more than money

Staying safe from cyber threats and scams

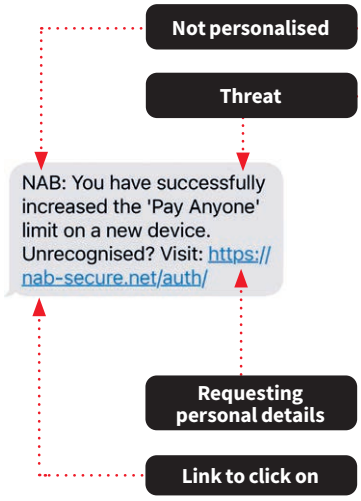
Tips from NAB's Security Team

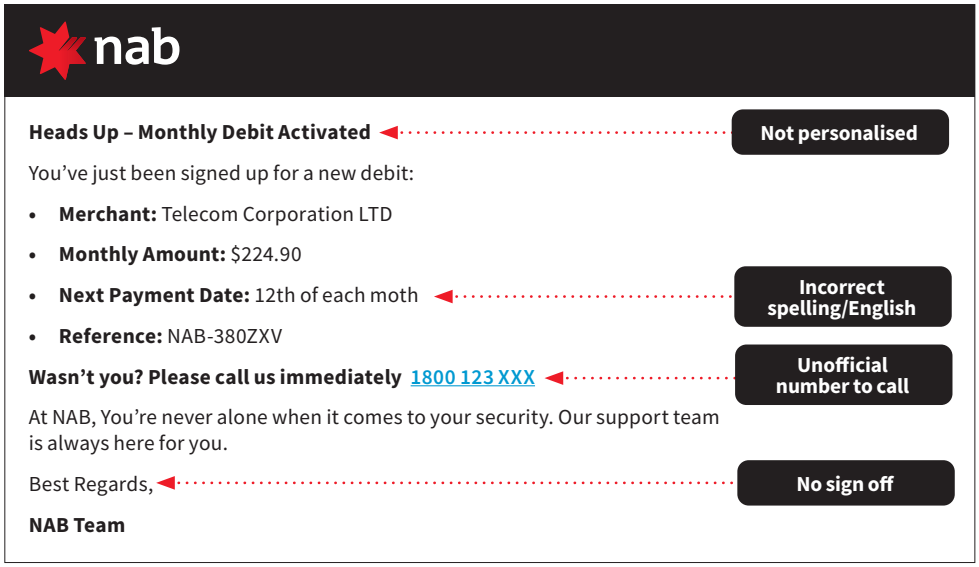
We're all doing more online than ever before. That's why knowing how to recognise the red flags and ways to protect yourself is vital. Here are NAB's top tips for staying safe online.

Learn how to spot the red flags!

Criminals will do their best to make fraudulent emails and text messages look legitimate. Their aim is to trick you into visiting fake websites and providing your personal information. These examples have some signs to help you recognise a suspicious message.

If you receive a suspicious email or text message, do not click on the links or attachments. To visit NAB's website, always type **nab.com.au** into your Internet browser, or use the NAB App. Not sure if a message is legitimate? Contact the organisation directly to check.





Stop

If you receive a suspicious message or call, stop to consider, could this be a scam? Criminal often use urgency to convince you the danger is real.

Check

With the person or organisation directly to verify if the request was legitimate. Criminals change tactics all the time, so it's important to stay up to date with the latest information. Visit:

- NAB Security Hub: **nab.com.au/security**
- The Federal Government's Australian Cyber Security Centre: **cyber.gov.au**
- The Federal Government's Scamwatch service: **scamwatch.gov.au**

Protect

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, NAB's number is on the back of your card' after transaction.

NAB Secure

Type of scams

Phone and remote access scams

Criminals may call you, impersonating your bank, telco or computer company and tell you there's an issue with your computer, banking or phone. They might ask you to download a program that gives them remote access to your device, so they can 'fix' the issue.

- Treat any unsolicited phone calls with caution. If you're unsure about the legitimacy of any call, hang up, and call back on an official phone number to verify its legitimacy.
- Never provide personal or banking information on unsolicited calls, or download special software to give someone access to your device.
- Ensure you carefully read any SMS codes sent to you. If it states, "Don't share this code with anyone, including NAB", do not disclose this code to anyone.

Investment scams

Investment scams target your personal wealth by convincing you to invest in fake schemes and companies. They may appear to be offers from legitimate financial institutions promising high returns with low risk.

- Never provide your NAB Internet Banking login details to a third party.
- Be wary of any unsolicited contact from investment schemes or 'free' advice that make big claims but provide minimal details.
- The opportunity may appear to be endorsed by celebrities or high profile people on social media. Check the legitimacy before committing.
- If it sounds too good to be true, it probably is. Check the **Investor Alert list** on **moneysmart.gov.au** for known scams.

Romance scams

Romance scammers take advantage of people looking to find romantic partners by creating fake profiles on dating sites and apps. Criminals gain trust, then use goodwill to ask for money or gifts.

- Google the person's name to see if they've been reported on any scam sites.
- Do a reverse Google image search of any photos they've sent, as they may already be on scam reporting sites.
- If your friend or relative has already sent money, they should report it to the police, ReportCyber and their bank.

Buying and selling scams

Purchasing scams take place on common ecommerce platforms used by genuine people, such as eBay, Gumtree, Facebook Marketplace and Carsales.

Be wary of buyers or sellers who, ask for identification documents, request to use payment methods such as gift cards, money wiring services, cryptocurrencies or PayPal's 'Family and Friends' method.

- Use secure payment options that come with protections, such as PayPal (not PayPal Family and Friends) or a credit card.
- Where possible, do some research on the buyer or seller and look for reviews.
- If possible, meet in person to exchange the item and cash.

Some ways to stay secure online

Use strong, complex passwords and a password manager tool

Use a unique, complex password for each account and keep them to yourself. Consider using passphrases, which are a combination of multiple random words containing upper and lower case letters, numbers and special characters. These are much harder for others to guess. You can save them in a password manager tool so you don't have to remember them too! Learn more about good password hygiene on **nab.com.au/passwordsecurity**

Social media scams

Criminals will often use sites like Facebook or LinkedIn to gather information about people and companies. Consider setting your profiles to 'private', and be mindful of what you're sharing.

Use Multi-factor Authentication (MFA)

Also known as two-factor authentication (2FA), turn on MFA wherever possible to add an extra layer of security on your online accounts and help prevent unauthorised access. Learn how to turn on MFA at **nab.com.au/mfa.**

Update software regularly

Using out of date software and operating systems can leave your devices vulnerable. Ensure you always have the latest anti-virus software and security patches installed. Turn on automatic updates so you never miss the latest software updates.

Back up your data regularly

Your data is valuable, so make regular back-ups of your data, and store them somewhere safe. Test your back-ups regularly to ensure they'll work if you need them.

Report it!

Report all suspicious NAB-branded emails and SMS to phish@nab.com.au or text 0476 220 003.

Stay up to date

Visit NAB's Security Hub at **nab.com.au/security** to see the latest security alerts and practical advice on protecting yourself online.