



# Stay safe. Protect your super with Vision Super.

At Vision Super, your security is our priority. Scammers and fraudsters are always looking for ways to steal personal and financial information, but by staying alert and following these simple steps, you can help protect yourselves.

1



## Protect your password—protect your future

A weak password is like leaving your front door open for scammers. Always use a strong, unique password or even better a pass phrase for all your online accounts and never share it with anyone. Enable **multi-factor authentication** (MFA) where possible for extra security. A password manager can also help keep your credentials safe and can generate and store very complex passwords. Learn how to create secure passwords at [cyber.gov.au](https://www.cyber.gov.au).

2



## Think before you click—one mistake could cost you everything

Scammers often pretend to be from banks, or government agencies, sending fake emails and text messages that try to trick you into clicking malicious links. If you receive an unexpected message about your super, do not click any links or open attachments—instead, contact Vision Super directly on **1300 300 820** to verify the request. More tips on avoiding scams can be found at [scamwatch.gov.au](https://www.scamwatch.gov.au).

3



## If something feels wrong, report it—silence helps scammers win

Scammers rely on confusion and hesitation. If you receive a suspicious call, email, or message about your Vision Super account, stop and verify it. Report any potential scams to **Vision Super immediately on 1300 300 820**, or submit a scam report to [scamwatch.gov.au](https://www.scamwatch.gov.au) or the **Australian Cyber Security Centre**.

4



## Protect your data like you protect your money

Your personal and financial information is valuable—keep it safe. Regularly check your Vision Super balance for any unusual activity, **never share your superannuation details over the phone**, and avoid logging into your account on public Wi-Fi. Update your devices and enable **two-factor authentication** where possible. For more financial security advice, visit [moneysmart.gov.au](https://www.moneysmart.gov.au).

5



## Be discreet—scammers only need one small detail to cause major damage

Never discuss your superannuation or financial details in public or on social media. Scammers can use seemingly harmless information—like your birthdate or email address—to steal your identity. If you suspect your personal details have been compromised, **contact Vision Super immediately** and visit [idcare.org](https://www.idcare.org) for expert advice on identity theft protection.

At Vision Super, we are committed to keeping your retirement savings secure. By following these steps, you can help safeguard your super and enjoy peace of mind.