more than money

What to do if you think you've been scammed

If you think you've been targeted by a scam and your personal details or finances are at risk, we're here to help. Being scammed is an overwhelming experience and it can be hard to spot the red flags. Here are some important steps you can take right away to help minimise losses, get support and protect yourself.

Act now ☑

- [ ] **Stop contact with the scammer immediately.** Don't reply to emails, calls, messages or letters from the scammer – and don't make any more payments to them.
- [ ] **Call us immediately.** If you haven't already let us know, call us on **13 22 65** and ask for our Fraud team if you've lost money or have concerns that someone has your banking details. Our specialist team is available any hour of the day to investigate and help you take the right steps.
- [ ] **Change your passwords.** If you think someone has access to your bank account, change your password to a complex one you don't use anywhere else. Make sure you use unique passwords for each of your online accounts (such as your email, banking and superannuation).
- [ ] **Turn on Multi-Factor Authentication (MFA).** Enabling MFA on your online accounts adds extra steps to confirm your identity when you log in, such as your password and a one-time code – so if a criminal has your password, they won't be able to log in without additional information known only by you. Learn more at **nab.com.au/mfa**.
- [ ] **Install trusted anti-virus software.** This helps detect future malicious software (malware) before it can infect your computer. If your devices have already been infected with malware, consider getting help from a technology specialist to make sure your system is virus-free. Visit **nab.com.au/software** to see our anti-virus offers.
- [ ] **Get expert advice from IDCARE.** IDCARE offers a free support service to individuals impacted by scams, cyber incidents and identity theft. NAB customers receive prioritised support by quoting NABPID. Call **1800 595 160** or visit **idcare.org**.
- [ ] **Tell your family and friends.** Let others around you know about the scam, so they can watch out for the red flags or potential follow up scams.
- [ ] **Continue to be alert.** Don't let your guard down, as criminals may re-target you by posing as someone who can help recover your money or personal information.

NAB Secure

more than money

Report the scam ☑

- ☐ **Report it to Australian Cyber Security Centre (ACSC).** When you submit a report through the ACSC's ReportCyber portal, they may refer it to the police for investigation. Visit **cyber.gov.au/report**.
- ☐ **Report it to Scamwatch.** This government agency can use your report to disrupt the scam and warn others. Visit **scamwatch.gov.au**
- ☐ **If you were scammed on social media, report it to the social media site.** If you were involved in a romance scam, you should report it to the online dating platform.

What happens next?

When you make a report to us, our dedicated Fraud Assist team will launch an investigation and try to get your missing funds back – this can take up to 6 – 8 weeks. In many cases this is difficult, as criminals are quick to transfer the funds offshore. If we're unable to retrieve your funds, we'll let you know about the available support options.

Remember, NAB will never ask you to:

- Click on a link in a text message
- Share your personal details or log in to your NAB Internet Banking via a link
- Share your PIN, passwords or security codes – these are for your eyes only
- Transfer your money to a 'safe' account – it's safe where it is
- Tell one of our bankers a story about your transaction that isn't true
- Provide access to your computer or online bank accounts

Find out more

To keep up to date with the latest scams and how to stop, check and protect to reduce your chance of being scammed, visit **nab.com.au/security**

NAB Secure