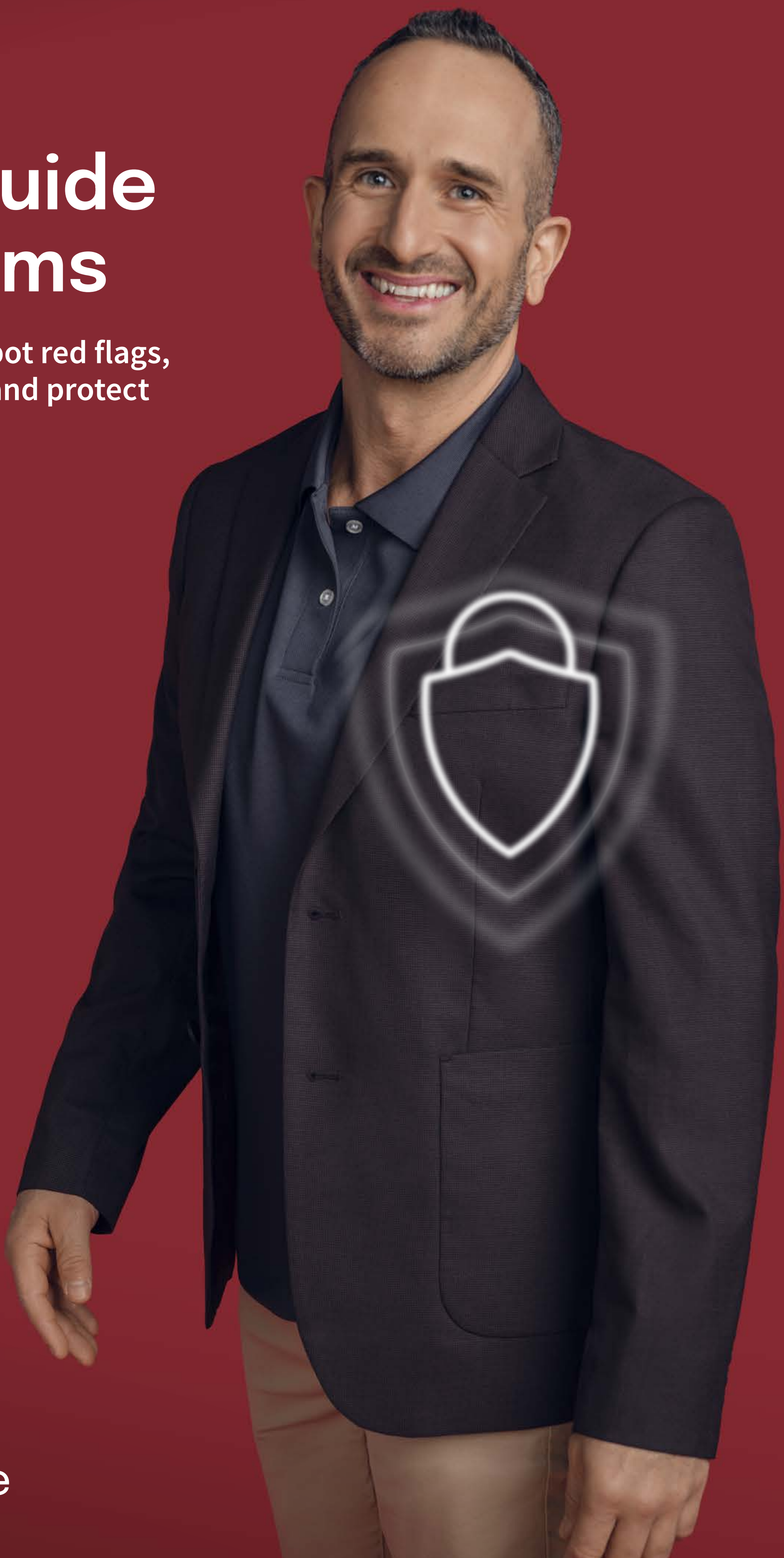
more
than
money

Easy Guide to Scams

Helping you to spot red flags, stay safe online and protect your money.



NAB Secure

Contents

Hello

This is a short guide providing information on scams to help you protect yourself and your money.

This is a short guide

For more details and support on scams:

- Go to our website nab.com.au/security
- Call us on:
  - **13 22 65** and ask for the Fraud team
- Contact us via chat.

