



How to Spot a Phishing Email

90% of cyber attacks start with a phishing email.

They trick you into giving away sensitive info by pretending to be someone you trust.
Here's how you and your team can avoid them...



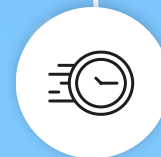
Check the sender - Does the email address look strange? Hover to check for fakes like **support@p4ypal.com**'.

Look for typos - Legit companies don't make obvious mistakes. Watch for poor grammar and awkward phrasing.



Suspicious links - Hover over links without clicking. Does the URL look odd or unrelated?

Urgent language - Phrases like **"Act now!"** or **"Your account will be suspended!"** are common red flags.



Unexpected attachments - Unsolicited files can carry malware. Don't open them.

Generic greetings - Emails that say **"Dear Customer"** instead of using your name may be fake.



Too good to be true - Promises of prizes or refunds? Likely a scam.



If in doubt don't click anything

Need help training your team how to spot scams?
We can help. Get in touch.