2025

TRAINING

PHISHING AWARENESS

by HANANE TATERKINE

What is PHISHING?

Phishing is a cyber-attack technique where attackers impersonate a legitimate entity to trick individuals into revealing sensitive information, such as login credentials, credit card numbers, or personal data.

Types of Phishing Attacks

Email Phishing

Fraudulent emails appear to come from trusted sources.

Vishing (Voice Phishing)

Phone calls attempting to extract confidential data.

Smishing (SMS Phishing)

Fraudulent messages sent via text.

Spear Phishing

Targeted attacks directed at specific individuals or organizations.

Common Techniques
Phishing

Urgency and Fear Tactics

Spoofed Email
Addresses &
Domains

Malicious Attachments
& Links

Fake Websites

Steps to Take If You Receive a Phishing Attempt

01 Do not click on any links or download attachments.

02 Report the phishing email to your IT/security team.

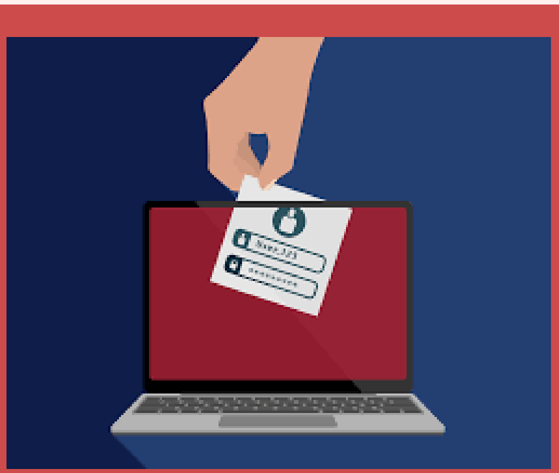
03 Mark the email as spam or phishing.

04 Delete the email from your inbox.

Why You Should Be Careful to Not Fall for Phishing ?

FINANCIAL LOSS

IDENTITY THEFT



DATA BREACHES

REPUTATION DAMAGE

Best Practices for Phishing Prevention

- Enable multi-factor authentication (MFA).
- Keep software and antivirus up to date.
- Regularly change and use strong passwords.

Stay Tuned..