Superannuation early-access scams

May 2020

Many Australians are facing financial hardship due to the COVID-19 pandemic. On 22 March, the Australian Government announced eligible individuals would be allowed early access to their superannuation.

Eligible individuals can withdraw in two instalments of up to $10 000 each. For more information, see the Treasury's fact sheet.

Scammers are taking advantage of the government's early-release measures in a variety of phishing scams designed to steal your superannuation.

You may want to check your myGov account to ensure there are no unexpected applications for financial relief on your behalf and that your contact details have not been altered. Even if you cannot recall giving your information to a scammer, it's possible your personal details have been revealed in a data breach that may have occurred some time ago.

Telephone

Scammers are cold-calling people and claiming to be from organisations that can help you get early access to your super. The scammers use a variety of excuses to request information about your superannuation, including offers to:

- help you access the money in your superannuation
- ensure you're not locked out of your account under new rules
- check if your superannuation account is eligible for benefits or deals.

Email and text messages

Scammers use fake vouchers, financial assistance claims or general information around COVID-19 as bait to 'phish' for your personal information, including your superannuation. Once they have your details they can pretend to be you and access your super.

How are scammers getting your personal information?

Scammers are sending emails and text messages impersonating well-known businesses and government agencies such as Services Australia or myGov, the Department of Health and the Australian Taxation Office (ATO), among others.

Scammers always use a disguise to trick you. In a recent example scammers used fake Coles and Woolworths messages claiming to offer free vouchers if you provided your personal information.

Remember These scams contain links to websites designed to steal your personal information or malicious attachments that will install malware on your device if opened.

Scammers can also get their hands on your personal information from a data breach if personal information is accessed or disclosed without

authorisation or is lost. The Office of the Australian Information Commissioner has information about data breaches and what to do if one happens to you. You can also see if your data is in any known data breaches at the website 'Have I Been Pwned?'

How to check your super and report unauthorised access to your account

1. Check your myGov account or contact the myGov helpdesk on 132 307 to see if an application for early access to your superannuation has been made fraudulently on your behalf.
2. If an early-access application has been made and you did not make it, or you do not have a myGov account, contact your superannuation fund and ask them not to proceed with the withdrawal. Tell them you did not make the request.

   Remember If you receive any notification about an early-access application that you have not made, contact your superannuation fund immediately.

   When contacting your superannuation fund or any government agency, always use contact details you have sourced independently. Do not use contact details in a text or email you have received.

3. Notify the ATO on 1800 467 033 that someone has attempted to withdraw your superannuation without your consent.
4. Call IDCARE on 1800 595 160—it provides specialist support and guidance to help with identity-related issues.

Tips to avoid superannuation scams

- Never give information about your superannuation to someone who has contacted you, even when you think it is a trusted organisation.
- The ATO is coordinating the early release of super through myGov. There is no need to involve a third party or pay a fee to get access under this scheme.
- Never follow a hyperlink to reach the myGov website. Always type the full name of the website into your browser yourself.
- If you have given information about your superannuation to a scammer, immediately contact your superannuation fund. If you have given personal or banking details, you should also contact your financial institution.

More information

More information on scams is available on the Scamwatch website, including how to make a report and where to get help.

ACCC 05/20_20-06 www.accc.gov.au