National Relay Service

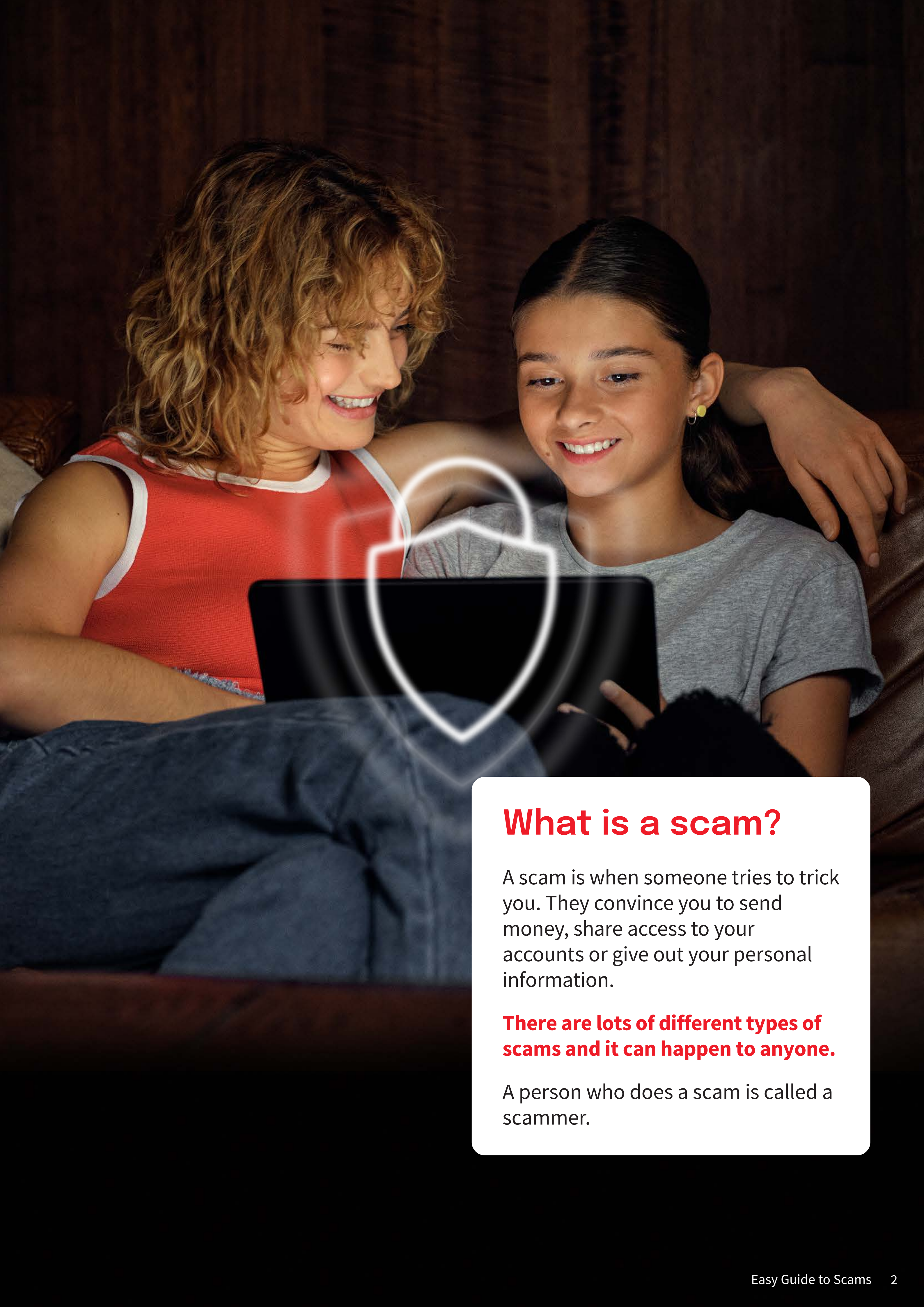
If you need help to speak or listen

You can use the National Relay Service or NRS to call us. If require assistance you can contact their helpdesk on **1800 555 660**.

To find out more ways to contact NRS, visit https://www.accesshub.gov.au/about-the-nrs/register-for-the-nrs.

If you do not speak English

You can call us and say **I need an Interpreter.** We will get someone to help with your banking.



What is a scam?

A scam is when someone tries to trick you. They convince you to send money, share access to your accounts or give out your personal information.

There are lots of different types of scams and it can happen to anyone.

A person who does a scam is called a scammer.

Scams are becoming harder to spot

Scams can happen to anyone. Scammers create situations that seem real to get you to share your personal information, provide account access or send money. Scammers pretend to be businesses, banks, government agencies and everyday people, but they are fake.

