STAYING CYBERSMART ONLINE

SUSPICIOUS MESSAGES

TRUST IN EVERY LAYER

ANZ

SUSPICIOUS MESSAGES
PREVENTION IS THE FIRST LAYER OF PROTECTION

Email, social media, phones calls and SMS are all a part of our daily life. Cybercriminals now use these channels to send messages pretending to be from a legitimate organisation to entice people to reveal their personal and confidential information such as banking details and passwords.

WHAT COULD HAPPEN?

Malware - Clicking on links or attachments in suspicious messages could lead to malicious software (malware) being downloaded onto your computer or mobile devices. Malware can infect your devices and access your personal and confidential information.

Fake websites - Responding to or clicking through suspicious messages could also direct you to fake websites where you may be asked to enter your login and password details which may be used to conduct fraud.

POSSIBLE SIGNS OF A SUSPICIOUS MESSAGE:

- The message is unexpected, is from an unfamiliar sender and/or contains unfamiliar links and attachments
- The message creates a sense of urgency to act. E.g. 'Update your online account details immediately' or 'Click now to claim your prize!'
- The message requests your personal or financial information, even if it appears to be from a legitimate source

WHAT IF YOU RECEIVE A SUSPICIOUS MESSAGE?

Before clicking any links, attachments, or following any instructions, contact the organisation sending the message. It is important to use a phone number from the organisation's website to confirm the legitimacy of the message.

WHAT IF YOU HAVE CLICKED ON A SUSPICIOUS LINK OR AN ATTACHMENT?

- Disconnect your device from the internet to prevent the cybercriminal from sending any personal or confidential information from your device
- Back up your files to a personal computer, external hard drive, network, or cloud
- Scan your computer or device for any malware using appropriate security software, or seek assistance from professional technical support provider
- Immediately contact your relevant financial institution if you see any signs of unexpected transactions

FOR FURTHER INFORMATION ABOUT STAYING SAFE ONLINE VISIT ANZ.COM AND SEARCH 'SECURITY'.

anz.com

Australia and New Zealand Banking Group Limited (ANZ) ABN 11 005 357 522.