nz]

4. What to Do if You Suspect Phishing

If you suspect that you've encountered a phishing attempt, taking immediate action is essential to protect your personal information and your organization's security. Here's what you should do:

Report It

- **Action:** Contact your IT department or security team immediately.

Do Not Click or Respond

- **Action:** Avoid interacting with suspicious emails, messages, or links.

Delete the Message

- **Action:** Remove the suspicious communication from your inbox.

Isolate Your Device

- **Action:** Disconnect your device from the network if you've clicked on a suspicious link or opened an attachment.

Change Your Passwords

- **Action:** Change your passwords immediately if you suspect they've been compromised.

[Graphic source: techradar]

5. Best Practices for Protection

Protecting yourself from phishing requires consistent attention to best practices. Implement the following to enhance your security:

Use Strong, Unique Passwords

- ✓ **Tip:** Create passwords using a mix of characters and avoid reusing them across accounts. Consider using a password manager.

Enable Multi-Factor Authentication (MFA)

- ✓ **Tip:** Secure your accounts with MFA, which adds a second layer of protection beyond your password.

Keep Software Updated

- ✓ **Tip:** Update your system and apps regularly, and enable automatic updates for ongoing protection.

Educate Yourself Regularly

- ✓ **Tip:** Stay updated on phishing threats and engage in security training to keep your knowledge current.

[Graphic source: Fortinet]

6. Additional Resources

- **[Company's IT Security Policy]**
- **[Link to Phishing Reporting Form]**
- **[Contact Information for IT Support]**