How to spot a scam

Check the sender

Double check the sender and know the signs. Inspect the 'from' e-mail address, look for poor spelling or grammar and strange greetings or signatures.

Don't login via email

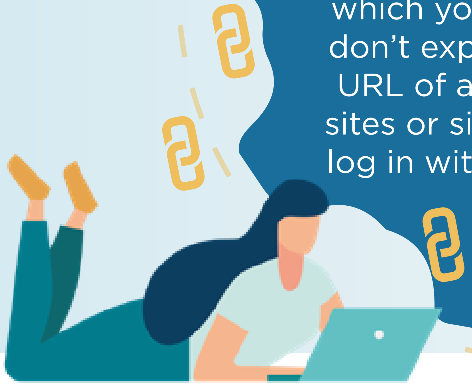
Legitimate sites will almost never ask for login details from an email. If you receive an email asking for your login details, is it likely that cybercriminals are trying to steal your login credentials.

Sense of urgency

Be wary of urgent requests asking you to take immediate action or buy something like gift cards or prepaid debit or credit cards. Often this may look like it's from a supervisor or personal of authority, asking you if you are available and can do them a favour.

Avoid the links

Do not click on the links, shared documents, or open attachments in messages with which you are unfamiliar or don't expect. Check the full URL of a link, look for fake sites or sites that ask you to log in with your credentials.



Is it really real?

Be suspect of any email that looks to be from IT, banks and financial institutions, Apple, Google, Microsoft or any other reputable organisation asking you to log in to verify your account information or are threatening to deactivate your account unless you respond.