Protect your super against fraud

September 2019

Australian superannuation funds represent a big and growing temptation for criminals, with identity theft one of the biggest risks when it comes to safeguarding your money.

Identity fraud can start with someone stealing your mail or other personal papers, creating false documents with the information they've stolen, and then attempting to access your account pretending to be you. Phishing scams, whereby emails or SMS messages are sent to trick you into handing over your personal financial or account details are another way scammers attempt to collect your personal information or gain access to your online accounts, and you should be wary of giving confidential information to anyone via email or over the phone.

Cyber criminals are using techniques such as password spraying, where common passwords and passwords from previous data breaches are used to gain access where the same password has been used by a person across multiple sites such as social media, email accounts, banking, a local pizza shop. Always use a strong unique password for each online site you visit.

Increasingly a common attack vector is targeting email accounts and once the cyber criminals gain access, they leverage the reset password functionality for other online services, such as banks, social media accounts, etc to gain further access. Where possible, enable multi-factor authentication to add additional security to your accounts.

Many of these scammers and cyber criminals can be cunning and highly organised, so the key is to be on your guard and ensure the security of your online accounts.

How Sunsuper helps prevent identity fraud

Sunsuper helps to prevent fraud with a range of measures to protect you including:

- Omitting unnecessary personal information, like your date of birth, in correspondence to you,
- Contacting you to verify the legitimacy of a change of your personal or contact details, if we are suspicious about the request,
- Monitoring benefit payment and transfer requests to detect those that may be fraudulent,
- Contacting you to verify the legitimacy of benefit payment or transfer requests if we are suspicious about the request,
- Training our staff to identify fraudulent requests and activity,
- Putting security measures in place to reduce the risk of unauthorised access to confidential data and documents, and
- Having strict proof of identity measures in place (see our Proof of identity requirements fact sheet at sunsuper.com.au for more information).

Tips to protect your super and online account

- Keep your Sunsuper Member Online login details secret and don't give it to anyone over the phone, or in an email. Sunsuper will never ask you to disclose your password.
- Use a long unique strong password or pass-phrase for each online account or service. Do not reuse the same password on multiple sites. Consider using a Password Management Tool to generate and store your secure passwords.
- If a phone call from someone purporting to work for Sunsuper arouses your suspicions, check with us on 13 11 84 to confirm the enquiry is legitimate before giving out any information.
- If a phone call from someone purporting to work for Sunsuper arouses your suspicions, check with us on 13 11 84 to confirm the enquiry is legitimate before giving out any information.
- Look out for your annual statement which is usually sent to you via your preferred channel from September, and monitor your financial and super accounts regularly on-line or via the Sunsuper mobile app.
- Review all correspondence from Sunsuper to note any changes to your account. If you receive notification of a change to your details that was not authorised by you please contact Sunsuper on 13 11 84 to notify us as soon as possible.
- Advise us if any of your personal documents like your passport or drivers licence are lost or stolen, your phone has been stolen, or your computer/email account has been compromised.
- Store your Sunsuper statements and other personal documents in a secure location.
- Securely destroy or shred any unnecessary documents that contain your personal information.
- Collect your mail on a daily basis and make sure your mailbox is secure.
- Do not click on any links in unsolicited email without first verifying their legitimacy.
- Take steps to protect your phone and email accounts. This can include such precautions as securing your phone by enforcing a password, PIN or fingerprint scan to unlock, and enabling multi-factor authentication on your email account.

By working together and following these few simple measures, we can reduce the likelihood of fraud and help protect your super.

13 11 84 (+61 7 3121 0700 when overseas)
GPO Box 2924 Brisbane QLD 4001
sunsuper.com.au
twitter.com/sunsuper
facebook.com/sunsuper
linkedin.com/company/sunsuper