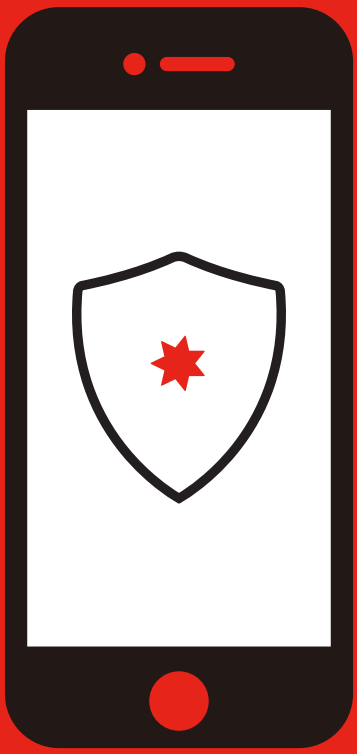
more than money

Don’t get caught off guard

Keeping your money and accounts safe.



NAB Secure

How do you make sure your money and accounts don't fall into the wrong hands? It all starts with securing your banking and personal information – including:

- Debit, Credit and NAB Now Pay Later (NNPL) cards and card information.
- Devices that you use to make payments or hold digital wallets on (e.g. your smartphone, tablet or wearable device).
- Personal Identification Numbers (PINs).
- Phone passcodes and pattern locks.
- Internet Banking passwords.
- All passwords (e.g. for email, devices or online accounts).
- SMS, Security Codes and Verification Codes.

Card and device security

- Don't let anyone else use your card or device where you have a digital wallet set up.
- Do not share your device PIN or PIN pattern with anyone.
- Do not enter your PIN or passcode into a web page opened from an email or SMS link, even if it appears NAB has sent it.
- Regularly check that you still have your card and device.
- Let us know as soon as you realise your card or device or PIN has been lost, stolen or used by someone else.
- Don't use an electronic banking facility such as an ATM, EFTPOS terminal or pay through a website if you think something isn't right – fraudsters can use fake equipment to steal cards or capture PIN details.
- Sign the back of new cards as soon as you get them.
- When your card expires, destroy it by shredding or cutting it up. Make sure you slice through the embedded microchip, magnetic strip and security code (CVV).

Keeping your banking information secure

- Don't share your passwords, PINs, passcodes or pattern locks and don't let anyone watch you enter them.
- We recommend accessing NAB's website by typing nab.com.au into your browser, rather than a link from within an email, SMS, a pop-up window, or from your browser history.
- Make your password/passcode/PIN hard to guess. Don't choose one that's easily identified with you (e.g. your birth date, car registration, telephone number or name).

- Be careful with your passwords, passcodes and PINs. Avoid writing them down or recording them in a device and choose different ones for each of your cards.
- Don't share your Visa Secure one time passcode with anyone, unless you are completing an online purchase that you initiated.
- Please be aware that if anyone else has Touch ID or Face ID set up on your device using their fingerprints or image, they may be able to access your banking accounts and change some of your settings. This could impact your liability for unauthorised transactions.
- Treat your device like your wallet or purse. Keep it close at all times.

If the guidelines above are not followed, you may be liable for any unauthorised transactions.

Liability for losses resulting from unauthorised transactions will be governed by the ePayments Code.

Avoid the red flags

- Treat any unexpected emails, SMS or phone calls with caution. NAB will not send you a link in an unexpected SMS messages. If you do receive an SMS containing a phone number asking you to contact NAB, search nab.com.au to verify that the phone number is legitimate where possible. You should treat any unexpected SMS messages with a link as suspicious. We'll never send you an email or SMS asking you to provide your personal or banking details via a link or attachment nor will we send you a link taking you directly to Internet Banking. If you do receive these kinds of messages claiming to be from 'NAB', don't act on them. Instead, forward the message to phish@nab.com.au and then delete it. Alternatively, you can forward a suspicious SMS to **0476 220 003**.
- When you dispose of any old devices, it's important to erase your personal data, deregister from services, delete your card from any digital wallets or any other Apps, and factory reset your device.
- If you feel like a call might not be genuine, hang up, and call back on an official phone number to verify the call was legitimate (the general NAB number is listed on this brochure, on the back of your cards and online). Never provide personal information or allow the caller to have remote access to your computer on unsolicited calls.
- We'll SMS you one-time passcodes for NAB Internet banking transactions, password resets, to add you card to digital wallets and your requests for Open Banking data

