

8 Key Tips for Identifying Phishing Emails



Phishing attacks attempt to persuade people to hand over information such as passwords or financial info. Today's attacks are more targeted, complex, and difficult to detect, making them more lucrative than ever.

Don't trust the display name

Just because an email says it's from someone you know or trust doesn't mean that it truly is. Even if the email address is legitimate, an email could be coming from an account that has been compromised by an attacker.

Beware of urgency

Phishing emails often convey that there is some sort of emergency in an effort to convince the recipient to act fast without thinking things through, such as an urgent request for a transfer of funds.

Evaluate the salutation

Is the greeting general or vague? Is the tone what you would expect from the person it is supposedly coming from?

Check spelling and grammar

Attackers are often careless when it comes to spelling and grammar. In some cases, they will purposely add in extra letters or characters in an effort to evade spam filters.

Investigate before you click

Read through the email carefully and thoroughly evaluate all parts before clicking on any of its contents. Do the the subject line and body text make sense?

Be wary of requests for personal information

Emails that ask for your personal information, regardless of how official it looks, should raise a red flag.

Watch out for more complex spear phishing

Hackers are using compromised colleague's accounts to impersonate employees and send high-quality, personalized messages to infiltrate an organization and steal your assets. Set a specific policy for financial transactions and confirm with the sender using a verified address.

Be cautious with links and attachments

Phishing emails often contain malicious links or attachments, which redirect users to fraudulent websites that steal their credentials or download malware on victims' devices.

Free Email Security Assessment
866-GD-LINUX

hello@guardiandigital.com

Guardian Digital is here to help you navigate safely today and plan for continued safety in an ever evolving digital future.

Call us, contact us, ask questions.