COVID-19 SCAMS

Last updated June 2020

ECONOMIC JUSTICE AUSTRALIA
For a fair social security system

A scam is an illegal scheme for making money, especially one that involves tricking people.

The Australian Government website Scamwatch.gov.au notes that since the outbreak of COVID-19 it has received over 2,700 reports of scams relating to COVID-19, with over $1 million lost to scams.

This factsheet covers:

- Types of scams that can target people receiving Centrelink payments
- How to protect yourself
- Reporting a scam.

Types of Scams

Scammers are expert and have many tricks to get people's trust. Scammers may:

- call you or come to your door
- contact you via social media, email or text message – possibly pretending to be a friend
- set up websites that look real – pretending to be government or business
- collect information about you so when they make contact they are more convincing.

Phishing scams

Phishing is a type of fraud used by criminals to deceive victims by impersonating well-known and trusted organisations or people. Phishing email or text messages are designed to look genuine. Scammers often pretend to represent an organisation by copying the format used by the organisation and including their branding and logo. They are trying to take you to a fake website that looks real but has a slightly different address. For example, if the legitimate site is 'www.realbank.com.au', the scammer may use an address like 'www.reallbank.com'.

If you give a scammer your details online or over the phone, they will use your details to carry out fraud – such as using your credit cards or stealing your superannuation. Known COVID-19 phishing scams include fake messages pretending to be from:

- Australian Government
- MyGov
- Australia Post
- Department of Health
- Australian Taxation Office
- Services Australia or Centrelink
- World Health Organisation and other international health sector organisations
- Banks, supermarkets or travel agents
- Insurance and telecommunications companies
- Microsoft or IT help desks.

The scammers send fake messages, either through email or SMS, pretending to be from real and well known businesses and government departments. These messages may ask you to:

- enter your personal information on a fake website
- trick you into opening malicious links or attachments that will damage your computer records
- try to get remote access to your computer
- request repayment of a fake debt, such as a tax debt, or an overdue account
- request payment for a fake service or something you did not purchase.

They may even send a link telling you to click the link to find out where you can get COVID-19 relief payments.

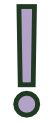
Superannuation scams

Scammers are targeting people who are looking for information about the Government's COVID-19 early release superannuation scheme.

These scams usually begin with someone calling you claiming to be from a superannuation fund or a financial services company. The scammer may try to get information about your superannuation by offering to:

- check whether you are eligible to access your superannuation early during COVID-19
- help you access the money in your super account
- check that you have not been locked out of your super account or telling you that your inactive super account will be locked if you do not merge it with another super account
- check whether your super account is eligible for various benefits or deals.

The scammer will then ask for your personal details so that they can "help you" and they may ask for your log in details. The scammer may also ask for payment in return for their help.



Scammers are also sending text messages claiming to be from the National Superannuation Review offering to review your superannuation.

If you are contacted in this way, do not share ANY personal details. End the call and call your superannuation fund directly to find out if the call was legitimate.

The only way to apply to withdraw your super under the early release scheme is online through the MyGov website. There is no need to involve a third party or pay a fee.

Once scammers have access to your information, they can set up a fake MyGov account and apply to access your superannuation under the early access scheme. You should regularly check your super account to ensure that the balance has not changed.

How to protect yourself

There are things you can do to stop yourself from being scammed:

What to do
Do not provide your personal, banking or superannuation details to strangers who have approached you. This includes your date of birth, Medicare or driver's licence number, log in details or account numbers. Never respond to unexpected messages or calls that ask for personal or financial details. Just press delete or end the call. Remember that reputable organisations including government

departments, banks, Amazon, PayPal, Google, Apple and Facebook will not call or email to check or update your personal information.
Do not click on hyperlinks in text/social media messages or emails from people you don't know, even if they appear to come from a trusted source. Always go directly to the website of a financial institution or online banking system and always log out when you're finished. Never provide a stranger remote access to your computer, even if they claim to be from a company like Telstra or your NBN provider.
Read all messages carefully and look for anything that isn't quite right, such as tracking numbers, names, attachment names, sender email address, message subject and hyperlinks.
Regularly check your superannuation account balance to ensure it has not changed.
Remain alert about unsolicited or unexpected contact from government agencies or banks – if it seems suspicious or unusual, it may be a scam. Take your time and consider who you might be dealing with. If you think the contact may be OK, contact the organisation yourself and ask them about the phone call/email/text message – if it's legitimate they can confirm it and if not, there's a good chance they already know about the scam. By alerting them to it, you can help protect others.
Avoid using shared or public computers to log into sensitive websites. Also make sure you keep your details up to date with organisations you deal with so they can notify you if something goes wrong.
Protect your passwords – choose difficult passwords that aren't related to personal information such as your date of birth or phone number, and change your passwords regularly. Be careful how you store your passwords and never share them with anyone.
Protect your devices – installing and updating security software, such as firewall, anti-virus, anti-spyware and spam filtering software, helps protect your devices against fraudulent activity by detecting and preventing online attacks.
Monitor the Scamwatch news webpage for general warnings and media releases on COVID-19 scams.
Talk to your family and friends about the risk of scams, and make sure they protect themselves.

Reporting a scam

If you have been scammed or have seen a scam, you can make a report on the Scamwatch website and report it to ReportCyber.

For more information, you can visit one of the following websites:

- Scamwatch
- Australian Cyber Security Centre, including its detailed report on COVID-19 scams
- To stay up-to-date on the latest online threats and how to respond, sign up to the Stay Smart Online Alert Service

Where can I get help?

If you think you may have been scammed you can get free legal advice from your local community legal centre – see https://clcs.org.au/findlegalhelp

For where to get free legal advice about Centrelink issues and appeals see http://ejaustralia.org.au/legal-help-centrelink/

This factsheet does not constitute legal advice.

Please contact any of our member centres if you wish to obtain free legal advice.
Find your closest member centre at www.ejaustralia.org.au