Phishing Awareness Training

Introduction to Phishing

Phishing is a type of cyber attack where criminals impersonate a legitimate entity to trick individuals into revealing sensitive information such as passwords, credit card numbers, or personal identification details. It is one of the most common and dangerous cyber threats today.

Types of Phishing Attacks

1. **Email Phishing:** The most common form, where attackers send fraudulent emails designed to appear legitimate.
2. **Spear Phishing:** A targeted attack aimed at a specific individual or organization, often using personalized information.
3. **Whaling:** A form of spear phishing that targets high-level executives or important personnel within a company.
4. **Smishing and Vishing:** Phishing via SMS (text messages) and voice calls.
5. **Clone Phishing:** An attacker makes a copy of a legitimate email, replacing links or attachments with malicious versions.

Recognizing Phishing Attempts

- **Suspicious Email Addresses:** Check the sender's email address carefully for misspellings or unusual domains.
- **Urgent or Threatening Language:** Phishing emails often create a sense of urgency to provoke a hasty response.
- **Generic Greetings:** Emails starting with "Dear Customer" instead of your name can be a red flag.
- **Misspellings and Grammar Mistakes:** Legitimate companies usually ensure their communications are polished and professional.
- **Unexpected Attachments or Links:** Hover over links to see the actual URL before clicking.

Avoiding Phishing Attacks

- **Think Before You Click:** Avoid clicking on suspicious links in emails, texts, or social media messages.
- **Verify Requests:** Contact the company directly through official channels to verify any requests for sensitive information.
- **Enable Multi-Factor Authentication (MFA):** Adds an extra layer of security even if your password is compromised.
- **Keep Software Updated:** Regular updates help protect against the latest phishing tactics.
- **Educate and Train:** Regularly update employees or team members on recognizing and handling phishing threats.

What to Do If You Suspect a Phishing Attempt

- **Don’t Engage:** Do not reply or provide any information.
- **Report It:** Forward the phishing email to your company’s IT department or phishing@domain.com.
- **Delete the Message:** After reporting, delete the suspicious email to avoid accidental interaction.
- **Run a Security Scan:** Use your antivirus software to ensure your system was not compromised.

Conclusion

Phishing attacks are ever-evolving, and staying vigilant is key to protecting your personal and professional information. Through education and awareness, we can reduce the risk of falling victim to these cyber threats.