Phishing Awareness: Stay Safe Online

What is Phishing?

Phishing is a type of cyber attack where scammers trick individuals into revealing sensitive information such as passwords, credit card details, or personal data.

This is usually done through deceptive emails, messages, or fake websites.

Common Types of Phishing Attacks:

1. Email Phishing - Fraudulent emails posing as legitimate sources to steal information.
2. Spear Phishing - Targeted attacks on specific individuals or organizations.
3. Smishing (SMS Phishing) - Fake text messages designed to steal personal details.
4. Vishing (Voice Phishing) - Scam phone calls pretending to be from trusted entities.
5. Clone Phishing - Creating a fake copy of a legitimate email with malicious links.

How to Identify Phishing Attempts:

- Check the Sender: Be cautious of emails from unknown or suspicious addresses.
- Look for Spelling Errors: Phishing messages often contain poor grammar and typos.
- Hover Over Links: Before clicking, hover to see if the URL matches the official website.
- Beware of Urgency: Scammers create a sense of urgency to make you act without thinking.
- Check for HTTPS: Legitimate websites use "https://" and not just "http://".

How to Protect Yourself:

Enable Two-Factor Authentication (2FA) - Adds an extra layer of security.

Verify Directly - Contact organizations directly instead of clicking suspicious links.

Keep Software Updated - Security updates help prevent attacks.

Educate Yourself and Others - Awareness is key to preventing phishing attacks.

Use Security Tools - Install anti-phishing browser extensions and email filters.

What to Do If You Fall Victim?

1. Change Your Passwords Immediately.

2. Report the Phishing Attempt to your IT department or service provider.

3. Monitor Your Accounts for any suspicious activity.

4. Enable Fraud Alerts with your bank if financial information was exposed.

Stay alert, think before you click, and protect your digital presence!