Don't Take the Bait: Defending Against Phishing Attacks

Simple, professional training — recognize, avoid, report

Learning Objectives

- Understand what phishing is and why it matters.
- Recognize phishing emails and fake websites.
- Learn common social engineering tactics used by attackers.
- Apply best practices to avoid falling victim.
- Test knowledge with simple quiz questions.

What is Phishing?

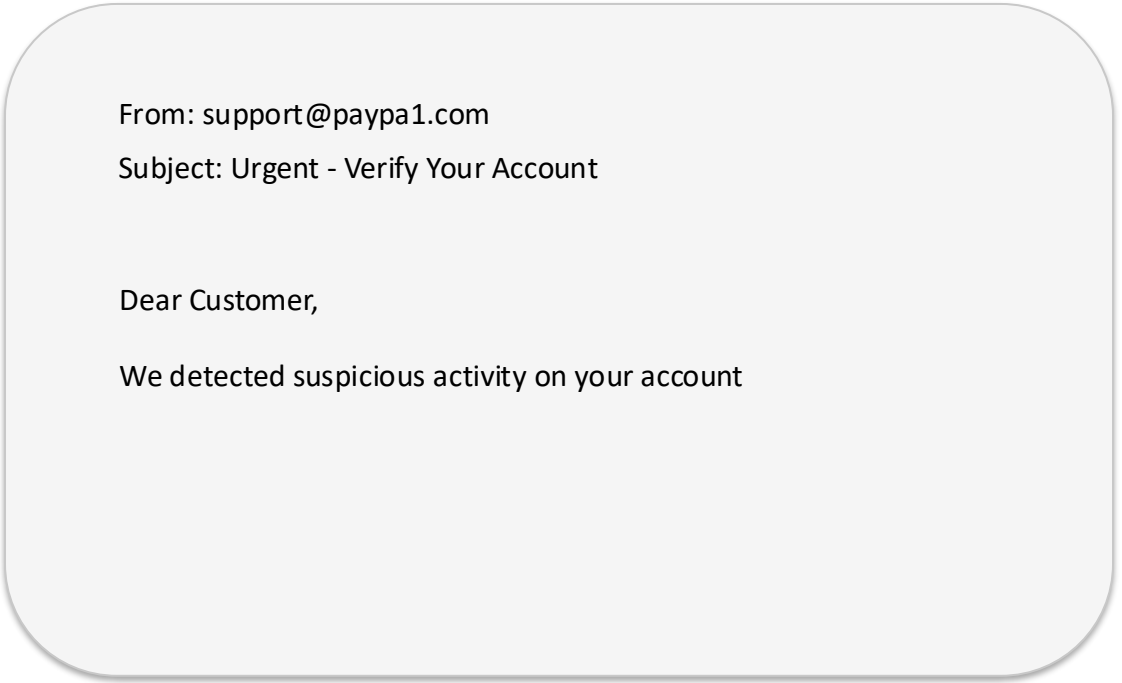
- A cyberattack that tricks people into revealing sensitive information.
- Common targets: passwords, bank details, personal data.
- Delivered via email, SMS (smishing), calls (vishing), or fake sites.

Types of Phishing

- Email phishing — broad, mass emails pretending to be trusted senders.
- Spear phishing — targeted attacks using personal details.
- Whaling — targets high-level executives.
- Smishing & Vishing — phishing via SMS or voice calls.

