Phishing Awareness Training

Learn how to spot phishing emails, fake websites, and social engineering tricks.

What is Phishing?

Phishing is a social engineering attack where criminals trick you into revealing sensitive information (passwords, OTPs, credit card data) or installing malware.

Red Flags in Emails:

- Urgent language: "Your account will be closed in 2 hours!"
- Suspicious links: Hover to preview; watch for lookalike domains.
- Attachments you didn't expect, especially `.html`, `.exe`, or `.zip`.
- Requests for passwords or OTPs **legitimate services never ask this by email**.
- Sender mismatch: display name vs. actual email address

Check the Website:

- Verify the URL carefully; look for typos or extra characters.
- Confirm HTTPS is present — padlock alone isn't enough, but it's a start.
- Use bookmarks for important sites (bank, email) instead of clicking links.

Best Practices

- Enable MFA on all important accounts.
- Keep software and browsers up to date.
- Report suspicious emails to your IT/SecOps team.
- Never share OTPs or recovery codes.

Presenter:

Waris Khan