People that run scams are always looking for new ways to make you share personal information, provide account access or send money. They are using new technology to create scams that look very real.

Three easy steps to avoid scams.

Stop

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

Check

Contact the person or organisation before you share any information or take any action. Always check the business email or phone number, by checking the real companies website. Ask them if the message or call was real. Scams change often, so it is important to stay informed. 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

If something does not feel right, take steps to protect. Hang up the phone, report the email or text message. Contact your bank straight away if you shared your banking details or see a strange transaction.

change grey colour to a diff background

Scam types

Most common scam types

According to the Australian Competition and Consumer Commission (ACCC) Scamwatch, there are 2 main types of scams:

Mass market scams
These scams are sent to lots of people at once. They often look like emails from your bank or pop-up messages saying your computer has a virus. The goal is to trick people into giving away money or personal information, such as their driver's licence or passport details.

Relationship scams
Relationship scams happen when a scammer takes time to gain your trust. This can include romance scams, investment scams, or pretending to be someone they are not. Once they have your trust, they may ask for money or personal information. People who experience these scams can lose money and may feel sad, worried, or embarrassed. They may also not believe they have been scammed.

A few of the most common types of scams are:

Phishing scams:
fake text messages and emails trying to steal your information.

Business scams:
asking you to pay fake bills.

Relationship scams:
pretending to care about you to get money.

Scambling (Scam Gambling):
uses fake online betting or gambling websites to take your money.

Investment scams:
pretending to offer investment opportunities, promising easy and quick money.

Buying and selling scams:
tricking you when you buying or selling items online.

Remote access scams:
asking to access your computer or phone.

Phone scams:
pretending to be someone you should trust and trying to make you act quickly.

Scambling or Scam Gambling

Scambling is a scam that uses fake online betting or gambling websites. These websites may promise easy wins, free credits, or rewards for inviting friends. People may find them through social media ads or people they know. The websites are made to trick people into sending money or sharing personal information.

Scambling can also be called 'Ding Ding' and 'Gammon Ding Ding'.

The top red flags to watch out for:

- You found the website through social media or someone you know
- You're asked to send money to a PayID that keeps changing
- It promises very large bonuses, free credits or rewards
- The website isn't well known or trusted
- It offers rewards for getting family and friends to join

If something seems too good to be true, it could be a scam.

Tool tip:

Before you play, ask: is this game allowed in Australia?

You can check by visiting: acma.gov.au/check-if-gambling-operator-legal

If you need to speak to us:

How to contact us

By phone: Call us on **13 22 65** and ask for our Fraud team

Call us on our First Nations Support Line on **1800 966 100**

Common red flags

There are different scam types, but common things to watch out for. There may be one or more of these that could warn you it's a scam:

1. **Unexpected contact:** You get an email, text message, phone call or contact through social media and messaging applications, that you were not expecting, from someone you don't know.

2. **Pressured to act fast:** You are told to make a quick decision without enough time to think or to ask someone you trust for help.

3. **Keep it secret:** Someone tells you, don't talk about it with family, friends or other people you trust.

4. **Requests for usernames, passwords or PINs:** Someone asks for your private account details that should only be known by you.

5. **Requests to install software:** Someone asks you to download an app or install a program on your device, that could give them access to your device or information.

6. **Requests for ID (identity) documents:** Someone asks for identity documents, such as drivers licence or passport, when there is no reason to provide them.

7. **Unusual payment requests:** You are asked to pay in a different way, such as with gift cards, cryptocurrency, money transfers. You are asked to accept money and then send it to someone else.

8. **Seems too good to be true:** You are offered something that sounds amazing, is very easy to get, or much better than you would expect.

Remember

- NAB will never ask for your banking password or PINs.
- NAB will never ask you to transfer money to a "safe account".
- Always check payment details yourself.

What to do if you believe you have been scammed

If you think you have been scammed or are speaking with a scammer. **Stop speaking** to them and **contact us**.

Here are some simple steps to follow:

Stop all communication.

Contact NAB (details can be found on the back page).

Change passwords (if they've been shared).

Turn on multi-factor authentication on all types of accounts.

Report the scam to Scamwatch.

Monitor your accounts.

If you've sent money or shared personal or banking information call 13 22 65 and ask for the Fraud team or call us via your NAB app.

Report the scam to Scamwatch on **scamwatch.gov.au**.

Tips on protecting your password

You use passwords to access your bank accounts, social media, email and more every day. Passwords are the keys to our online identity. That's why protecting them is so important. Creating a strong password is the first step to protecting yourself online.

To help stay safe online, follow these password tips.

