



# How to be safe from scams

National Australia Bank



Easy English

## Hard words



This book has some hard words.

The first time we write a hard word

- the word is in **blue**
- we write what the hard word means.

## You can get help with this book



You can get someone to help you

- read this book
- know what this book is about
- find more information.



We will write contact information at the end of this book.

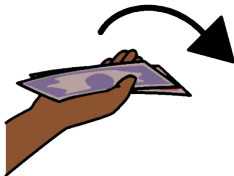
## About this book



This book is from National Australia Bank or NAB.



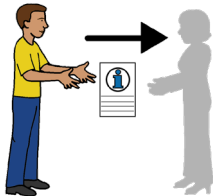
This book is about how to be safe from **scams**.



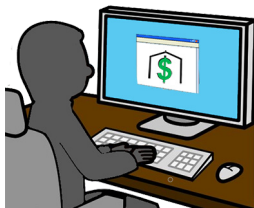
A scam is when someone tries to make you

- give away your money

or



- share your personal details
  - for example, your name or birthday.



A person who does a scam is called a **scammer**.

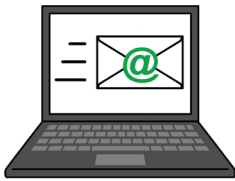


Scams can happen to anyone.



We want to help you be safe from scams.

## Be careful of strange messages



A strange message could be

- an email



- a text message.



The strange message might ask you to give personal information.

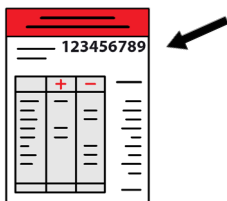


For example, your

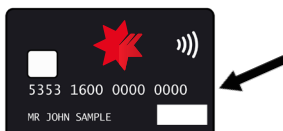
- address



- school



- bank account number

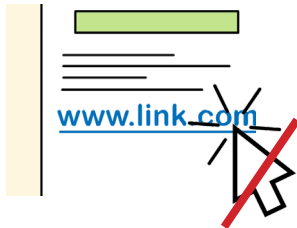


- credit card number.

## If you get a strange message



The strange message might have a link or attachment that is fake.



Do **not** click on the link or open the attachment.



You should delete the strange message.



The strange message could also look like it is from someone you know.



You should check with the person you know to see if the message is real **or** fake.

You could ask someone you trust to help you.



## If you get a strange phone call

Hang up if you think a phone call is strange.



If you think it is a strange call do **not** give your personal information.

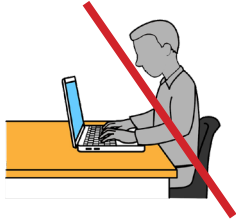


You can call the organisation to check if it was a real call.

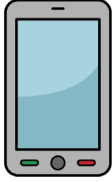
For example, you can call us if the person said they were from NAB.



The scammer might pretend to be an expert who can help you.



If you think it is a strange call do **not** let the person change anything on your **device**.

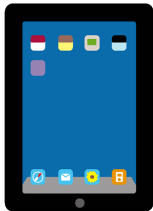


A device could be

- a smart phone



- a computer



- a tablet.

## Romance or dating scams

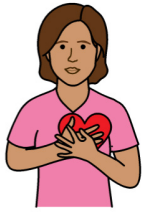
A **romance or dating scam** is when a scammer



- wants to have a relationship with you



- wants you to trust them very quickly.

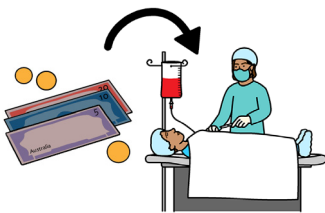


The scammer might

- say they are in love with you very quickly

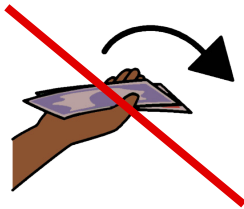


- start a relationship with you to get money or gifts



- pretend they need money to fix a problem
  - For example, a health problem.