sharing - so its important to keep your phone secure. We might also send you a security code to verify you when you call us. This is the only code we will ask you to provide to us. Make sure you read the SMS in its entirety before sharing that code with us. Otherwise, do not provide the one-time passcode or security codes to anyone calling you even if they say they are from 'NAB'. NAB will never ask you to enter your one-time passcode into a third party website.

- When enrolling your card into a digital wallet we will send you a verification code to complete your enrollment with digital wallet provider. Never share this code with anyone else or enter it into a website.
- If your mobile phone ever stops working, get in touch with your service provider to make sure you haven't been a victim of 'mobile phone porting'. This is where scammers use your information to transfer your phone number to another provider so they can intercept SMS passcodes sent to you.
- When downloading Apps, ensure that they are from official App stores (App Store or Google Play). Never download an App from a link in an email or SMS.
- Regularly check your account statement, Internet banking, and transaction history. If you spot a transaction you don't remember or recognise, let us know straight away.
- Only use trusted devices and trusted Wifi networks to do online banking. Never accept a request to download a program or certificate to your device in order to use a public Wifi network.
- Regularly check your Open Banking data sharing permissions (consents for your banking to be shared with an accredited third party) which can be done through NAB Internet Banking/NAB App. If you spot content you don't remember or recognise, call us straight away. For instructions on how to do this, please visit nab.com.au/openbanking.
- Install up-to-date anti-virus software on your devices to detect and prevent online attacks.
- Report any scams to the Australian Federal Government's Scamwatch service at scamwatch.gov.au.
- Keep up-to-date with online threats and advice at nab.com.au/security, or Australian Cyber Security Centre at cyber.gov.au.

Reduce the risk of identity theft

- Secure your letterbox with a lock to prevent your mail being stolen.
- Let us know straight away if your email, address or contact details change.
- Never give out personal information to people you don't know or trust.
- Don't publish confidential information about yourself on social media, including your full name, date of birth, address or phone number – criminals can use this information to impersonate you.
- Shred documents containing your personal information before throwing them away.

When to notify NAB

If your card, phone or device has been lost or stolen, call us immediately on 1800 033 103 (within Australia) or +61 3 8641 9121 (from overseas) 24 hours, 7 days a week. (Calls from mobile phones are charged at applicable mobile phone rates).

You can also block, unblock and replace your linked personal and business cards by clicking on Cards in the main menu in NAB Internet Banking, the Cards menu in the NAB App or by calling NAB. If you have enrolled your NAB card into a Digital Wallet or digital payments and want to block all digital payments transactions, please call NAB. In addition, you can stop online transaction and contactless payments in your NAB App or online banking, including Digital Wallets. To do so, log into your mobile banking, select cards, select the relevant card, then usage controls and turn off Online Transactions and Contactless Payment controls.

If you believe something isn't right with your account let us know straight away. Call the numbers listed above if your card, phone or device has been lost of stolen. For all other concerns, call the numbers listed on the back of this brochure, especially if:

- Someone finds out your PIN, passcodes or passwords.
- There's an error, unauthorised access or unauthorised transaction on your account.
- You've provided your banking details to an unsolicited email, unknown caller or entered it into any website.

Three ways to minimise the chance of being scammed

Stop, Check, Protect.

Stop

Stop before you act

Pause before you act on that email, text or call – and ask yourself, could this be a scam?

Check

Check before you share

Make sure you verify the contact before sharing any personal information – check the trusted websites, secure Apps or registered business email or phone number.

Protect

Protect if you suspect

Act quickly if something feels wrong – hang up the phone, report the email or text and immediately contact your bank if you've shared your banking details or notice a suspicious transaction.

For more information visit
nab.com.au

For more information call
for personal **13 22 65**
for business **13 10 12**

Help for people with hearing or speech difficulties. Contact us on **13 22 65** through the National Relay Service.