1. Make your passwords strong

Strong passwords have a minimum of 12-14 characters and use a mix of:

- uppercase and lowercase letters
- numbers
- special characters like !, &, and *.

For example, the passphrase 'CloudHandWashJump7' is 17 characters long and contains different characters. This is more complex than the average password.

2. Make passwords hard to guess

Could someone who knows you guess your passwords? For this reason, it's best to avoid using personal information such as your children, partner or pets name as your password.

So it's best to avoid using:

- dictionary words
- repeated characters like zzzz
- personal information

3. Store passwords safely

Writing passwords down is never recommended. You could lose them, or someone else could see them and use them.

There are programs and apps known as password managers that will store all your passwords in a secure vault.

A password manager only needs one strong password to access it and has extremely strong protection to make sure that only you can access it.

4. Create new, unique passwords

If you need to reset a password, don't just change one part of it, change the whole password.

If your original exposed password had a '1' at the end, an attacker would likely try '2' next. That's why it's important to change the whole password.

5. Don't share passwords, ever.

Never share your password with someone, not even with someone you trust. This includes family and friends.

Regardless of whom you share it with, once you share your passwords you lose control of how it's stored or how and when it's used.

6. Use different passwords for each of your online accounts

Use a different password for each account. If someone gets one of your passwords, they will not be able to access your other accounts.

Make every password unique. This helps protect your accounts from criminals who try to use stolen passwords to log in to other accounts.

Case Study

How NAB can help support during a scam.

David's Story

David is 56 years old. He has a wife, 2 young kids and works full time.

What happened to David

David receives an email that looks like it is from his bank. The email says there has been unusual activity on his account and asks him to call a phone number immediately. David is worried and calls the number.

A person answers and says they are from the bank's security team. They tell David his money is at risk and pressure him to act quickly.

The person on the phone says they can help and asks David to:

- Share his Internet Banking password
- Read out a security code sent to his phone

David believes he is speaking to the bank and follows the instructions.

Later, he discovers the phone number isn't NAB and he notices transfers totalling $10,000 from his account which he hasn't made.

How did NAB support David

David calls NAB's Fraud team straight away, told them what happened and said he did not make those transfers. The Fraud team quickly created a case and started the process to try get the money back. David got a call from NAB and was told that NAB was able to get the money back into his account.

What could David had done to protect his accounts:

✓ Stop and think "Could this be a scam?" before acting

✓ Contact the bank on the real phone number from the bank's official website or the back of his card

✓ Never share passwords or PINs with anyone

✓ Be cautious if anyone pressures you to act urgently.

Key Point:

In this case, NAB was able to get David's money back, but that's not always the case.

If you receive an unexpected text message or email asking you to call a phone number, always check the contact details first before responding. Never share passwords, or PINs with anyone.

Useful resources

For more useful information on scams and how to keep you and your accounts safe, visit one or more of the following:

For general Scam information and how NAB can support, visit NAB's website on nab.com.au/security

If you are a First Nations person, visit the Financial Rights Centre on financialrights.org.au.

For general Scam information, updates and ways to keep your money safe, visit Scamwatch on scamwatch.gov.au

For help when it comes to making informed choices around money, visit Moneysmart on moneysmart.gov.au.

If you believe you have had your personal information stolen, visit I.D Care on idcare.org

For advice on how to keep yourself and accounts safe from threats, visit the Federal Government's Australian Cyber Security Centre on cyber.gov.au

Contact us

If you need help

If you cannot find the information you need on our website, or having difficulty here are some ways we can help.

Call us on:

13 22 65 ask for our Fraud team.

First Nations Customer Support Line: 1800 966 100

If you need help to speak or listen

You can use the National Relay Service or NRS to call us. If require assistance you can contact their helpdesk on **1800 555 660**.

To find out more ways to contact NRS, visit https://www.accesshub.gov.au/about-the-nrs/register-for-the-nrs.

If you do not speak English

You can call us and say **I need an Interpreter.** We will get someone to help with your banking.

Live chat with us on our website

Click the chat button on the bottom right side on our website.

Visit a NAB branch

You can find your nearest branch, by looking at our website nab.com.au/branch.

On demand AUSLAN interpreter support available in branch.

Stop

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

Check

Contact the person or organisation before you share any information or take any action. Always check the business email or phone number, by checking the real companies website. Ask them if the message or call was real. Scams change often, so it is important to stay informed. 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

If something does not feel right, take steps to protect. Hang up the phone, report the email or text message. Contact your bank straight away if you shared your banking details or see a strange transaction.