## If you think it is a romance or dating scam

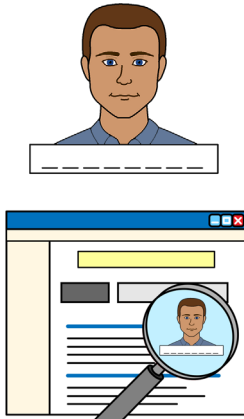


Do **not** send any money to the person even if they promise to return it.

If you are worried you can ask someone you trust to help you.



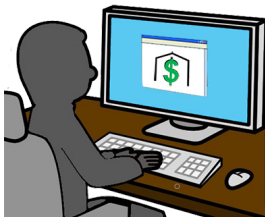
You can do an internet search to see if the person has done a scam before.



You can search the internet with

- their name
- their photos.

## Impersonation or spoofing scams

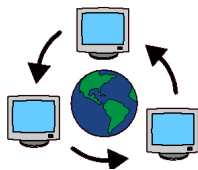


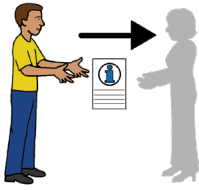
An **impersonation or spoofing scam** is when a scammer pretends to be from a real company.



For example, from

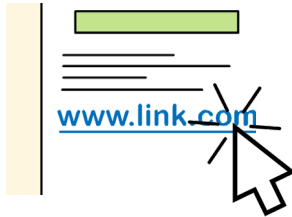
- your bank
- your internet provider
- the government.





The scammer might

- ask for personal information
- tell you to send them money quickly

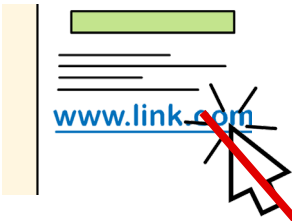


- tell you to click on a link



- say they will fix a problem on your device.

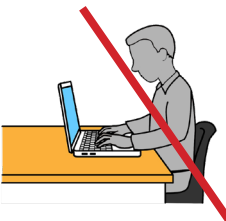
### If you think it is an impersonation or spoofing scam



Do **not** click on any links or attachments.



Do **not** give your personal information.



Do **not** let the person change anything on your device.



You can call the company to check if it was a real call.

For example, you can call us if the person said they were from NAB.



We will **never** send you a message with a link for you to

- give personal information



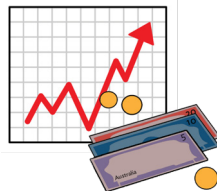
- log in to your bank account.

## Investment scams



An **investment scam** is when the scammer

- wants you to give them money now

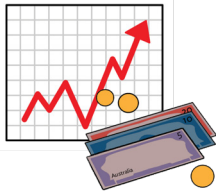


- tells you that you will get more money back in the future.

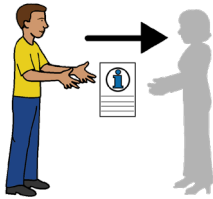


A scammer might

- pretend to have advice about your money

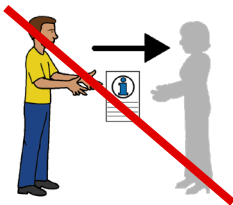


- ask you for money for an investment.

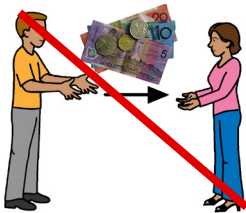


The person might ask you for personal information.

## If you think it is an investment scam



Do **not** give your personal information to anyone.



Do **not** pay any money if you are worried.



You should tell us if you gave money to an investment scam.

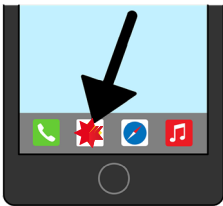
## If you give money for any scam



If you think it is a scam you should tell

- the police
- NAB
- your friends and family.

## Be careful when you use internet banking



**Internet banking** means when you go into your bank account

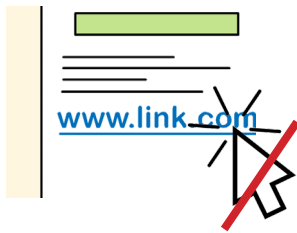
- on our website
- in the NAB app.

