

Ask yourself: Does this look like usual business?

Phishing emails **sometimes come from legitimate email addresses**.
There are many other ways to detect a phishing email.



Is the email **marked urgent**?



Do the **links, URLs or attachments** look suspicious?



Is this how you would **normally receive shared files**? Is this how you would normally be asked to **change a password** or **change bank details**?



Do the **attachments** or **subject lines** follow the **usual naming conventions** of your workplace?



Are the **subject lines** **generic** or **unspecific**?



Would **this person** usually **email you** about **this matter**?



Is the email asking me to go to a website to **enter personal details** or my **password**?



Is there **little** or **no explanation** of **requested changes** regarding an **important matter**?



If something looks strange, or you clicked on a suspicious link, **report it immediately to your cyber security team**.