



Australian Government



National
Anti-Scam
Centre

National Anti-Scam Centre

A guide to scams

Easy Read version





How to use this guide



The National Anti-Scam Centre wrote this guide.

When you see the word 'we', it means the National Anti-Scam Centre.



We wrote this information in an easy to read way.

We use pictures to explain some ideas.

Bold

We wrote some important words in **bold**.

Not bold

This means the letters are thicker and darker.



We explain what these bold words mean.

There is a list of these words on page 39.



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.scamwatch.gov.au/research-and-resources/the-little-black-book-of-scams



You can also find Easy Read information about different types of scams on our website.

www.scamwatch.gov.au/types-of-scams



You can ask for help to read this guide.

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



This is a long document.

You don't need to read it all at once.

You can take your time.



We recognise First Nations peoples as the traditional owners of the land we live on – Australia.



They were the first people to live on and use the:

- land
- waters.

What's in this guide?

About the National Anti-Scam Centre	6
<hr/>	
About scams	8
<hr/>	
Types of scams	12
<hr/>	
Scams that happen a lot	20
<hr/>	
How to protect yourself from scams	27
<hr/>	
What to do if you think you've been scammed	34
<hr/>	
Where to report a scam	36
<hr/>	
More help and support	37
<hr/>	
Word list	39
<hr/>	

About the National Anti-Scam Centre

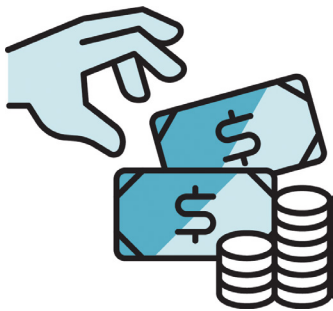


A **scam** is a crime.

We call it a scam when someone:



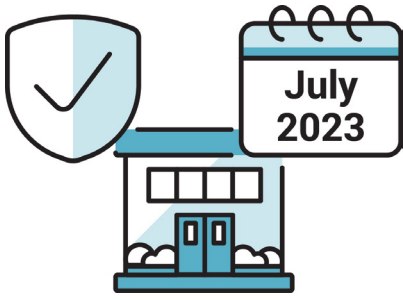
- lies to you



- tries to take your money



- tries to get your personal information.



The National Anti-Scam Centre works to keep Australians safe from scams.

The Government started the National Anti-Scam Centre in July 2023 to share information about scams.

We can help people understand:



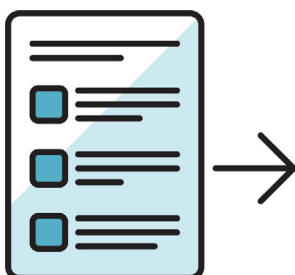
- different types of scams



- how people who do scams lie to people



- how people can stay safe from scams.



We explain what to do if you think you've been scammed on page 34.

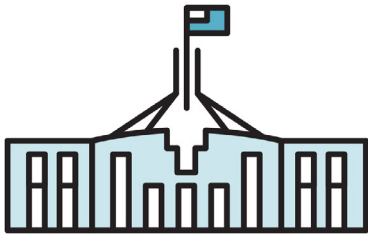
We also explain where to report a scam on page 36.

About scams

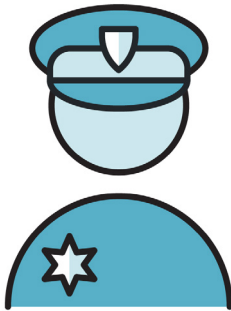


People who do scams will pretend to be someone you trust.

This might include:



- the Australian Government



- the police or the courts



- a well-known organisation or business you trust – like your bank or post office.

This might also include:



- your friends or family members



- someone you might want to have a very close relationship with



- an internet or phone provider



- an **employer**.

An employer is a person who hires other people to work for them.

People who do scams might tell you:



- they have a good deal for you

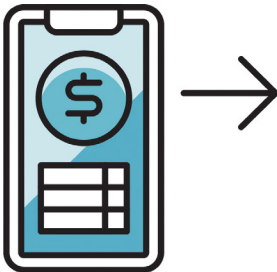


- a sad story and ask for help



- something bad might happen to you.

People who do scams might ask you to:



- transfer them money

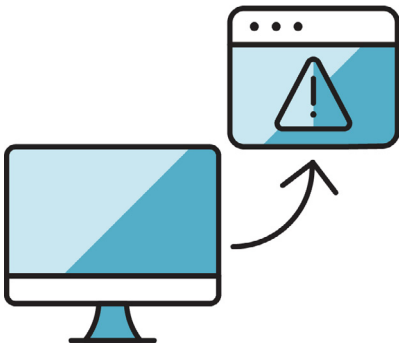


- send them your personal information



- pay them in different ways, like a gift card.

