How to be safe online

An Easy Read guide

How to use this guide

ANZ wrote this guide.

When you see the word ‘we’, it means ANZ.

We wrote this guide in an easy to read way.

We use pictures to explain some ideas.

Bold

Not bold

We wrote some words in **bold**.

This means the letters are thicker and darker.

We explain what these words mean.

There is a list of these words on page 28.

This Easy Read guide is a summary of another guide.

This means it only includes the most important ideas.

You can find the other guide on our website.

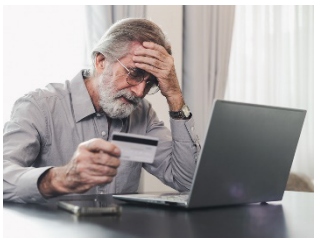
www.anz.com.au/security

You can ask for help to read this guide.

A friend, family member or support person may be able to help you.

What's in this guide?

About this guide



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.

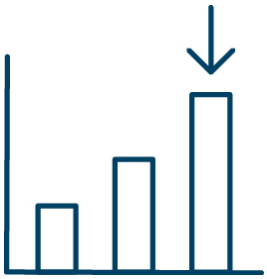
Scams can happen to anyone.

We want to keep:

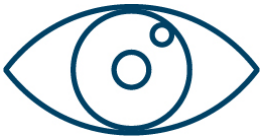
- you safe

- your money safe.

This guide talks about:



- the most common types of scams



- what to look for

- what to do if you have been affected by a scam

- how to stay safe from scammers.

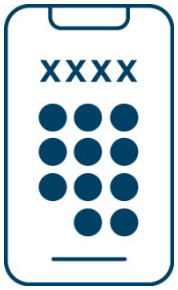
How we help protect you

We will never ask you for your personal information through:

- an email
- a text message.

This includes your:

- password



- Personal Identification Number (PIN)

- One-Time Passcode (OTP)

- bank account details.

If you think a scammer is pretending to be us, you should:

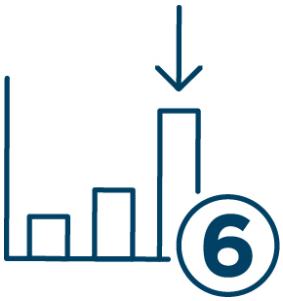
- ignore the phone call or text message

and

- tell us straight away.

The most common types of scams

There are many different scams.



We want to tell you about 6 of the most common types of scams.

We explain these scams on the following pages.

Business scams

This type of scam is when a scammer will:

- send you a fake email
- call you
- pretend to be a real business.

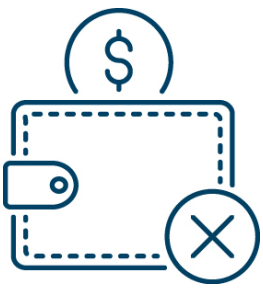
In the email, the scammer will tell you they have new bank details.

And that you need to send all future payments to their new bank account.

A scammer might also send you a fake **invoice**.

An invoice is a document that includes:

- a list of services that you need to pay
- how much you need to pay.



You don't need to pay for services on a fake invoice.

Remote access scams

Remote access is when someone can:

- control your device from any location
- manage data and information you have on your device.

This type of scam is when a scammer will ask you for remote access to your computer.

For example, they might ask you for log in details for your computer to:

- take your money
- get into your bank account.

The scammer might also send you a fake invoice to pay for computer products they sell.

For example, they might say something is wrong with your:

- device, like your mobile phone

- internet.

And try to sell you a product that can help keep your device safe from scammers.

Investment scams

You make an **investment** when you use money for something that will get more money in the future.

This can be:

- your money
- someone else's money.

This type of scam is when a scammer will:

- call you

  or

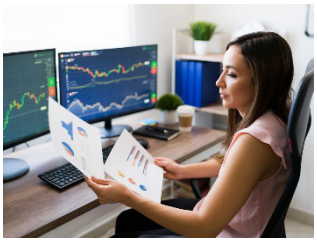
- send you an email.

They will ask:

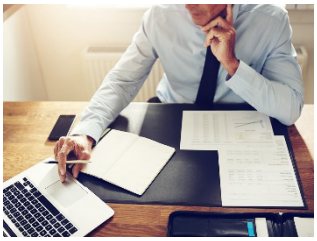
- you for money
- a business for money.

The scammer might offer to make an investment for you.

It is common for the scammer to pretend to be a:



- **stock broker** – someone who uses your money to make more money for you in the future



- **portfolio manager** – someone who makes decisions about your money to make more money for you in the future.

