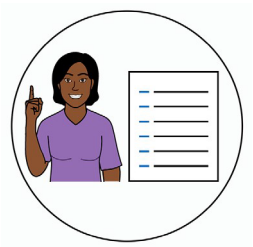
Scams

St. George Bank

Easy English

Hard words



This guide 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 guide

You can get someone you trust to help you

- read this guide

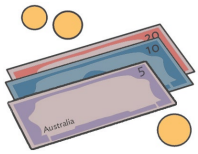
- know what this guide is about

- find more information.

About this guide

This guide is from St. George Bank.

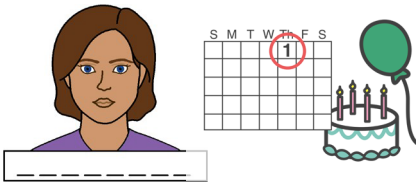
This guide is about **scams**.



A scam is when someone tries to trick you and make you give away your

- money

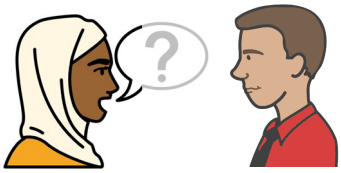
or



- personal information
  - for example, your name or birth date.

Scams can happen to anyone.

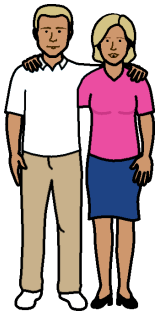
There are lots of different types of scams.



We want to make sure you can get help if a scam happens to you.

Types of scams

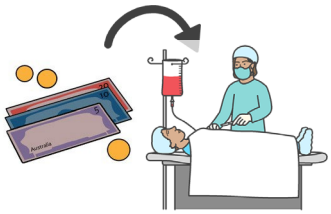
Romance and relationship scams



Someone who wants to scam you might

- start a relationship with you to get money or gifts
  - for example, they might talk to you about money on a dating website

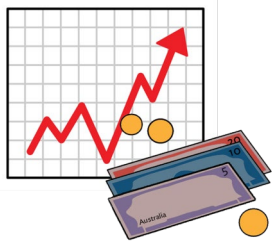
- make you put money or **assets** into their name
  - assets are things you own that are worth money. For example, your car or house



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

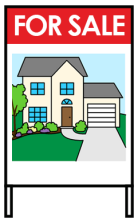
- ask to be in your **Will**.
  - a Will says what to do with a person's money and assets when they die.

Investment scams



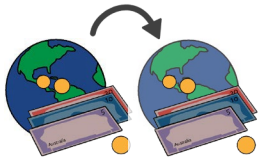
Someone who wants to scam you might pretend to give financial advice about **investing** your money.

Investing means you put your money somewhere to get more back in the future.



The investments could be in

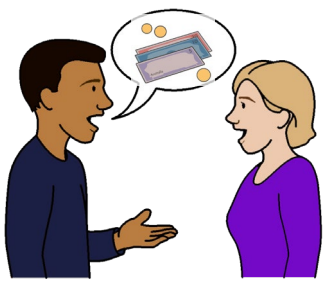
- real estate



- buying overseas money

- virtual money that is made on a computer.

For example, bitcoin.



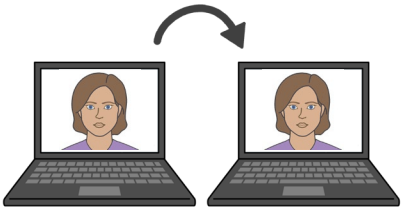
Someone who wants to scam you might

- pretend to be an investment expert

- tell you they can make you lots of money.

Remote access scams

Someone who wants to scam you might ask for **remote access** to your device.



Remote access means they can control your device from another device.

For example, your computer or mobile phone.

When someone has remote access they can see everything you do on the device.
For example, they can see all of your financial and personal information.

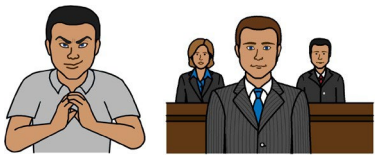
Financial information could be details about your money or your bank accounts.

To get remote access someone might

- pretend to be an expert who can fix your computer

- ask you to download software onto your computer.

Threat and penalty scams



Someone who wants to scam you might pretend to be a business, organisation or government.

They might use urgency, threats and **intimidation** to get your money or personal information.

Intimidation means they tell you something bad will happen if you do **not** do what they ask.

For example, someone calls and tells you

- they are from the tax office and you owe the government money

- you will be arrested by the police if you do **not** pay a fine

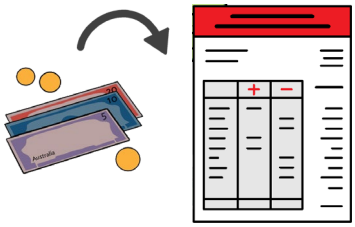
- you will be deported if you do **not** pay a fine or fee.

Business email scams

Someone who wants to scam you might send you an email that looks like it is from

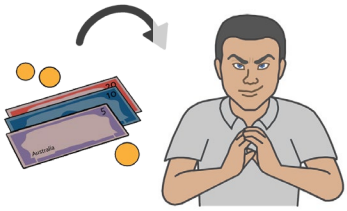
- a supplier

- someone from your work.



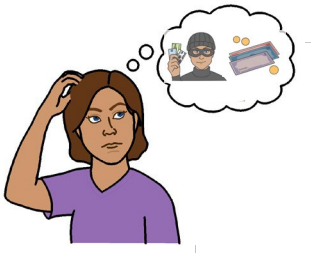
The email might be for the payment of an **invoice** to a new or updated account number.

An invoice is a bill that tells you how much and who you need to pay for something.



