





Phishing Attacks: How to Recognize & Avoid Them

Stay Safe from Online Scams

Created by: NIMRA NAVEED






What is Phishing?

-  A cyber attack where criminals trick you into giving sensitive info.
-  Usually done through emails, fake websites, or phone calls.
-  Goal: Steal passwords, bank info, or personal data.
-  Example: 'Your bank account is locked. Click here to fix it.'







Why Phishing Works

- 😞 Uses psychological tricks (fear, urgency, curiosity).
- 🏦 Pretends to be from trusted organizations (banks, delivery services, colleagues).
- ❓ Victims often act before thinking.






Common Types of Phishing

-  Email phishing – Fake emails with dangerous links/attachments.
-  Spear phishing – Targeted attack against a specific person or company.
-  Smishing – Fake SMS/text messages.
-  Vishing – Voice calls pretending to be support or banks.
-  Clone phishing – A real email is copied, but link is replaced with a fake one




Red Flags in Phishing Emails

-  Urgent or threatening language.
-  Suspicious links (hover to check before clicking).
-  Unexpected attachments (.zip, .exe, .docm).
-  Generic greetings instead of your name.
-  Spelling/grammar mistakes.
-  Sender email doesn't match organization.

Phishing Websites

-  URL looks strange (paypa1.com instead of paypal.com).
-   No https:// or security lock.
-  Poor design, broken images.
-  Pop-ups asking for sensitive info.







Social Engineering Tactics

-  Pretend to be IT support and ask for your password.
-  Pose as a boss/colleague asking for urgent money transfer.
-  Offer free prizes or lottery winnings.





Real-World Examples

- ✉ Fake emails vs real emails.
- 🔍 Spotting red flags in side-by-side examples.

How to Protect Yourself

-  Don't click links in suspicious emails.
-  Hover over links to check real URL.
-  Verify sender before replying.
-  Keep software and antivirus updated.
-  Use multi-factor authentication (MFA).
-  Report phishing attempts to IT/security team.



What To Do If You Suspect Phishing

-  Do not reply or click.
-  Report to your IT/security team.
-  If you clicked, change your password immediately.
-  Watch for unusual account activity.

Quick Quiz

- ? Q1: Which of these is a phishing email?
- ? Q2: What should you do if you clicked a phishing link?
- ? Q3: Name 2 red flags in phishing messages.

Summary

-  Phishing = tricking you into giving information.
-  Always check email, links, and attachments carefully.
- ⚡ Stay alert – think before you click!