SCAM ALERT

WARNING ⚠ WARNING ⚠ WARNING ⚠ WARNING

Fake emails and messages (aka scams or phishing) can look just like the real thing. They may appear to be real messages from companies you know, like Amazon, the Post Office, HMRC, and PayPal, but they are designed to steal your email and passwords, or to lure you into parting with money.

Check the sender address (URL)

- Is it spelt correctly? Have any characters been replaced with similar letters or numbers? [www.info@paypol.com]
- Are there extra characters or words that shouldn't be there? [www.info@paypal8732/login.com]

Check the links

- Hover over a link to reveal the address it is taking you to.
- Does it match the link text, is the URL taking you to a legitimate site?

Check the subject line

- Does the subject line encourage you to act quickly?
- Does it say 'URGENT', 'Action needed' 'Limited time only'?

Check if there is an attachment

- Scammers may add documents that contain malicious software (malware).
- This malware could enter your device if the document is opened.
- Do not click or download these files.

Check the message

- Are there any spelling or grammar errors?
- Are they trying to scare you with words such as, 'your account has been suspended' or 'payment required'?

Check what they are asking

- Are you being asked to confirm your password, credit card number, or other private information?
- Always check you are on the secure, legitimate site before entering any details.

If in doubt – delete it out!

© The Security Company (International) Limited 2023.