It is likely that the payment details will have changed so the money goes to the scammer instead of the real company you want to pay.

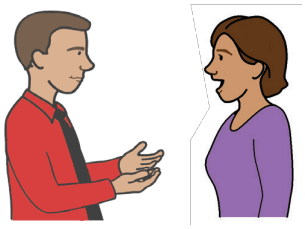
Signs and how to protect yourself



It can be hard to know if a scam is happening.

You can protect yourself from scams when you know what the **warning signs** are.

Warning signs are small clues that make you think something bad is happening.



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

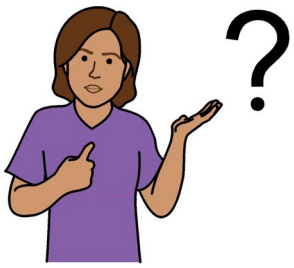
Someone contacts you when you do not expect it

This could be

- a phone call or SMS

- an email or letter

- at your front door in person.



If someone contacts you when you do **not** expect it

- find out who they are

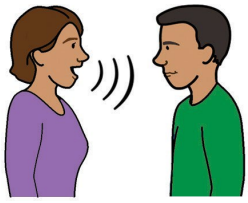
- ask why they are contacting you

- check if you recognise the email address.

If you get a call that you do **not** expect or if you do **not** know the caller, it is best to hang up straight away.

Check for real contact information on our bank app or website.

Do **not** use the information given by the caller.

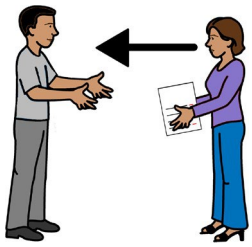


You can ask someone you know and trust to help you work out if it is a scam.

Someone asks you to do something strange

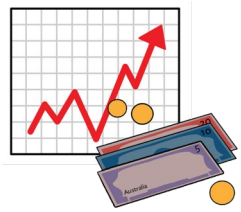
It is strange if someone you do **not** know asks you to

- download software to access your computer or device

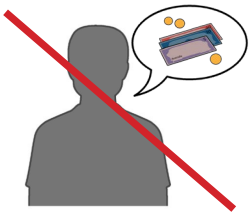


- give your personal information

- make an unexpected payment



- invest money quickly to **not** miss out on something.



It is best to **not** do what they ask until you can find out more information.

Check for real contact information on our bank app or bank website.

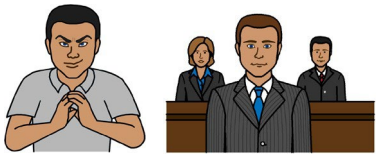
Do **not** use the contact information given by the caller.

If you think you have downloaded software to your computer or device

- turn it off straight away

- get help from a computer or mobile phone expert.

Be careful who you trust



Most people who want to scam you pretend to be other people or companies to get your trust.

Real people or companies do **not**

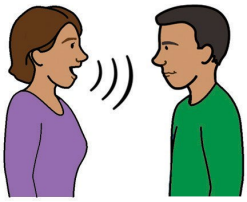
- stop you from asking your support network for help

- lie about what they do or ask you to lie about what you are doing.

Real people or companies will **not** ask for

- remote access to your device

- your online banking details
  - for example, passwords, or security codes.



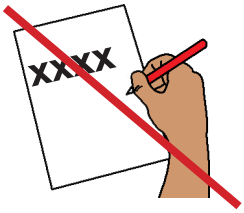
Find information yourself or talk to friends or family before you make any decisions.

Do **not** only rely on information the person you are talking to gives you.

Only get financial advice from a professional.

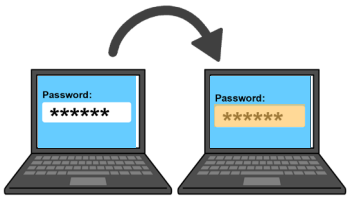
Do **not**

- open attachments or links in an email or SMS from people or organisations you do **not** know



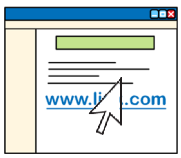
- write down or share passwords, PINs, security codes or personal information.

What to do if a scam happens



Change your PINs and passwords if

- you think someone has your details
- you have clicked on a link in a strange email or message
- you think a scam has happened to you.



If you have clicked on a link in a strange email or SMS or need help, contact us straight away.

Call 133 330

Tell us about strange messages asking for your banking details, money or other personal information.

Send the email or SMS to us and then delete it.

Email hoax@stgeorge.com.au

SMS 0497 114 629

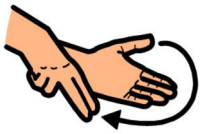
You can get help to talk to us

If you do **not** speak English you can call us and ask for an **interpreter**.

Call 132 032

An interpreter gives your message from one language to another.

For example



- English to Auslan

- English to Mandarin.

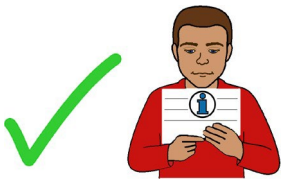
National Relay Service

If you need help to speak or listen you can use the National Relay Service to contact us.

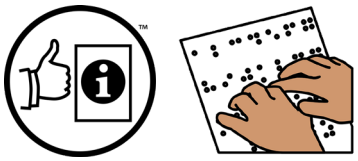
Call 1800 555 660

Website

accesshub.gov.au/about-the-nrs



We can help you with information that is **accessible**.



Accessible means

- you can get the information in different ways

- everyone can understand the information.

Call us to ask about our accessible information.

Call 133 330

Go to our website to find accessible information.

stgeorge.com.au/accessibility

Read more about scams on this website.

stgeorge.com.au/security

Notes