Phishing Quick Guide

What Is Phishing?

Phishing is when attackers pretend to be trusted people or companies to trick you into clicking malicious links, opening harmful attachments, or revealing sensitive information such as passwords or financial details.

How to Recognize a Phishing Message

- Unexpected or unusual requests.
- Urgency or fear (“Your account will close soon!”).
- Suspicious or mismatched links.
- Strange sender address or domain.
- Unexpected attachments.
- Requests for passwords or codes.
- Odd tone, spelling errors, or generic greetings.

How to Stay Safe

- Don’t click unexpected links.
- Don’t open unverified attachments.
- Verify messages on official websites or phone numbers.
- Never share passwords or MFA codes.
- Enable multi-factor authentication (MFA).
- Keep your device updated.
- Slow down — phishing works when you rush.

If You Think You’ve Been Phished

- Stop interacting with the message.
- Change your password immediately.
- If reused, change it everywhere.
- Enable MFA.
- Run an antivirus scan.
- If it's a work account, notify IT/security immediately.

Stay alert. Slow down. Verify before you click.