REPORT SCAMS

TO SCAMWATCH

Scamwatch is run by the Australian Competition and Consumer Commission (ACCC). It provides information to consumers and small businesses about how to recognise, avoid and report scams. https://www.scamwatch.gov.au/

If you've lost money to a scam or given out your personal details to a scammer, you're unlikely to get your money back. However, there are steps you can take straight away to limit the damage and protect yourself from further loss.

1. Contact people you know
2. Contact your financial institution
3. Recover your stolen identity
4. Report scams to the authorities
5. Get help from Australian agencies
6. Report scams to Facebook services
7. Change your online passwords
8. Contact your local consumer protection agency
9. Contact a counselling or support service
10. More information

Contact people you know

You should warn your friends and family about scams. If you're a business, let your industry association and other contacts know about the scam.

Contact your financial institution

If you've sent money or shared your banking details with a scammer, contact your financial institution immediately. They may be able to stop a transaction or close your account if the scammer has your account details. Your credit card provider may be able to perform a 'charge back' (reverse the transaction) if your credit card was billed fraudulently.

If you're not sure if you're being scammed, **stop sending money**. Scammers will keep asking for more money until you stop.

Recover your stolen identity

If you suspect you are a victim of identity theft, it is important that you act quickly to reduce your risk of financial loss or other damages.

You can:

- **contact IDCARE** - a free government-funded service which will work with you to develop a specific response plan to your situation and support you through the process. Visit the IDCARE website or call 1800 595 160 (if in Australia) or 0800 121 068 (if in New Zealand)
- **apply for a Commonwealth Victims' Certificate** - a certificate helps support your claim that you've been the victim of identity crime and can be used to help re-establish your credentials with government or financial institutions. Visit Victims of Commonwealth identity crime

Report scams to the authorities

We encourage you to report scams to the ACCC via the Report a scam webpage.

You can also report a scam to the appropriate agency to help them warn the community about scams and take action to disrupt scams.

Type of incident	Agency
Banking	Your bank or financial institution
Centrelink, Medicare, Child Support and myGov related scams	Services Australia Scams and Identity Theft Helpdesk - call 1800 941 126
Cybercrime	ReportCyber
Financial and investment scams	Australian Securities and Investments Commission
Fraud and theft	Your local police - call 131 444 In Victoria call your local police station
Image based abuse (sextortion), cyberbullying and illegal content	Office of the eSafety Commissioner
Spam	Australian Communications and Media Authority
Tax related scams	Australian Taxation Office

Get help from Australian agencies

For tips about online safety and security and an Australian Government directory for where to get help see the Be safe Be alert online quick reference guide.

Report scams to Facebook services

If you experience a scam on Facebook, Messenger, Instagram or WhatsApp you should contact the platform and inform them of the circumstances surrounding the scam.

How you can report scams on Facebook services - guidance for Australians

Change your online passwords

If you think your computer or device has been hacked or infected with malware or ransomware, use your security software to run a virus check if you think your computer has been compromised.

If you think one of your online accounts (e.g. your bank account, email, online shopping account or social networking site) has been compromised, you should change your password immediately. Most reputable websites provide step-by-step instructions for how you can recover a hacked account.

Contact your local consumer protection agency

While the ACCC is the national agency dealing with general consumer protection matters, state and territory agencies may also be able to assist you and also provide scam alerts and information on how to avoid them.

- Access Canberra
- Consumer Affairs Victoria
- New South Wales Fair Trading
- Northern Territory Consumer Affairs
- Queensland Office of Fair Trading
- South Australia Office of Consumer and Business Affairs
- Consumer, Building and Occupational Services Tasmania
- Western Australia Department of Commerce—Consumer Protection

Our Network

If you believe that you have experienced misuse or abuse online, and have technical details to show that it originated from a 1telecom service, please tell us about it below so we can investigate further.

You can also use this form to report suspicious emails, phishing scams, telephone scams, and suspicious SMS messages which relate to 1telecom as a brand.

Please note: We may not respond to all submissions, and any responses or follow-up will be via email only.

Not with 1telecom?

If the misuse originates from another network, you should report the event to that Internet Service Provider (ISP) directly.

MISUSE OF SERVICE REPORT

	First	Last
Name		
Phone Number		
Email Address		
Reported to Scamwatch?		

select one of the following

- ○ Malicious network traffic coming from a Buroserv IP address or system
- ○ Spam coming from a Buroserv IP address or system
- ○ Suspicious emails, phone calls, SMS messages or phishing scams
- ○ Prohibited Content
- ○ Copyright infringement (use of your copyright eithout permission)

Please provide logs that contain the follow ing information:

1. The exact date and time of the event (including time zone or GMT offset),
2. The source IP address,
3. The destination IP address, and
4. The source & destination ports (if possible)

Without this information, w e may be unable to investigate.