Only use a device that you think is safe when you use internet banking.

Do **not** download a new program or app if you are using public Wi-Fi.

## Be careful when you download an app

Only download an app from **app stores**.



App stores are

- Apple App Store
- Google Play.

You should **never** download an app from a link in an email or text message.

## What to do if your phone stops working



Contact your mobile phone provider.



Your mobile phone provider can check if your phone stopped working because of a scam.

## Sometimes we need to check who you are



We might need to check who you are when

- you call us



- you use internet banking.



We will send you a **passcode**.

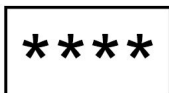
A passcode

- is a text message with numbers



- only works once

- **must** be used straight away.



You **must** enter the numbers when you are asked for the passcode.



Do **not** tell anyone the passcode even if they say they are from NAB.

## Check your bank statements



You should check your bank statements and look for any strange payments.

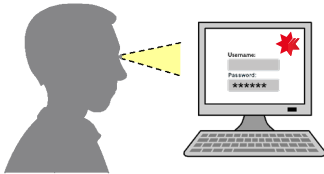


Tell us if you see a strange payment.

## When should you talk to us?



Talk to us if you think something is wrong.

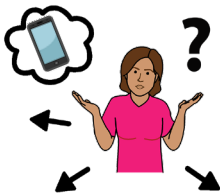


You should talk to us if

- someone finds out your PIN or password



- someone else has used your account



- your mobile phone is lost or stolen



- you gave your personal information to someone else.





## More information

For more information contact NAB.



Call 13 22 65



Website [nab.com.au](http://nab.com.au)

## You can read the full document on our website

The document is called

### **Don't get caught off guard.**



Website [nab.com.au/securitytips](http://nab.com.au/securitytips)

## If you get a strange message

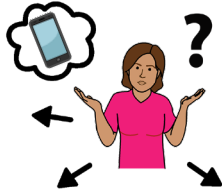


You can copy and paste the message

- in an email to [phish@nab.com.au](mailto:phish@nab.com.au)



- in a text message to 0476 220 003.



## If your card or device has been lost or stolen



If you are in Australia



Call 1800 033 103



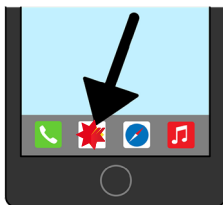
If you are overseas



Call +61 3 8641 9121



You can call any time of day or night.



You can also block or replace your card with NAB internet banking or the NAB app.



## If you want to find out about a scam

You can read more information about scams on the Scamwatch website.



Website [scamwatch.gov.au](http://scamwatch.gov.au)

If you do not speak English and need to report a scam



Call 13 22 65



Press 3

Press 1

When someone answers you can say  
I need an interpreter.



We will get someone to help you.



If you need help to speak or listen

You can use the National Relay Service or NRS to call us.

You must sign up to the NRS to use the service.



Call 1800 555 660



Give the relay officer the NAB number you want to call.



You can find more ways to contact the NRS on their website.



Website

[accesshub.gov.au/about-the-nrs/nrs-call-numbers-and-links](https://www.accesshub.gov.au/about-the-nrs/nrs-call-numbers-and-links)

© 2023. National Australia Bank Limited 12 004 044 937 AFSL and Australian Credit Licence 230686. All rights reserved, except as permitted under the Australian Copyright Act 1968. Text, images and information incorporated in this Easy English publication were created by Scope (Aust) Ltd at [scopeaust.org.au](https://scopeaust.org.au) and Tobii Dynavox.

National Australia Bank has undertaken reasonable enquiries to identify where material or content is owned by third parties and to secure permission for its use and reproduction. Permission may need to be obtained from third parties to use, reproduce or modify this material. The Picture Communication Symbols ©1981–2023 by Tobii Dynavox. All Rights Reserved Worldwide. Used with permission. Boardmaker™ is a trademark of Tobii Dynavox.

This document is complementary to and does not replace the NAB Security Tips Brochure, which is available at [nab.com.au/securitytips](https://nab.com.au/securitytips)