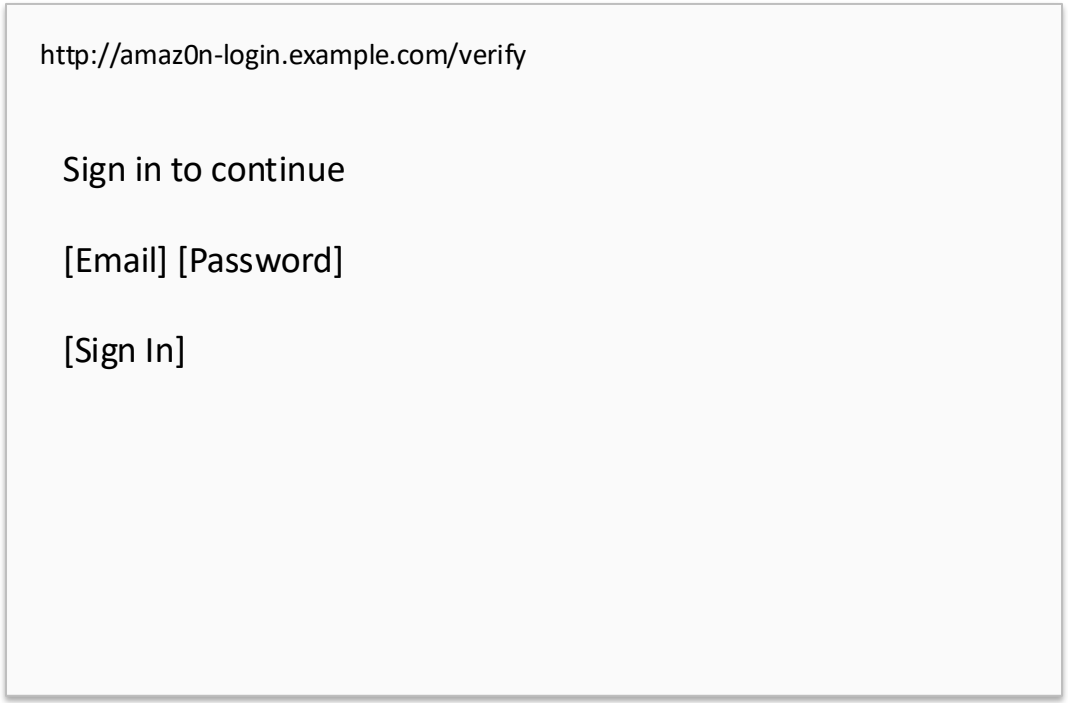
How to Recognize Phishing Emails

Suspicious sender address (e.g., support@paypa1.com).
Generic greetings like 'Dear Customer'.
Urgent language: 'Act now or we will close your account'.
Unexpected attachments or links; spelling/grammar errors.
Hover over links to see mismatched URLs.



Spotting Fake Websites

Misspelled or odd-looking domain names (e.g., amaz0n.com).
No HTTPS / missing padlock or invalid certificate.
Low-quality design or broken images.
Forms asking for sensitive info immediately.



Social Engineering Tactics

Authority: Impersonating banks, IT, or officials.
Urgency: Forcing quick, unconsidered action.
Fear: Messages that scare you into responding.
Curiosity: Promises of prizes or secret info.
Trust: Impersonation of colleagues or friends.

Best Practices — Do's & Don'ts

DOs:
- Verify sender identity before clicking links.
- Use multi-factor authentication (MFA).
- Keep devices and software updated.
- Use strong, unique passwords (password manager).
- Report suspicious messages to IT/security.

DON'Ts:
- Don't click links from unknown senders.
- Don't share passwords or MFA codes.
- Don't download unexpected attachments.
- Don't provide sensitive info over email/SMS.

Real-World Examples

Target (2013): phishing of a vendor led to data breach.
Google Docs Scam (2017): fake sharing link requested permissions.
COVID-19 themed scams: fake vaccine/donation pages.

Quiz #1: Spot the Phish

Which of the following is most likely a phishing email?

A) Email from your bank with a personal greeting & recent transaction listed.
B) Email from support@paypa1.com saying 'Your account will be locked! Click here now.'
C) Message from your colleague using the company domain.

Quiz #2: Safe Link Checking

What's the safest way to check a link in an email?

A) Click it quickly to see where it goes.
B) Hover to preview or copy the URL and type it into browser yourself.
C) Paste it into a search engine and choose the first result.

Recap: Key Takeaways

Phishing tricks users into revealing sensitive data.
Watch for suspicious senders, urgency, and fake URLs.
Use MFA, strong passwords, and keep systems updated.
Report phishing attempts and 'think before you click.'

Call to Action

Think before you click — report suspicious messages to your IT/Security team