Protecting your superannuation from cyber threats and scams

April 2025

As a valued member of ANZ Staff Super, we take the security of your superannuation seriously.

This factsheet explains some of the current cyber and scam risks that can impact superannuation accounts and shares some tips on how to stay safe.

Cyber threats

A cyber threat is a broader risk to your personal or financial information or account that comes from things like hackers, viruses or security breaches. It includes attempts by criminals to access your personal or financial information through various systems, often without you knowing.

In the context of superannuation, this could mean someone trying to gain access to your super account by using personal details – like your password – that were stolen in an unrelated data breach, such as from a shopping or email account. Once they have that information, they may try to log in to your super account to take control of it.

That's why it's important to use strong, unique passwords and never reuse the same password across different accounts.

How we are working to help keep your super safe

We have a range of security measures in place to help protect your account, including:

- Mandatory multi-factor authentication on the Member Online portal and the ability to enable biometric authentication on the Member App
- If your contact details are changed electronically, we will send an alert email to you
- If you call us, we will ask you a number of security questions to confirm your identity
- If you initiate a payment request (such as setting up a pension or seeking a compassionate or hardship payment), you will need to meet strict identification requirements and provide confirmation that the receiving bank account is in your name.

In addition to these steps, our administrator deploys a range of continuous monitoring and threat detection mechanisms that target suspicious or unusual instructions or attempted transactions. The security of your account is monitored 24 hours a day, 7 days a week.

Simple steps you can take to reduce cyber risk

While cyber threats are usually technical in nature, there are still things you can do to help protect your funds:

- Use a strong, unique password for your super account
- Make sure you only log in through the official website and app, never through links in unexpected emails or texts
- If you receive notification of a change of details that you didn't make, or notice anything irregular, call us on **1800 000 086.**

Scams

A scam is a type of fraud where someone tries to trick you into giving away your personal or financial information, often by pretending to be from a trusted organisation—like your super fund, a government agency, or a bank.

In the context of superannuation, a scam might involve a fake phone call, text message, or email asking you to confirm your account details, transfer funds, or click on a suspicious link. These scams can be very convincing and often create a sense of urgency to get you to act quickly. It's important to remember that your super fund will never ask for your password or login details over the phone or by email.

If something doesn't feel right, it's always safest to hang up or delete the message, then contact us directly on **1800 000 086.**

Common superannuation scams

Phishing scams

In a phishing scam, scammers will impersonate representatives from your super fund, contacting you by phone, email or text message to request personal information, account details or login credentials. They may direct you to fake websites designed to capture your information.

Tip: Always verify communications by contacting your super fund directly using official contact channels.

Issued by ANZ Staff Superannuation (Australia) Pty Limited ABN 92 006 680 664 AFSL 238268 RSEL 0000543 as Trustee for the ANZ Australian Staff Superannuation Scheme ABN 83 810 127 567 (ANZ Staff Super)

Cold calling and unsolicited offers

You might receive unsolicited calls or social media messages offering free reviews of your super account, claiming your fund is underperforming. These scammers use high-pressure tactics to convince you to switch funds or provide personal information.

Tip: Be cautious of unsolicited offers and contact us directly on **1800 000 086** if you have any concerns.

Early access scams

You might receive a phishing email or cold call where the scammer claims they can help you access your super early, often for a fee. They may seek personal information and try to steal your identify. Accessing super early is strictly regulated and unsolicited approaches are suspicious.

Tip: Be cautious of unsolicited offers and contact. If you need to access your super early (for example, you are experiencing financial hardship), please call us on **1800 000 086** for assistance.

Simple steps you can take to reduce the risk of scams

Here are some tips to protect yourself from super-related scams:

- Never share your personal or account information with unknown contacts – we will never ask you for passwords or log in details via email, phone or SMS
- If you're not sure about something, talk to someone you trust before you go ahead. This could be a family member, your accountant or financial advisor, or your fund
- If someone claiming to be from ANZ Staff Super contacts you unexpectedly, call back on our official number **(1800 000 086)** for assistance
- Be suspicious of unsolicited offers or early access schemes – offers that sound too good to be true – especially from cold calls and social media – almost always are
- Don't deal with anyone who isn't licensed- a scammer won't have a valid licence to set up or manage super funds
- Regularly check your super account – log in to Member Online or the Member App
- Use a strong, unique password for your super account
- Take steps to prevent identity theft, including shredding personal documents and being careful of what you share on social media
- Keep up to date with scam alerts via sites like moneysmart.gov.au.

If you think you've been scammed

If you think your ANZ Staff Super account may have been compromised in some way:

1. Report it to us

Call us on **1800 000 086** or email: enquiry@anzstaffsuper.com

2. Change your passwords

Change your passwords and call relevant financial institutions to let them know what's happened.

3. Contact IDCARE

IDCARE is Australia's national identity and cyber support service that helps people who have been impacted by scams, identity theft and cybercrime. They provide free support, practical advice and education and can be reached on **1800 595 160** or idcare.org/contact/get-help.

Version: Protecting_your_super_from_cyber_threats_factsheet_080425