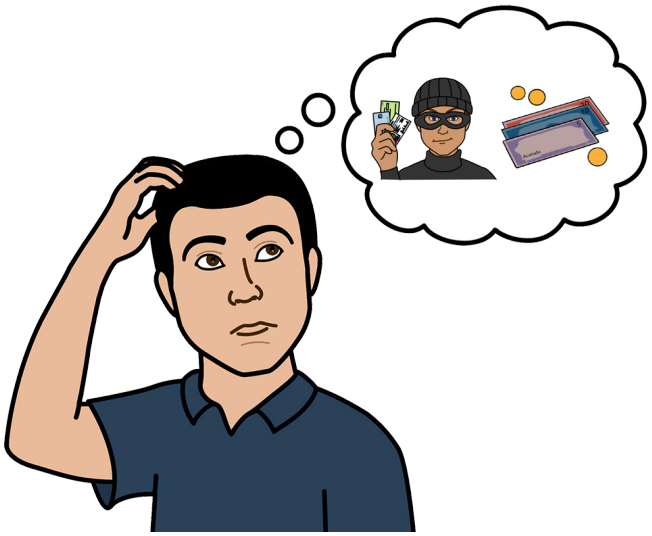
Commonwealth Bank



Scams and fraud

Commonwealth 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.

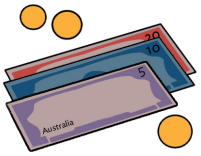
About this book

Commonwealth Bank

This book is written by Commonwealth Bank.

This book is about **scams and fraud**.

Scams and fraud are when someone tries to trick you to give away your



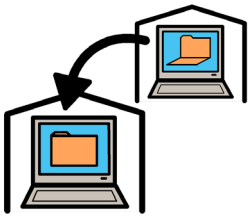
- money

or

- personal details.

Types of scams and fraud

Remote access scams

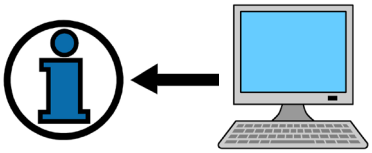


The scammer might

- ask for remote access to your device

- pretend to be an expert who can fix your computer

- put **malware** on your device.

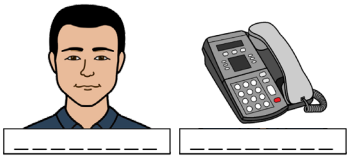


Malware means unsafe software programs that can take your personal information from your computer.

Employment scams

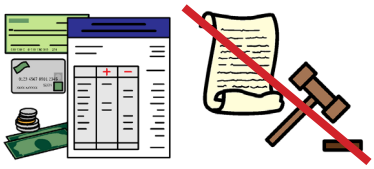
The scammer might

- say they have a job for you



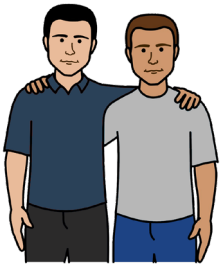
- ask for your personal details

- ask for payment for a starter kit



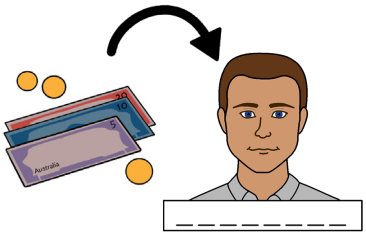
- try to move money through your bank account in a way that is **against** the law.

