Spotlight on scams

Last year, Australians made over 600,000 scam reports and lost $2.7 billion[1].

Superannuation is often targeted by scammers as most working adults in Australia will have a super account containing a significant amount of money.

As scams and cybercriminals get increasingly sophisticated, we must protect ourselves by staying informed and learning how to spot the signs of a scam to reduce the risk of falling prey.

Here are a few ways scammers may try to access your super:

- **Impersonation and phishing for personal details**

Scammers may impersonate trusted organisations such as a bank or super fund, contacting you via SMS-es, calls and emails, and request you to take action via the links they provide. Clicking on such links may take you to a fake webpage where they steal your login information when you attempt to log in to your account.

A scammer could use that information to access your super account or myGov account to steal your personal information. They could then create another super account or a fake Self-Managed Super Fund (SMSF) in your name, then transfer the funds and withdraw them.

- **Promises of high investment returns through an SMSF**

If it sounds too good to be true, it probably is. Scammers may try to lure you into opening an SMSF through them, with false promises of high investment returns or unusual investment vehicles such as cryptocurrency.

Such scammers may attempt to build trust over a period of time to convince you to open the SMSF and provide them with authority to manage the funds. When that happens, they'll be able to access and withdraw the funds without your knowledge.

- **Deepfake technology**

With advancements in AI technology, scammers create realistic videos and audio clips impersonating high level executives or familiar voices. Please be aware if you receive a video call or voicemail asking for your superannuation information or other personal information. Always verify through secondary contact especially if it was unexpected. If it seems suspicious, it likely is.

How you can protect yourself

There are many things you can do to stay safe and reduce the risks of getting scammed.

- Ensure your accounts have strong, unique passwords and change them frequently. Where available, make sure you have Multi-Factor Authentication (MFA) enabled.
- Check your account and statements regularly for any unusual transactions.

- Be wary of providing your personal identification documents to people you don’t know.
- Act quickly if something feels wrong. If you've shared financial information or transferred money, act quickly by contacting your bank immediately. Help others by reporting to Scamwatch Report a scam.
- Do your research and only engage licensed financial advisers. You can check if someone is licensed on MoneySmart’s Financial Advisers Register. You can also use APRA's Disqualification Register to check if someone has been disqualified.

We’re here to help

If you’re concerned about a possible SMSF scam or suspect that your identity has been compromised, please contact us on 1800 640 886 immediately.

Visit **mediasuper.com.au/supersafe** to learn more on how you can protect your super from scammers.

---

[1] The Australian Competition & Consumer Commission, Scam losses decline, but more work to do as Australians lose $2.7 billion, 8 April 2024, https://www.accc.gov.au/media-release/scam-losses-decline-but-more-work-to-do-as-australians-lose-27-billion