PHISHING AWARENESS TRAINING

INTRODUCTION

Phishing is a cyber attack where attackers attempt to trick individuals into revealing sensitive information such as passwords, financial details, or personal data. These attacks often occur through emails, fraudulent websites, or social engineering tactics. This training module will help you recognize and avoid phishing threats.

SECTION 1: UNDERSTANDING PHISHING

- **What is Phishing?**
  a. A form of cyber attack used to steal confidential information.
  b. Often involves emails, fake websites, or messages that appear legitimate.

- **Types of Phishing Attacks:**
  a. Email Phishing: Fake emails that look like they come from trusted sources.
  b. Spear Phishing: Targeted attacks on specific individuals or organizations.
  c. Whaling: Attacks aimed at high-profile executives.
  d. Smishing: Phishing through SMS messages.
  e. Vishing: Phishing using voice calls.

SECTION 2: RECOGNIZING PHISHING ATTEMPTS

- **Common Signs of Phishing Emails:**
  a. Urgent or threatening language (e.g., "Immediate action required!").
  b. Requests for sensitive information.
  c. Suspicious sender addresses or domain names.
  d. Poor grammar, spelling errors, and unusual formatting.
  e. Unexpected attachments or links.

- **Identifying Fake Websites:**
  a. Check for HTTPS and valid security certificates.
  b. Look for slight misspellings in URLs (e.g., "g00gle.com" instead of "google.com").
  c. Avoid clicking on links in unsolicited emails; instead, type the address manually.

SECTION 3: AVOIDING PHISHING ATTACKS.

- **Best Practices for Email Safety:**
  a. Verify the sender before clicking links or downloading attachments.
  b. Hover over links to check the actual destination URL.
  c. Use spam filters and security software.

- **Protecting Your Personal Information:**
  a. Never share sensitive details over email, phone, or text messages.
  b. Enable multi-factor authentication (MFA) for added security.
  c. Regularly update passwords and use strong, unique passwords for different accounts.

SECTION 4: RESPONDING TO PHISHING ATTACKS

- **If You Suspect a Phishing Attempt:**
  a. Do not click on any links or open attachments.
  b. Report the email to your IT department or security team.
  c. Mark the email as spam to prevent future attempts.

- **What to Do If You Fall Victim:**
  a. Change your compromised passwords immediately.
  b. Monitor accounts for unauthorized activity.
  c. Notify your bank or service provider if financial details were shared.

CONCLUSION

By staying vigilant and practicing cybersecurity awareness, you can protect yourself and your organization from phishing attacks. Always think before you click, verify before sharing information, and report suspicious activities to keep digital spaces secure.