PHISING Awareness Training

Let`s start by understanding what phishing is and why it`s important to start vigilant

Today, we'll discuss what phishing is and how to recognize and avoid phishing attempts.

What is phishing?

- Phishing is a fraudulent attempt to obtain sensitive information, such as usernames, passwords, and credit card details, by disguising as a trustworthy entity in electronic communication.

- Phishing attacks can occur via email, text messages, phone calls, or even social media.

- Attackers often use tactics like urgency, fear, or curiosity to manipulate individuals into clicking on malicious links or providing personal information.

Learn to spot phishing emails

- Spoofed Emails: Emails that appear to be from legitimate sources but are actually from attackers.
- Urgency: Messages that create a sense of urgency, such as "Your account will be suspended unless you act now!"
- Fake Links: Hyperlinks that lead to fake websites designed to steal your information.

How do we stop getting phished?

- Be cautious of unsolicited emails, especially those requesting sensitive information or urgent action.
- Verify the sender's email address and look for any spelling or grammatical errors.
- Avoid clicking on suspicious links or downloading attachments from unknown sources.
- Hover over links to preview the URL before clicking to ensure they lead to legitimate websites.
- Enable multi-factor authentication (MFA) whenever possible to add an extra layer of security to your accounts.