Phishing Awareness Training

Recognize, Avoid, and Report Phishing Attacks

Name : LARAIB KAWNAL

Learning Objectives

Understand	Understand what phishing is and why it’s dangerous
Recognize	Recognize common phishing traits
Learn	Learn immediate steps to take if you suspect phishing
Practice	Practice with a short quiz

What is Phishing?

Fraudulent attempt to obtain sensitive info by pretending to be a trusted source

Common channels: Email, SMS (smishing), phone (vishing), social media, fake websites

Common Types of Phishing

- Email phishing: fake bank or service emails
- Spear phishing: targeted attack
- Smishing & Vishing: SMS and voice phishing
- Clone phishing: modified copy of a legitimate email
- Website phishing: fake login pages

Example Phishing Email

FROM: SUPPORT@YOURBANK.EXAMPLE.COM

URGENT REQUEST TO VERIFY ACCOUNT

SUSPICIOUS LINK: HTTP://YOURBANK.VERIFY-EXAMPLE.COM/LOGIN

How to Spot a Phishing Email

Sender address mismatch

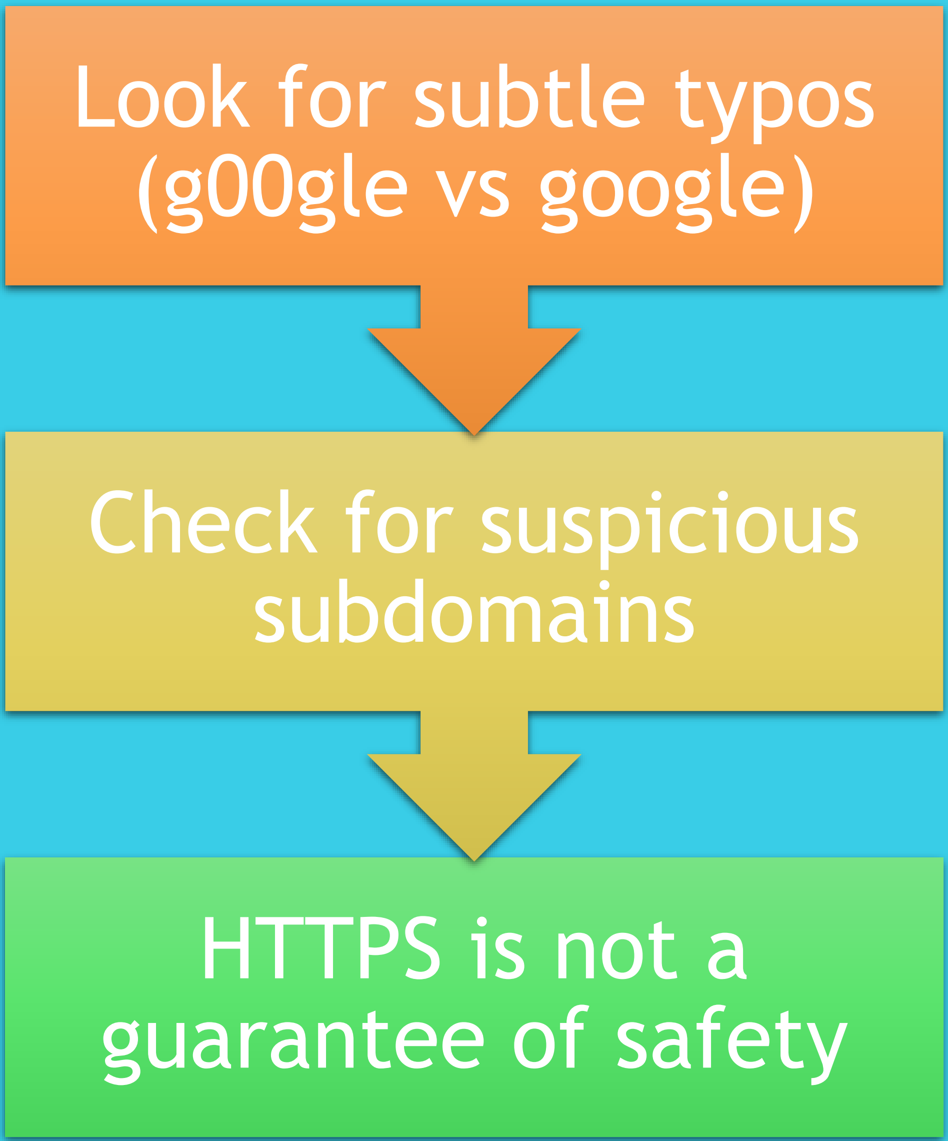
Generic greeting (Dear Customer)

Urgency or threatening language

Unexpected attachments or links

Poor grammar or formatting

URL & Domain Red Flags



Look for subtle typos (g00gle vs google)

Check for suspicious subdomains

HTTPS is not a guarantee of safety

Social Engineering Tactics

Authority: pretending to be a boss

Urgency: act now or lose access

Familiarity: mentions colleague names

Rewards: prize or gift offers

What To Do If You Suspect Phishing

1. Do NOT click links or download attachments

2. Report to security team

3. Change passwords if credentials were entered

Best Practices

Enable	Enable multi-factor authentication
Keep	Keep systems updated
Use	Use unique passwords
Verify	Verify sensitive requests through known channels

Resources

- OWASP Phishing Guidance
- Google Safety Center - phishing
- Microsoft Security - phishing & spoofing