more than money

Spot the red flags
of bank impersonation scams

Beat the scammers by knowing the scam

Bank impersonation scams involve criminals tricking you into handing over your money or personal details by pretending to be from your bank. Criminals often impersonate trusted sources through fake calls, texts, social media ads or emails. They create a false sense of urgency to pressure you into acting quickly.

Share our tips with your friends and family to help them protect themselves and their money.

Spot the red flags

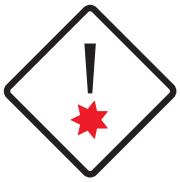
- **Messages and calls that don't use your name or identify the sender or caller.** Criminals often use vague greetings like "Dear Customer" instead of your actual name. If they're pretending to be from your bank, they may avoid mentioning the bank's official name. Your bank will never ask you to share one-time security codes or to transfer money.
- **A sense of urgency.** Criminals may claim your account will be locked or funds lost unless you act immediately. They may ask you to click a link, scan a QR code, or download an attachment. Your bank will never ask you to provide personal or banking details through a link.
- **Fake security risks.** Criminals will often claim to be from your bank's security team or fraud team, stating they have found security issues with your account. They will often pressure you to move your money to a new, so-called 'safe' account they provide, saying it's the only way to protect your funds.
- **Poor spelling and grammar.** This can be a dead giveaway, but criminals are getting better at copying official bank emails, including logos and branding.
- **One-time security code or transfer requests.** Your bank will never ask you to transfer money or share a one-time security code with them.
- **Requests for remote access.** Criminals may try to take control of your device by getting you to download software or click a link. If someone asks you to install anything unexpectedly, it's a red flag.

NAB Secure

more than money

Stop, Check, Protect

to minimise your chance of being scammed



Stop before you act

Always remember that a banker will never ask you to transfer money or share a one-time access code with them. **Stop** and think before you act.

Check before you share

If you're unsure whether a message or call is legitimate, **check** the identity of the person or organisation before sharing any information. You can do this by calling the organisation on their official, publicly-listed number on their website.

Protect if you suspect

Acting quickly if something doesn't feel right can go a long way in helping to **protect** your money and information. If you think you've been scammed or your banking details have been compromised, call us on **13 22 65** and ask for our Fraud team.

Find out more

Visit **nab.com.au/security**

NAB Secure