Bank scams

This type of scam is when a scammer pretends to be a bank.

They will send you a text message.

In the text message, they will give you a fake phone number.

And ask you to call the bank.

Or they might give you a website link to click on.

When you click on this link, it might take you to a website to fill out your personal information.

For example, log in details for your online bank account.

The scammer might also call you after they send you the text message.

They will try to tell you:

- someone is trying to get into your bank account
- your money is not safe.

The scammer will then tell you to move your money into another bank account.

Blackmail scams

Blackmail is when someone says they will do something bad to:

- hurt you
- get what they want.

This might be in person or online.

This type of scam is when a scammer might tell you they will share private photos of you if you don't:

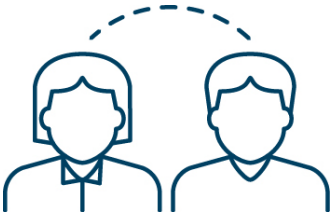
- send them money straight away

- share your personal information with them.

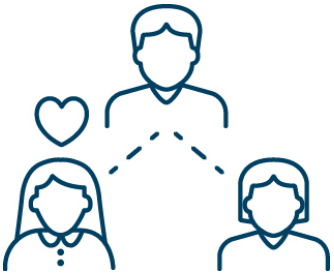
When a scammer blackmails you, they might:

- be mean and frightening
- upset you
- threaten you.

Romantic relationship scams



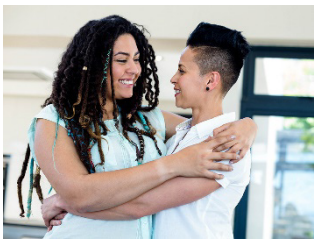
Your **relationship** with someone is how you are connected to them.



You can have lots of different relationships with people.

For example, you can have a **romantic relationship** with someone.

A romantic relationship is a very close relationship you have with another person.



When you have a romantic relationship with someone, it should be with a person you:

- trust
- respect
- care about.

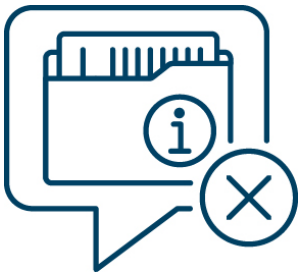
This type of scam is when a scammer pretends to have a romantic relationship with you.

You might start having a romantic relationship with a scammer.

But you only know them a little bit.

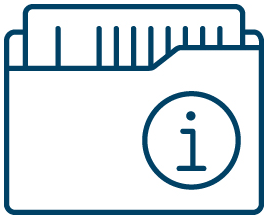
The scammer does this because they want to earn your trust.

Then ask you to send them money.



You shouldn't share too much personal information with people you only know a little bit.

What to look for



Scammers will try lots of different ways to get your personal information.

They might:

- send you an email
- send you a text message
- call you.

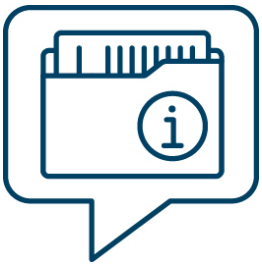
And ask you to open a website link or an attached file to get into your bank account.

They might ask you to make a payment online using:

- your log in details for your bank account

- a gift card

- digital money.



They might ask you to send them your personal information straight away.

Or they might ask you to make a payment straight away.

They might call you but use a recorded voice.

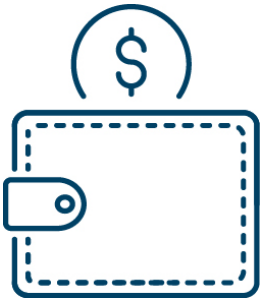
On the phone call, they might ask you to share personal information that can help them open your bank account.

For example, they might ask you to share your bank account password.

They might:

- ask you to let them control your device

- ask if you would like to borrow money from them



- tell you about a deal that will save you money.

What to do if you have been affected by a scam

If you think you have been affected by a scam, you should stop talking to the scammer.

You can block the scammer's:

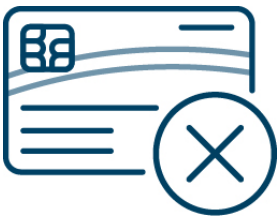
- phone number
- email address.

You should also change your password.

And make sure you use a different device the scammer can't get into.

For example, a computer or tablet.

If you can't get into your online account, contact us for support.



If you think a scammer has your bank card details, you should cancel your card straight away.

