Common types of scams

Password Reset

This is a common scam email stating you have requested a password reset. Chances are that you did not request this reset, and cyber criminals are hoping you will be alarmed and will quickly click on the link without much thought.

Shipping Notifications or Order Cancellations

These emails can be hard to detect as scammers will mimic real email notifications sent by companies such as Amazon or Australia Post, to make you think they are legitimate. Check for spelling and grammatical errors within the email and hover over links and see what URL they actually redirect to.

Open an important attachement or email

Scammers will send emails posing as members of well-known organisations with the goal to get you to open an important attachment or click on a link. Be careful! Opening attachments can install malware and links can redirect to fake pages prompting you to enter login credentials.

Account Cancellation

This scam claims you've requested an account to be cancelled. Scammers claim you need to log in to reverse the cancellation request and send you a link to click on. In reality, the information you provide to login to the fake site is captured and used by the attacker to login to the real site and do damage.

Urgent Request

Scammers pose as a government or known organisation claiming they have an emergency and need you to urgently pay a fine by gift card or transfer money. The use of urgent language is used to attempt to scare you into action. Don't be fooled or rushed into anything.