The ABCs of staying safe from email scams

Avoid the links

Do not click on links, shared documents, or open attachments in messages with which you are unfamiliar or don't expect.

Be wary of urgent requests

Be mindful of any urgent request asking you to take immediate action or buy something like gift cards or prepaid credit and debit cards. Often this request may look like it is from a supervisor or person of authority, asking if you are available, can do them a favour, or to take quick action without thinking.

Check the details

Double check who is sending the email and know the signs:

- inspect the 'from' email address and make sure it matches who claims to be sending the email
- look for poor spelling and grammar and strange signatures
- ignore any requests asking you to provide login, account or other personal information
- check the full URL of a link, look for fake sites or sites that ask you to log in with your credentials.

Don't take the bait

Be suspect of any email that looks to be from IT, banks, financial institutions and well-known organisations, asking you to log in and verify your account information or makes threats to deactivate or cancel your accounts unless you respond.

Think before you click