Phishing

What is it?
How to identify it?
How to protect yourself from it?

Phishing is a malicious act of communicating during which the attacker impersonates legitimate companies to trick individuals to share personal information.

Types of phishing:

- Deceptive Phishing: This is the most common type where attackers use emails to impersonate legitimate companies to trick people into sharing personal information.
- Smishing: Attackers use SMS text messages to harvest personal information.
- Vishing: Also known as voice phishing, where attackers use phone calls to impersonate legitimate entities to trick people into revealing sensitive information. This can involve live calls or pre-recorded messages.
- Quishing: A new form of phishing that uses QR codes to redirect users to malicious sites when scanned.

Phishing signs to look out for?

- Urgent language
- Request for personal information
- Generic greetings
- Poor grammar
- Links that don't match the sender's domain
- Unsolicited attachments
- Too good to be true offers

How to protect yourself from phishing?

- Verify the sender's identity before sharing any sensitive information.
- Regularly review your bank and credit card statements for unauthorized transactions. Report any suspicious activity immediately.
- Stop and Think Before You Click the Link: Don't click on suspicious links, download unknown attachments, or trust unexpected requests for money or personal information. Be skeptical.
- When in doubt, delete communications or hang up calls to protect yourself from phishing attacks.