

Fraud and how to protect your superannuation

Fact Sheet

Sadly, fraud is a major risk when it comes to protecting your money in today's society and that includes your super. There is a growing tendency for criminals to attempt to access the superannuation of Australians through identity fraud.



How do you help protect my super against identity fraud?

To help prevent the risk of identity fraud on your account, we have incorporated these measures:



Identity fraud can result from:

Someone stealing your mail or other personal papers and then pretending to be you to access your account.

Malware software, such as viruses, spyware and trojans, which are malevolent programs that are installed onto your device without your knowledge and can be used to potentially steal your personal information.

Phishing scams, which involve sending emails or SMS messages to trick you into handing over your personal information.

Other techniques that cyber criminals are using include password spraying and email targeting.

Password spraying involves using passwords from previous data breaches or common passwords to gain access to multiple sites where the same password has been used.


Through the targeting and accessing of email accounts, cyber criminals can leverage the reset password functionality for other online services to obtain personal information.

- Removing any unnecessary personal information from any correspondence we issue to you.
- Contacting you to verify the legitimacy of any suspicious change or transaction request.
- Monitoring benefit payment and transfer requests to detect those that may be fraudulent.
- Training our staff to identify fraudulent requests and activity, with firm proof of identity measures.
- Implementing security measures to reduce the chance of unauthorised access of your details.

How you can protect your super and online account

There are several actions you can take to ensure you outsmart any potential theft attempt.

<p>If a phone call from someone purporting to work for us arouses your suspicions, check with us to confirm the legitimacy of the enquiry before providing any information.</p>	<p>Monitor your accounts regularly and review all correspondence from us to note any changes to your account. If you notice any changes that were not authorised by you, please contact us as soon as possible.</p>
<p>Use a long, strong and unique password for each online account and don't reuse the same password for multiple sites.</p>	<p>Keep your personal account and online login details secure and never provide this information to anyone. We will never ask you to disclose your password.</p>
<p>Store your statements and other personal documents in a secure location.</p>	<p>Do not click on any links in unsolicited emails or SMS messages without first verifying their legitimacy.</p>
<p>Advise us if any of your personal documents such as your passport, licence, phone etc are lost or stolen, or your computer/email account has been compromised.</p>	<p>Keep your login details secret and never give it to anyone face to face, over the phone, or in an email. We will never ask you to disclose your password.</p>

 For more information on how we protect your superannuation account, please call us on 13 11 55 between 9am and 5pm (Eastern Standard Time) Monday to Friday.