Phishing Awareness Training - Handout

1. What is Phishing?

Phishing is a cyber attack where attackers impersonate legitimate entities to trick you into revealing sensitive information. This can be through emails, text messages, or fake websites.

2. Types of Phishing Attacks

- Email Phishing: Fake emails urging you to click malicious links or attachments.
- Spear Phishing: Personalized attacks aimed at individuals.
- Smishing: Phishing via SMS.
- Vishing: Voice calls from impersonated contacts.
- Clone Phishing: Re-sent legitimate emails with malicious content.
- Business Email Compromise: Impersonating executives or vendors.

3. Recognizing Phishing Emails

- Suspicious sender address
- Generic greetings (e.g., 'Dear Customer')
- Urgent or threatening language
- Spelling/grammar mistakes
- Hover links that don't match URLs
- Unexpected attachments

4. Fake Websites

- Check for HTTPS and padlock
- Avoid links with misspelled domains (e.g., faceb00k.com)
- Poor layout or outdated branding

5. Social Engineering Tactics

- Pretexting: Fake identity to gain trust
- Baiting: Offers or free downloads with malware
- Quizzes harvesting personal info (e.g., 'Your pet's name')

6. How to Stay Safe

- Never click suspicious links
- Use antivirus and keep software updated
- Use 2FA (Two-Factor Authentication)
- Report suspicious emails to IT

7. Reporting Phishing

- Don't reply or click

Phishing Awareness Training - Handout

- Report to your organization or email provider
- Forward suspicious emails to phishing@yourcompany.com