

How to Spot a Phishing Email

Phishing emails are the most common cyber threat, behind the majority of data breaches. They're designed to look like messages from trusted sources, tricking you into clicking, downloading, or sharing sensitive information.



How They Work:



Impersonating Trusted Senders

Attackers mimic banks, suppliers, or even colleagues to make emails look legitimate. They often use urgent subject lines like "Payment overdue" or curiosity hooks like "Invoice attached."

Tip: Check sender addresses carefully for small spelling errors or unusual domains.

Malicious Links

Phishing emails include links that appear safe but actually redirect to fake login pages or malware sites.

Tip: Hover over links before clicking to reveal the true web address.



Suspicious Formatting

Poor grammar, strange layouts, or fake logos are often giveaways that an email isn't genuine.

Tip: Be cautious if the design looks "off" compared to normal company emails.

Unexpected Attachments

Files attached to phishing emails can install malware or ransomware on your device.

Tip: Never open attachments you weren't expecting, even if they look official.



Verifying Requests

Phishing often relies on catching people off guard. If something feels unusual, it's definitely worth confirming.

Tip: Contact the sender directly using a trusted phone number or email—never reply to the suspicious message.