Relationship and dating scams

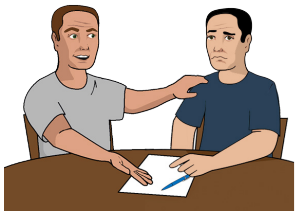


A scammer might

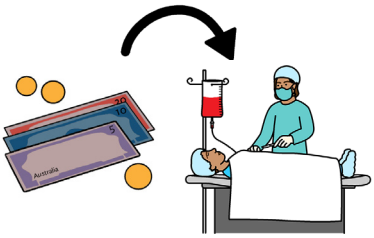
- start a relationship with you to get money or gifts



- make you put money or assets into their name



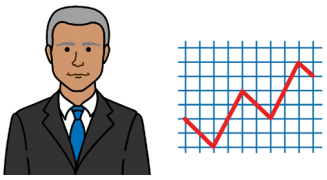
- ask to be in your will



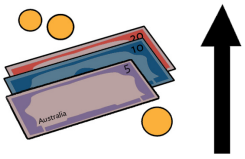
- pretend they need money to fix a problem

  For example, a health problem.

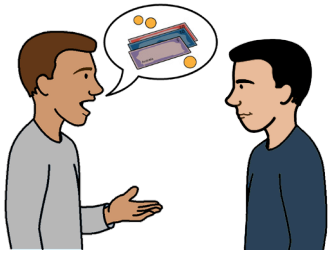
Investment scams



A scammer might pretend to be an **investment** expert.



Investment means you put your money into something to get more back on it in the future.



A scammer might

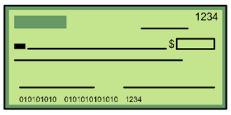
- pretend to have advice about your money
- ask to have your money for an investment.

Online shopping scams

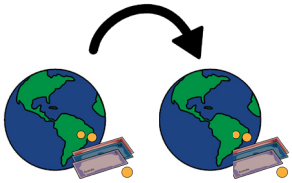
A scammer might

- pretend to sell you something online

- make a fake online shopping website



- ask for unusual payment methods including
  - money order or wire transfer



  - international funds transfer.

Workplace email scams

The scammer might

- get into an email account from your work

- pretend to be someone from your work

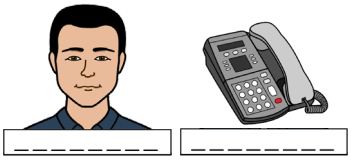
- steal money from your work.

Email or SMS scams

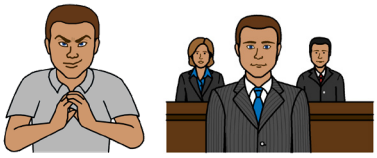
A scammer might

- contact you on email or SMS

- send you a link to a fake website



- get your personal details on a fake website



- pretend to be someone you should trust.

  For example

  – a government organisation

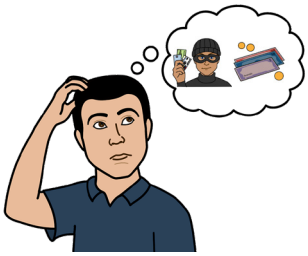
  – a bank.

Who can be a victim?

Anyone can be a **victim** of scams and fraud.

A victim is the person who gets scammed.

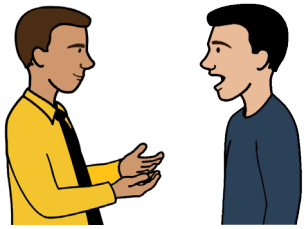
Are you a victim?



It can be hard to know if you are a victim of scams and fraud.

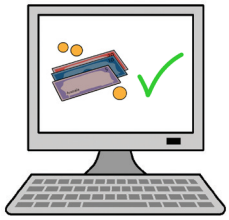
There are **signs** of scams and fraud to look for.

Signs are clues that could mean you are a victim of scams and fraud.



We can help you look for signs of scams and fraud and show you where to get help.

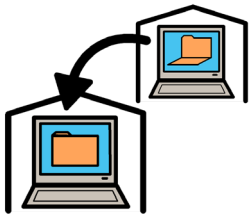
Signs of scams and fraud



You might become a victim of scams and fraud if

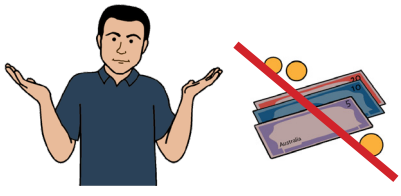
- you get an offer online to make easy money that sounds too good to be true

- someone you do **not** know tries to call or email you

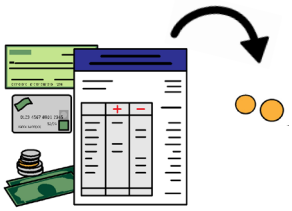


- someone you do **not** know asks for remote access to your computer

- you feel bullied or rushed to give money or information



- money has moved from your account and you do **not** know why.



