



STAYING CYBERSMART ONLINE

# SUSPICIOUS MESSAGES

---

TRUST IN EVERY LAYER

# 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](https://anz.com) AND SEARCH 'SECURITY'.

In accordance with Our Guidelines to Email and SMS Communications, ANZ will not send you an email or SMS asking you to verify or provide your account Details, financial Details, or login details for ANZ Phone Banking, ANZ Internet Banking or ANZ Mobile Banking. We send emails and these often contain hyperlinks. However, if we send you an email with a hyperlink, the link will take you to a page on the ANZ website, where you can find out more before logging in, applying or downloading.

This document raises awareness and provides general information only. It may be necessary or appropriate to ensure that measures are taken in addition to, or in substitution for, the measures presented having regard to your particular personal or business circumstances. This flyer is distributed in Australia by Australia and New Zealand Banking Group Limited ABN 11 005 357 522 ("ANZBGL"); in New Zealand by ANZ Bank New Zealand Ltd; and in other countries by the relevant subsidiary or branch of ANZBGL, (collectively "ANZ"). Nothing in this flyer constitutes a recommendation, solicitation or offer by ANZ to you to acquire any products or services, or an offer by ANZ to provide you with other products or services. All information contained in this flyer is based on information available at the time of publication. While this flyer has been prepared in good faith, no representation, warranty, assurance or undertaking is or will be made, and no responsibility or liability is or will be accepted by ANZ in relation to the accuracy or completeness of this flyer. 05.2015 AU20999