PHISHING AWARENESS

INTRODUCTION TO PHISHING

What is Phishing?
Definition: A cyber attack involving fraudulent communication designed to trick individuals into revealing sensitive information.
Types of Phishing: Email phishing, Spear phishing, Whaling, Smishing, Vishing.

Importance of Phishing Awareness
Statistics on phishing attacks.
Impact on individuals and organizations.

RECOGNIZING PHISHING EMAILS

Recognizing Phishing Emails

Common Features of Phishing Emails
Suspicious sender addresses (e.g., mismatched domain names).
Generic greetings and lack of personalization.
Urgent or alarming language prompting immediate action.
Requests for sensitive information (passwords, account details).
Poor grammar and spelling mistakes.

RECOGNIZING PHISHING WEBSITES

01

Indicators of Phishing Websites
Unusual URLs (misspelled domain names, additional characters).
Lack of HTTPS and security certificates.
Poor website design and user experience.
Fake login forms or pop-ups requesting sensitive information.

SOCIAL ENGINEERING TACTICS

What is Social Engineering?
Definition: Manipulation tactics to trick individuals into divulging confidential information.

- Common Techniques

Pretexting: Creating a fabricated scenario.
Baiting: Offering something enticing to get information.
Quid Pro Quo: Offering a service in exchange for information.
Tailgating/Piggybacking: Gaining physical access by following someone.

PREVENTIVE MEASURES AND BEST PRACTICES

01

Email Security

- Use strong, unique passwords for email accounts.
- Enable multi-factor authentication (MFA).
- Regularly update and patch email clients.

02

Web Security

- Always verify the website URL before entering sensitive information.
- Avoid clicking on suspicious links.
- Use a reputable security suite or anti-phishing toolbar.

03

Personal Practices

- Be cautious of unsolicited communications.
- Verify requests for information through official channels.
- Educate yourself and others about common phishing tactics.

RESPONDING TO A PHISHING ATTEMPT

What to Do if You've Been Phished

- Immediately change passwords and secure your accounts.
- Notify relevant institutions (e.g., banks, email providers).
- Monitor accounts for suspicious activity.

Steps to Take if You Suspect Phishing

- Do not click on any links or download attachments.
- Report the phishing attempt to your organization's IT or security team.
- Delete the email or block the sender.

THANK YOU