Australian Banking Association

Staying safe from scams

An Easy Read guide

How to use this guide

The Australian Banking Association (ABA) wrote this guide. When you see the word ‘we’, it means the ABA.

We wrote this guide in an easy to read way.

We use pictures to explain some ideas.

Not bold

Bold

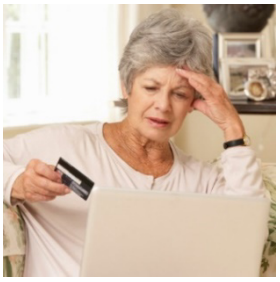
We have written some words in **bold**.

This means the letters are thicker and darker.

We explain what these words mean.

You can ask for help to read this guide.
A friend, family member or support person may be able to help you.

What is a scammer?



We call it a **scam** when someone tries to:

- trick you
- take your money
- take your personal information.

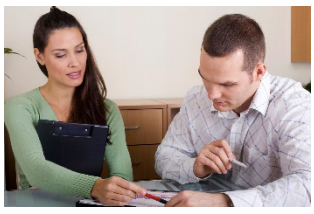
A **scammer** is a person who does a scam.

Scammers can do scams in different ways.

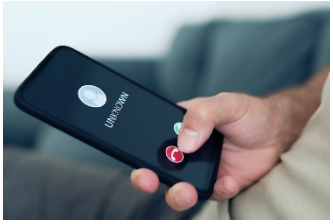
Scams can happen to anyone.

If you're not sure you're being scammed:

- don't send money or give information



- ask for help from someone you trust



- hang up the phone or delete the message.

They might send you an email that looks real.

But it is fake.

They might send you a text message that looks real.

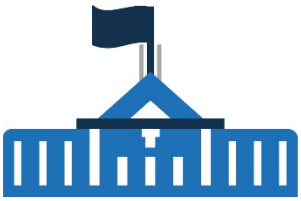
But it is fake.

They might call you from a fake phone number.

They might pretend to be someone you trust, like:

- your bank

- a health service



- the government, like the Tax Office

- other organisations, like Telstra.

Scammers do these things to get your:

- personal information
- money.

Your bank won't ask you for your bank details like:

- Personal Identification Number (PIN)
- password.

And your bank will never contact you about things like this by:

- text message
- email
- phone.

Your bank will never contact you saying they will:

- cancel your account straight away

or

- threaten you.

Organisations will never ask you to:

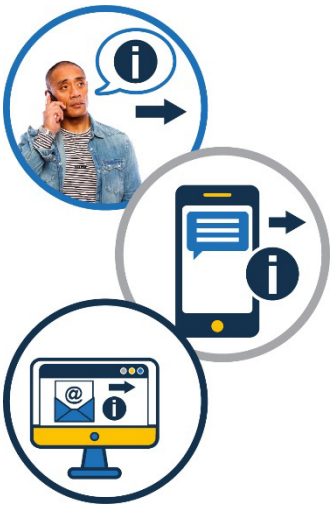
- change your information
- download software
- let them use your phone or computer.

This includes government organisations.

When should you contact your bank?

If you think you've been scammed, you should contact your bank as soon as you can.

This helps your bank protect your money.



You should tell your bank if you've shared your banking or personal information in a fake:

- call
- text
- email.

You should tell your bank if you:

- used any links
- downloaded any files.

You should tell your bank if you see anything strange in your bank account.

What to look for

Scammers might try to get your personal information in different ways.

They might ask you to tell them your:

- address

- birth date

- bank account information

- **Tax File Number (TFN)**.

You get a TFN from the Australian Taxation Office (ATO).

Your TFN is how the ATO knows who you are.

They might tell you to use a link.

They might say something is wrong with your:

- computer
- internet.

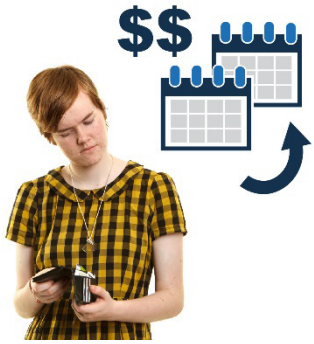
They might ask you to let them control your computer.

Scammers might ask you to pay them.

They might ask you for:

- money

- a gift card.



They might offer you a chance to put your money towards something, so you get more money in the future.

They might be in a relationship with you and ask for:

- money

- gifts.

Some scammers might offer you something that sounds very good.

If it sounds like a very good offer, it might be fake.

Some scammers use email addresses that don't match the organisation they say they are from.

Staying safe from scammers

We have some tips for how you can stay safe from scammers.

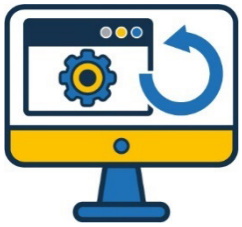
You should never:

- share your passwords
- write them down.

Passwords help keep your devices safe.

Make sure your computer:

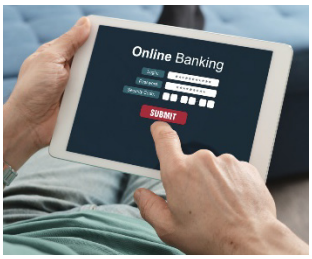
- has good software for keeping it safe



- the software is up to date.

You should never share your PIN.

Most of the time this is a 4-digit number.



You should check your bank account often.

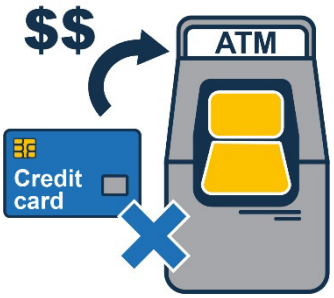
This will help you see if there is anything wrong with your bank account.

You should not swipe your bank card when you buy items.

It’s safer to:

- tap your card

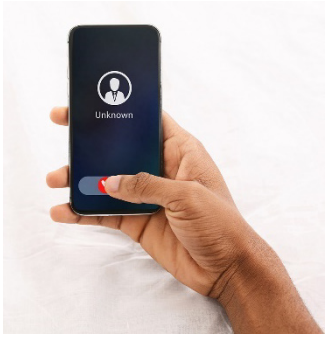
- insert your card.



If you have a **credit card**, you should ask the bank not to let it be used to get cash from ATMs.

When you use a credit card, you spend money you have borrowed from the bank.

You should talk to your bank about how you can keep your bank account safe.



You should hang up if someone asks for your personal information on the phone.

You should:

- find the organisation's website yourself

- go to their website

- find their phone number

- call them.

If you get an email asking you to pay a bill, you should call the organisation.

They can help you check the payment details.

You should never open files from people or organisations you don’t know.

If you’re not sure if something is a scam, you get help from:

- a family member

- a friend

- the organisation.

You can visit the Scamwatch website:

- for more information

- to report a scam

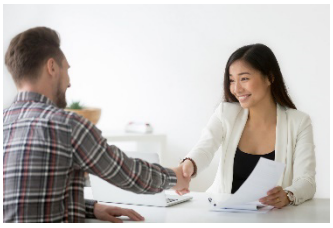
- to get help if you have been scammed

- to find out how to stay safe from scammers.

www.scamwatch.gov.au/

Who should you talk to if you need more help?

You should contact your bank if you need more:



- support

- information.

The Information Access Group created this Easy Read document using stock photography and custom images. The images may not be reused without permission. For any enquiries about the images, please visit **www.informationaccessgroup.com**.
Quote job number 4447-I.