To cancel your card, you can:

- log into your ANZ online account

- use the ANZ app

- call us.

You can call us:

- 24 hours a day

- 7 days a week.

If you live in Australia, you can call:

13 33 50

If you live overseas, you can call:

+61 3 9683 8833

You can also send us an email with proof of the scam message.

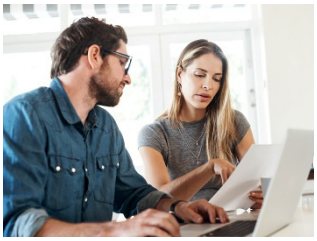
This can include a photo or screenshot.

hoax@cybersecurity.anz.com

You should also check your bank account to see if anything strange has happened.

How to stay safe from scammers

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



If you think you have been affected by a scam, talk to someone you trust.

For example, a family member or friend.

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

To check if it really is the person you are talking to, you can agree on a word that only:

- you know
- your family members know.

Don't click links from someone you don't know if you get:

- a text message
- an email.

You should never let a stranger control your devices.

Or force you to make decisions quickly.

Check the company details if they ask you:

- for personal information
- to pay an invoice.

To do this, you should:

- find the real company number online

  and

- call them.

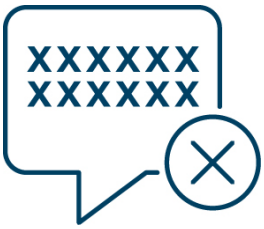
Then ask to speak to someone.

Make sure you don't call back the fake phone number the scammer used to call you.

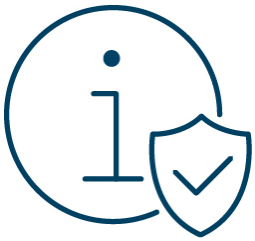
To protect your bank information, use a unique:

- password
- PIN.

Never save this information on your browser or devices.



And never share your bank customer number with anyone.



Use extra steps to protect your bank information.

For example, a one-time passcode to make a payment.

You should check your bank account often.

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

Word list

This list explains what the **bold** words in this document mean.

Blackmail

Blackmail is when someone says they will do something bad to:

- hurt you
- get what they want.

This might be in person or online.

Investment

You make an investment when you use money for something that will get more money in the future.

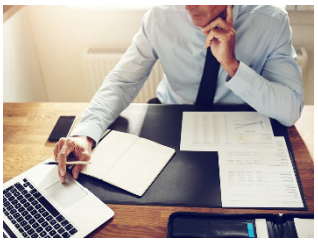
This can be:

- your money
- someone else's money.

Invoice

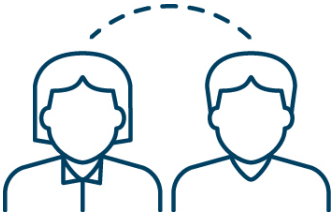
An invoice is a document that includes:

- a list of services that you need to pay for
- the amount that you need to pay.



Portfolio manager

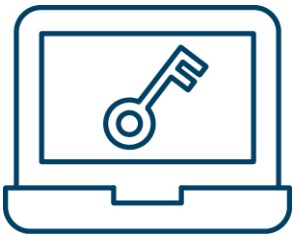
Someone who makes decisions about your money to make more money for you in the future.



Relationship

Your relationship with someone is how you are connected to them.

Remote access



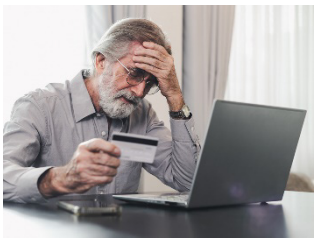
Remote access is when someone can:

- control your device from any location
- manage data and information you have on your device.

Romantic relationship

A romantic relationship is a very close relationship you have with another person.

Scam

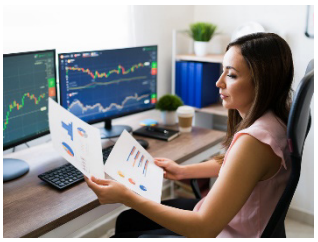


We call it a scam when someone tries to:

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

Scammer

A scammer is a person who does a scam.



Stock broker

Someone who uses your money to make more money for you in the future.

Disclaimer

This document includes general information only.

It might not be right for you.

Or you might have different goals.

Think about getting your own advice about the information in this document.

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 5342.

Australia and New Zealand Banking Group Limited (ANZ) ABN 11 005 357 522.

www.anz.com.au/security