A USER GUIDE FROM TESSIAN

TESSIAN

How to Catch a Phish

6.4 billion fake emails are sent everyday.

Spear phishing emails are targeted attacks designed to trick you into doing something like sending money, sharing credentials or clicking a malicious link.

Spear phishing attacks are on the rise, very convincing, and hard to spot.

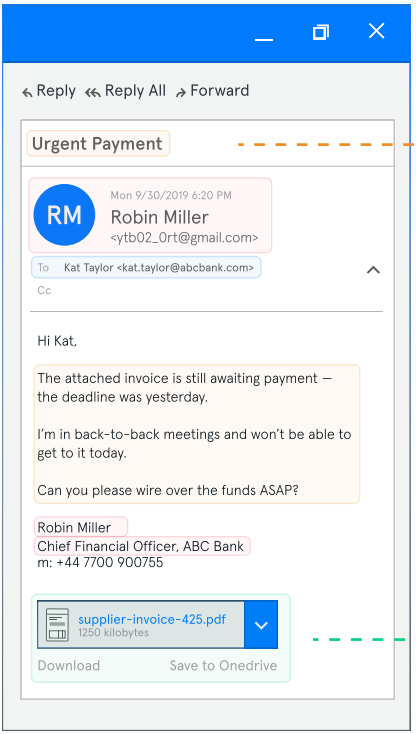
Use this guide to check any emails that look suspicious.

Target (aka you)

Do you have access to money, sensitive systems or powerful people? Or, are you a new employee? If so, you're a prime target. Be careful!

Intent

Are you being asked to do something urgently? If this isn't normal, it may be a fake request.



Sender Identity

Attackers will impersonate people or companies you know, or people in positions of power. Look at the from: and reply: email addresses. Do they look correct? Fraudsters can change domains and display names to make emails look authentic.

Payload

Many - but not all! - attacks contain links and attachments that look harmless, but are actually malicious. If you suspect this email is not safe, do not click on any links or open any attachments; they could lead to pages that steal credentials or deploy malware.

If you think you've received a spear phishing email, do not reply to it and alert your IT team ASAP.

TESSIAN