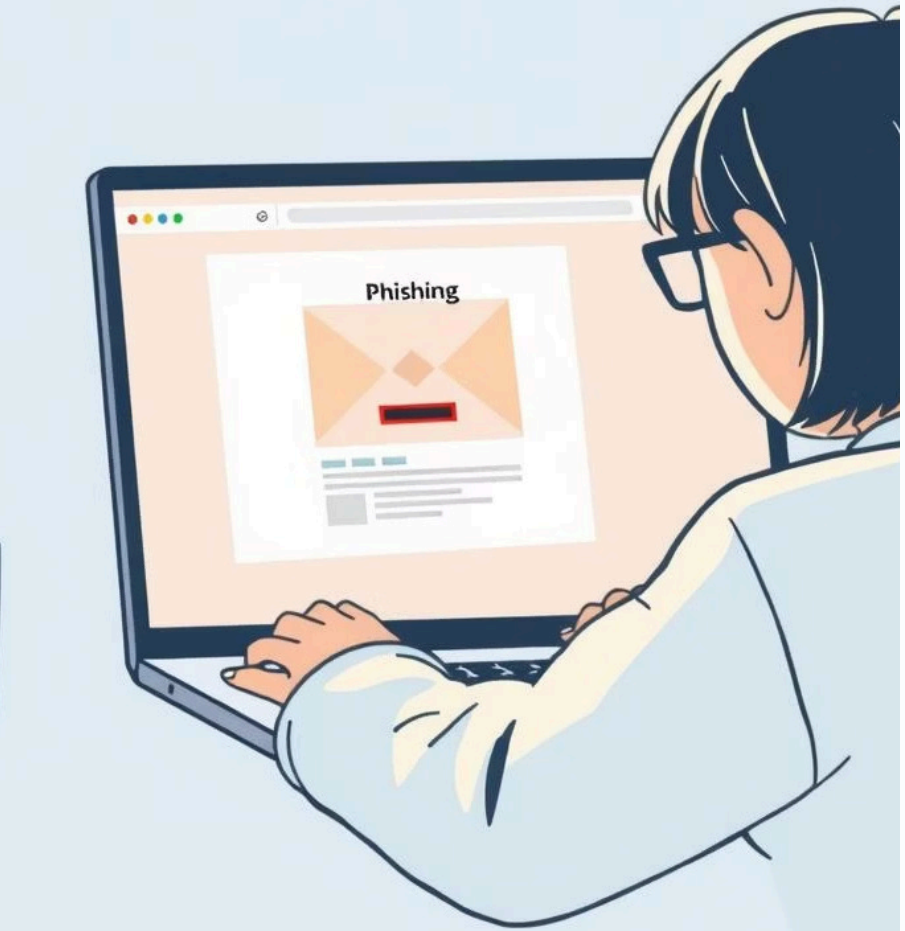

Phishing Awareness Training

How to spot phishing emails and fake websites

Presented by: Mahnoor Ikram

What Exactly is Phishing?

1

Phishing is a deceptive tactic where malicious individuals **impersonate trusted entities** to trick you into revealing sensitive information.

2

It's like a digital disguise, aiming to steal your data, such as usernames, passwords, and credit card details.

For example: A fake bank email asking you to click a suspicious link to "verify your account" is a classic phishing attempt.

Why is Phishing So Dangerous?

Financial Loss

Phishing can lead to unauthorized transactions and direct monetary theft from your bank accounts or credit cards.

Account Takeover

Attackers can gain full control over your online accounts, including email, social media, and other critical platforms.

Identity Theft

By gathering enough personal information, phishers can steal your identity, leading to severe long-term consequences.

Common Red Flags in Phishing Emails

1. Suspicious Sender Address: The "From" email address doesn't match the official company domain or looks slightly off.

2. Spelling & Grammar Errors: Official communications are typically proofread. Frequent typos or grammatical mistakes are a major giveaway.

3. Urgent or Threatening Language: Phrases like "Act now or your account will be suspended" or "Immediate action required" aim to create panic.

4. Requests for Sensitive Information: Legitimate organizations rarely ask for passwords, credit card numbers, or other personal data via email.

How to Safely Check a Link

Do Not Click Immediately

Resist the urge to click on any link in a suspicious email, no matter how convincing it looks.

Hover to Reveal URL

Move your mouse cursor over the link (without clicking) to see the actual destination URL appear, usually in the bottom-left corner of your screen.

Scrutinize the URL

Check the revealed URL for discrepancies. Look for subtle misspellings, extra characters, or unusual domains (e.g., bank-secure-login.com instead of yourbank.com).

Manual Navigation

If you suspect the link, type the legitimate website address directly into your browser's address bar instead of using the email link.

Social Engineering Tactics

Phishing often leverages social engineering, manipulating you into taking action by exploiting human psychology.

Fear & Urgency

Threatening account closure or legal action to rush you into making a mistake without thinking.

Greed & Excitement

Offering fake prizes, incredible job opportunities, or huge discounts to entice you to click.

Trust & Authority

Impersonating colleagues, supervisors, or well-known brands to gain your confidence.

Best Practices to Avoid Phishing

Never Share Passwords Via Email

Legitimate companies will never ask for your password through email or text messages.

Enable Two-Factor Authentication (2FA)

2FA adds an extra layer of security, requiring a second verification step even if your password is compromised.

Verify Sender Directly

If in doubt, contact the company directly using their official phone number or website, not details from the suspicious email.

Keep Software Updated

Regularly update your operating system, web browsers, and antivirus software to patch security vulnerabilities.

Interactive Phishing Quiz

1

Question 1

An email asks you to reset your password and contains several spelling errors. Should you click the link?

Answer: No. This is a clear sign of a phishing attempt.

2

Question 2

You receive an email from "YourBank" but the link domain shows "bank-secure-login.com". Is it safe to click?

Answer: No. The mismatching domain indicates a malicious link.

3

Question 3

Is it recommended to enable Two-Factor Authentication (2FA) on your online accounts?

Answer: Yes! 2FA significantly enhances your account security.

Real-World Example: A Phishing Email Deconstructed

Dissecting the Scam:

- Sender's address: Often a variation of the legitimate domain.
- Urgent tone: "Your account is limited!" or "Suspicious activity detected!"
- Generic greeting: Lacks your name, using "Dear Customer" instead.
- Embedded links: Designed to look legitimate but direct to fake websites.
- Call to action: Demands immediate login or update of personal details.

Always remember: When in doubt, delete the email and visit the official website directly.

Stay Safe Online

Trust Your Instincts

If something feels off, it probably is. Never hesitate to question an unsolicited email or message.

> If you're unsure about the legitimacy of an email or message, do not click any links or attachments. Instead, reach out to a trusted person or IT support for verification.

Presented by: Mahnoor Ikram