BY: THANDEKA SKHOSANA

Phishing Awareness

Introduction to Phishing:

- **Definition:**
  - Phishing is a type of cyber attack where attackers deceive individuals into providing sensitive information by pretending to be a trustworthy entity.
- **Importance:**
  - It can lead to identity theft, financial loss, and unauthorized access to personal and professional information.

How Phishing Works

Outlining The Processes of Phishing

01 **Bait:** Attacker creates a fake email or website.

02 **Hook:** Victim receives the email or visits the website.

03 **Line:** Victim is tricked into providing sensitive information.

04 **Sinker:** Attacker uses the information for malicious purposes.

Common Phishing Techniques

EMAIL PHISHING

Fake emails that appear to be from legitimate sources.

SPEAR PHISHING

Targeted phishing aimed at a specific individual or organization.

WHALING

Phishing attacks aimed at senior executives or high-profile targets.

SMISHING

Phishing through SMS or text messages.

VISHING

Phishing through voice calls.

Recognizing Phishing Emails

01 Generic greetings like "Dear User."

02 Suspicious email addresses..

03 Urgent or threatening language.

04 Spelling and grammatical errors.

05 Unexpected attachments or links.

Identifying Phishing Websites

01 Misspelled URLs or domains that look similar to legitimate ones.

02 Lack of HTTPS (secure connection).

03 Urgent or threatening language.

04 Spelling and grammatical errors.

05 Unexpected attachments or links.

Social Engineering Tactics:

Techniques Used

- Pretexting: Creating a fabricated scenario to steal information.
- Baiting: Offering something enticing to get victims to take action.
- Quid pro quo: Promising a benefit in exchange for information.
- Tailgating: Following someone into a restricted area.
- Examples: Provide real-life scenarios of social engineering attacks.

How To Protect Yourself

Tips to always look out for

EMAIL SECURITY:

- Do not click on links or download attachments from unknown sources.
- Verify the sender's email address.
- Hover over links to check their actual destination.
- Use email filtering and anti-phishing software.

WEB SECURITY:

- Always check for HTTPS in the URL.
- Type the website address directly instead of clicking on links.
- Use reputable security software.

GENERAL SECURITY:

- Keep software and systems updated.
- Use multi-factor authentication (MFA).
- Regularly update and use strong passwords.

Organizational Best Practices

Strategies:

- **Training and Awareness:** Regularly train employees on recognizing and responding to phishing attacks.
- **Simulated Phishing Campaigns:** Conduct phishing simulations to test employees' awareness.
- **Incident Response Plan:** Have a clear plan for reporting and responding to phishing attacks.
- **Policy Enforcement:** Implement and enforce policies related to email and internet usage.

- **Stay Vigilant:** Always be cautious and skeptical of unexpected emails and messages.
- **Verify Sources:** Double-check the authenticity of email addresses, links, and attachments.
- **Educate and Train:** Continuously educate yourself and others about the latest phishing techniques.
- **Use Security Tools**: Implement and maintain robust security measures, including MFA and up-to-date software.
- **Report Suspicious Activity**: Know how and where to report suspected phishing attempts within your organization.