About Scams and How to Protect Yourself

1300 046 888

IMPORTANT INFORMATION

About Scams & How To Protect Yourself

Scam activity is on the rise in Australia. Scammers are using a wider array of methods, techniques, and communication avenues to reach unsuspecting victims. They are also becoming more refined at impersonating legitimate government departments, businesses, and organisations to attempt to gain access to your money and personal information. In 2021 alone, the ACCC recorded 286,602 reports of scams amounting to losses at almost $323 million.

Scam Calls, Messages and Emails

Scam calls, messages or emails are designed to dishonestly obtain a benefit or cause a loss. Generally, they are trying to attempt to fraudulently obtain money or information from you. Often the scammers claim to be from well-known organisations including government institutions (such as Australia Post, or the Australian Taxation Office, the Australian Federal Police), or from well known businesses (such as Microsoft, Apple (iTunes), the NBN, banks, and telecommunications companies).

EXAMPLES OF COMMON SCAMS

Tech Support Scams

Generally, the scam begins with a scammer pretending they're calling from the technical support team of a telecommunications company, a computer company, or a software company. The scammer will try to scare you about a computer or internet problem so that they can convince you to give your personal or banking details, and/or direct access to your computer via a remote desktop application.

Wangiri Fraud

Wangiri fraud is when you receive missed calls from international numbers you do not recognise or either a mobile or fixed-line phone. Fraudsters generate missed calls to a whole range of Australian mobile numbers, in the hope you will call back their expensive international numbers, generating profit for the customer. Do not call any unrecognised international numbers back. Especially if no voicemail is left.

Email or SMS Phishing Scams

You may receive an SMS claiming to be from a well-known organisation asking you to verify personal information, such as passwords and credit card details. These messages may also contain links to fraudulent websites that may infect your device with malicious software (Malware). Some scams involve messages containing prizes or rewards such as "Congratulations! You've been selected as one of our lucky customers to be given a brand new [tablet/mobile/laptop]". Do not reply to the message. Take a screenshot if possible. Do not click on any links or provide any personal details if prompted or asked.

COVID-19 SMS Scam

People have reported receiving SMS purporting to be from the 'Australian Government Department of Health' containing messaging relating to issues around COVID-19 Safety, or 'testing results'. These

scams contain fake links to government websites, where you may be exposed to attempts to obtain your personal information.

Malware

The most common way you may be exposed to malicious software (malware) is where you may receive a scam email or text message asking you to click on a link or open an attachment. This may result in you downloading software like viruses or other unwanted programmes on your device so that these can be used to:

- access stored personal information,
- lock your device and demand payment to unlock it (Ransomware)
- use your device without your knowledge, for example to distribute spam emails or participate in cyber attacks
- install keyloggers which track and log the keys being typed (especially for account details and passwords)

PROTECTING YOURSELF FROM SCAMS

- Protect your personal information by not sharing it with unknown or unsolicited contacts.
- Do not respond to missed calls or SMS from unknown international Numbers, unknown Australian Numbers or an unknown source.
- Block suspicious or unknown Australian Numbers or international Numbers on devices. Use Blocking services or products where available.
- If you do not recognise the number, let the call go through to voicemail. If a voicemail is left, organisation the caller is purporting to be from but do not call back any number they leave. Instead, call the publicly listed official number of the organisation.
- Contact your financial institution immediately if you believe you have lost money to a scammer.
- Change default PINs and passwords on new equipment.
- Select strong PINs and passwords (Not “1234” or “0000” or “password” etc).
- Lock devices with a secure PIN.
- Ensure voicemail PINs are secure.
- Disable PABX ports and features that are not used (e.g. remote call-forwarding).
- Change PINs and passwords regularly.
- Do not click on web page links (URLs) or make return calls to telephone Numbers contained in SMS from unknown international Numbers or unknown Australian Numbers or an unknown source.
- Block suspicious or unknown Australian Numbers or international Numbers on devices.
- Use blocking services or products where available.
- Ensure you have anti-virus software and that it is up-to-date.
- Avoid doing any task requiring personal details (such as online banking) from public access computers or via public Wi-Fi hotspots.
- Do not download applications from third-party download sites.
- Avoid opening suspicious or unsolicited emails –delete them directly from your inbox. If you do accidently click on a link which opens a website, do not enter any information onto the website and delete the email.
- Delete any unknown or unsolicited SMS immediately. You may choose to take a screenshot for recording purposes.

SOME THINGS TO LOOK OUT FOR WITH SCAM CALLS, MESSAGES AND EMAILS

- Suspicious looking URLs or Sender ID, even with what appears to be a single letter misspelt.
- Unaddressed or emails with generic greetings such as “Dear Sir/Madam”, or “Dear Customer”.
- Emails that contain a web page link (URL) that takes you to another website.
- An ‘urgent’ request for information such as “updating your credit card details” due to a “failed payment”.
- Emails that include a .zip, .exe or other suspicious attachment.
- Emails that include grammatical errors, spelling mistakes, broken sentences, or errors in layout or logos.
- Messages with scare tactics such as “your account has been compromised”, or “a warrant has been issued for your arrest”.
- Deals, offers or prizes, such as holidays, goods and services, and cash prizes.
- Requests for personal information.
- Requests to ‘click a link’ and fill in a web form.
- Emails that contain account information that does completely match the information that you know an organisation may have about you, for example outdated personal information.
- Low call quality – this can indicate the source being a non-secure off-shore location.
- Poor or unprofessional communications skills.
- High pressure tactics, such as requiring urgent action to avoid a fine or penalty, resolve a debt with a government body, prevent disconnection of an important service (electricity, water, internet), deal with a security threat or technical issue on your device or internet connection. If you have been scammed or are concerned that you have been...
- Report this to the ACCC’s Scam watch website
- Contact the organisation that may be involved or that the scammers claim to be from and report it to them.
- In event of a suspected scam call reaching you, please immediately report this to our dedicated support teams who in turn will escalate and engage with our upstream carriers to investigate the call 1300 017 150.
- Contact your local police.
- Report the crime to the Australian Cyber Security Centre (ACSC).

FOR MORE INFORMATION ON SCAMS

The Australian Communications and Competition Commission (ACCC) The Little Black Book of Scams

Scam Watch https://www.scamwatch.gov.au/ including where you can get help

ACMA https://www.acma.gov.au/scams-and-online-misinformation

Stay Smart Online https://www.cyber.gov.au/

The Telecommunications Industry Ombudsman (TIO)