Phishing Awareness Training: Protecting Ourselves and Our Data

Protecting Ourselves from Phishing Attacks

Protecting Ourselves from Phishing Attacks

Phishing attacks:

- **Deceptive attempts** to steal personal information, login credentials, or financial data.
- Use **emails, phone calls, text messages, or fake websites** that appear legitimate.
- Phishers try to **trick you into clicking malicious links** or downloading attachments containing malware.

What is Phishing?

- Phishing is a **deceptive attempt** to steal personal information, login credentials, or financial data.
- It uses **emails, phone calls, text messages, or fake websites** that appear legitimate.
- Phishers try to **trick you into clicking malicious links** or downloading attachments containing malware.

Common Phishing Tactics

- **Urgency and Scarcity:** Phishers create a sense of urgency or pressure to act quickly, leaving you less time to think critically.
- **Suspicious Sender Addresses:** Check the sender's email address carefully for typos or inconsistencies.
- **Generic Greetings:** Phishers often use generic greetings like "Dear Customer" instead of your specific name.
- **Grammatical Errors and Misspellings:** Look for unprofessional language, typos, and grammatical errors, which are common in phishing attempts.
- **Suspicious Attachments or Links:** Don't click on links or open attachments from unknown senders.

What to Do if You Suspect a Phishing Attempt

- Do not click on any links or open attachments.
- Do not reply to the email or provide any personal information.
- Report the phishing attempt to your IT department immediately.
- Forward the suspicious email to your IT department for further investigation.