Scammers might try to take small amounts such as 1 dollar to test your account.

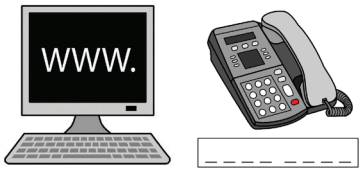
Tips to stay safe

1 Hang up the phone straight away if you think it is a scam

Scammers might call and pretend to be from a bank or government organisation.

2 Do not click on links sent to you in an SMS

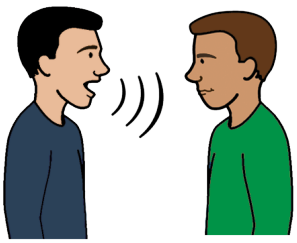
Scammers might send you unsafe links to take your personal details.



3 Check for real contact information

A scammer might give you contact information that looks like it is from a real organisation.

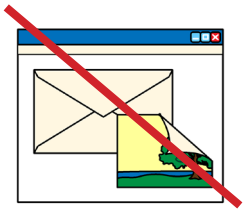
Find the real organisation website to see if the information is correct and **not** a scam.



4 Talk to someone you trust

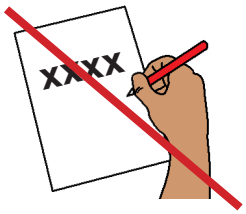
You can ask someone you know and trust to help you work out if it is a scam.

More tips to stay safe



Do **not**

- open attachments from people or organisations you do **not** know

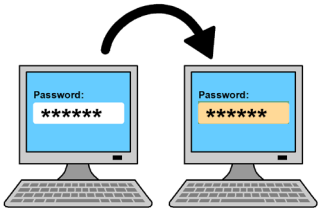


- write down or share passwords, PINs or personal information

To stay safe, make sure you

- use up to date virus software

- tap or insert your card at the shops.



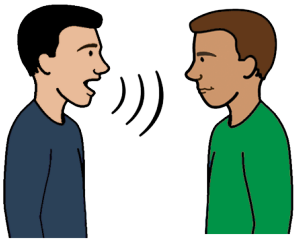
If a scam has happened

- Change your PINs and passwords

- CommBank customers should call 13 22 21 straight away.

More help

It is a good idea to get advice before you make changes to your money.



You might talk to an expert or support person.

You can see full information on our website commbank.com.au/support/security/sms-phishing-scams.html

Get help for scams and fraud

Contact IDCARE for more help.

Call

1300 432 273

Website

idcare.org

Go to the Scamwatch website

scamwatch.gov.au

More information

For more information contact Commonwealth Bank.

Call us 13 22 21

6 am to 10 pm

Website

commbank.com.au

National Relay Service

If you are deaf or have a hearing or speech impairment you can use the National Relay Service.

Website

nrschat.nrscall.gov.au/nrs/internetrelay

Call 1300 555 727

Commonwealth Bank

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

© Commonwealth Bank of Australia 2020. ABN 48 123 123 124. All rights reserved, except as permitted under the Australian Copyright Act 1968. Text, images and information incorporated in this Easy English publication created by Scope (Aust) Ltd at scopeaust.org.au and Tobii Dynavox.

Commonwealth Bank of Australia 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 ©1981–2020 by Tobii Dynavox. All Rights Reserved Worldwide. Used with permission. Boardmaker™ is a trademark of Tobii Dynavox.

Commonwealth Bank of Australia.

Commonwealth Bank

scope