Check the email address

Fraudsters will pose as reputable individuals.

- If the name attached to the email is familiar (someone you know or regularly correspond with), check **to be sure the email address matches.**
- If it's a co-worker, the email address should be listed in the company email directory (if you have one).
- Be sure the domain name is spelt correctly. Often, fraudsters will create fake domains that closely resemble the real one, but will alter a letter or two hoping that recipients don't notice. For example, J@rnbusiness.com vs J@mbusiness.com.
- Be aware that the displayed name can be hiding the actual sender's email address.

Check the email thoroughly

Urgency is a red flag.

- Treat any email relating to payments as suspicious if it uses urgent language, or provides excuses for the lack of a call back option.
- Some phishing emails are poorly written. Even if the spelling is correct, they often contain poor grammar. Treat external emails with extreme caution, especially those containing links or attachments. Be aware that Generative AI is making it easier for attackers to create convincing malicious emails.
- If you are not expecting the communication and/or do not recognise the sender, **do not click links or open attachments**.