more than money

Staying safe from cyber threats and scams

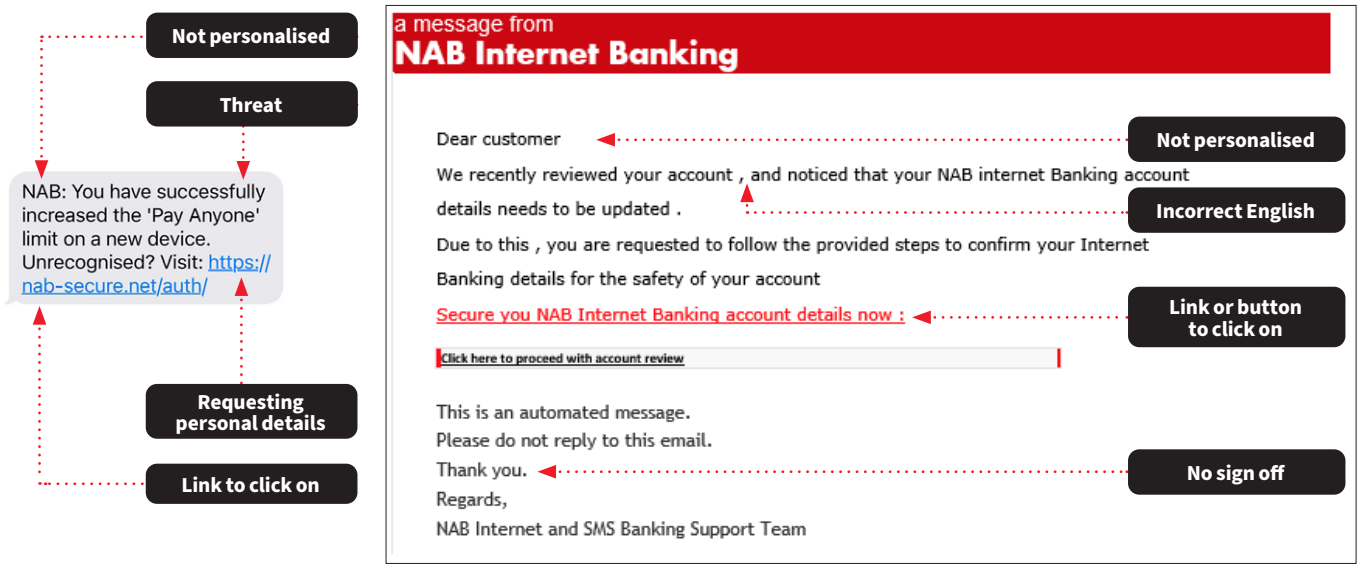
Tips from NAB's Security Team

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.

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.



Report it!

If there's been suspicious activity or fraud on your accounts, or if you've been impacted by cybercrime, please report it immediately to:

- Your bank
- Report all suspicious NAB Branded Emails and SMS to phish@nab.com.au or text 0476 220 003
- The Australian Cyber Security Centre (ACSC): **cyber.gov.au/report**

Stay up-to-date

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**

NAB Secure

Type of scams

Phone and remote access scams

Criminals may call you, impersonating a bank, telco or computer company and tell you there's an issue with your computer, banking or phone. They'll ask you to download a program that gives them remote access to your computer, so they can 'fix' the issue. If you do this, they can access all the information on your computer. You should never give an unsolicited caller access to your computer. These scam calls aim to pressure you into providing your personal or banking information.

- 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 the call was legitimate.
- Never provide personal or banking information on unsolicited calls.
- Ensure you carefully read any SMS codes sent to you. If it states "Don't share this code with anyone, including NAB. Your NAB secret code is xxxxx." or "Don't share this code with anyone, including NAB. Secret code for Password Reset is xxxxx ", do not disclose this code to anyone.
- Check the **moneysmart.gov.au** list of companies you should avoid.

Investment scams

Investment scams target your personal wealth by convincing you to invest in fake schemes and companies.

They are widespread and can take many different forms.

- 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 of high return and low risk but provide minimal details.
- If in doubt, seek a second opinion and ask 'is this for real'?

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.

Romance scams

Romance scammers take advantage of people looking find romantic partners by creating fake profiles on dating sites and apps. Criminals gain the victims trust, then using 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 Multi-factor Authentication (MFA) or 2FA

Multi-factor authentication (MFA), sometimes known as 'two factor authentication' or '2FA', provides an extra layer of security for online accounts such as banking and email. When using MFA, in addition to your password, a second piece of information is required to access your account, such as an SMS code or a security token. This can prevent unauthorised access to your accounts, even if someone knows your password. Learn how to turn on multi-factor authentication for your accounts at **nab.com.au/mfa.**

Update software

Using out of date software and operating systems can leave your computer or phone vulnerable. Update your computer software regularly – and make sure you always have the latest anti-virus software and security patches installed. Turning on automatic updates means you'll never miss the latest software updates.

Use a password manager

Your passwords are the keys to everything you do online. Use a different password for each account, keep them to yourself, and make them strong – use numbers and symbols in addition to letters. 'Password Manager' software can help you create and store passwords securely.

Back up your data

Your data is valuable, so make sure you 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.

Stop: If you receive a suspicious message or call, stop to consider, could this be a scam?

Check: with the person or organisation directly to verify if the request was legitimate

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.