People who do scams might also:



- send you links to scam websites



- ask you to open attachments in their messages.



People who do scams use these websites and attachments to steal your personal information.

Types of scams

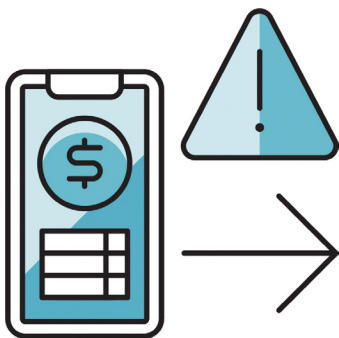


People who do scams can use different types of technology.

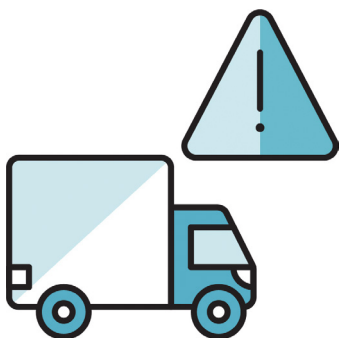
We explain these on the following pages.

Text and SMS scams

A scam text message or SMS might tell you that:



- there is a problem with a payment you made



- there is a problem with a delivery



- someone has **hacked** your accounts.

When someone has hacked your accounts, it means they can use your account without you wanting them to.



A scam text message or SMS might also tell you that they will cancel a service you use, if you don't do something.

For example, your phone service.



You can read our document about text and SMS scams on our website.

www.scamwatch.gov.au/types-of-scams

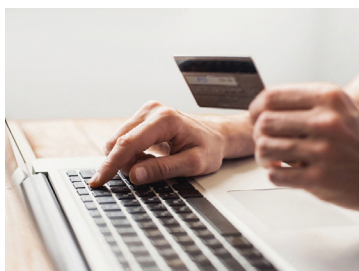
Email scams



People who do scams can make their emails look like they're from a real organisation or business.

For example, they might use the same logo.

A scam email might ask you to:



- make a payment using different bank details



- log in to an account with your username and password



- confirm your banking details to get a payment you weren't expecting.



A scam email might say it has:

- information about you
- photos of you.



And it might threaten to show other people.



You can read our document about email scams on our website.

www.scamwatch.gov.au/types-of-scams

Phone call scams



The person doing a phone call scam might know things about you that you haven't told them, like your name.

They might ask you to:



- let them use your computer



- move your money into another bank account

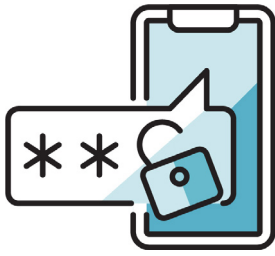


- download a program on your computer



- download an app on your phone.

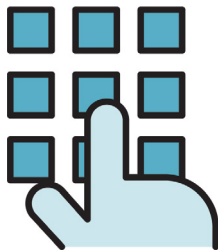
They might also ask you for information, like:



- a passcode that you can only use once



- your passwords



- your Personal Identification Number (PIN)



- your credit card details



- your banking details.



You can read our document about phone call scams on our website.

www.scamwatch.gov.au/types-of-scams

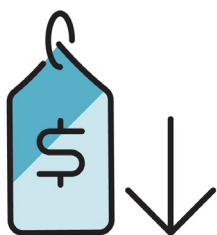
Website scams



People who do scams can make a website look real, by using:

- fake reviews
- fake ads or error messages.

A scam website might:



- sell items that are very cheap compared to usual



- tell you about how you can make money quickly and easily



- only show good reviews.



You can read our document about website scams on our website.

www.scamwatch.gov.au/types-of-scams

Social media and app scams

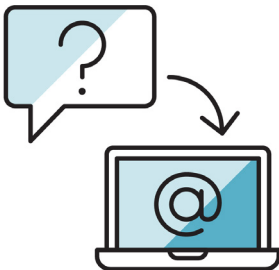


Social media and app scams can happen on different types of:

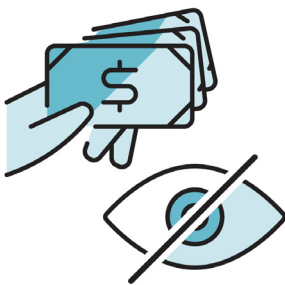
- social media, like Facebook
- apps, like WhatsApp.



People who do scams might pretend to be someone you know.



People who do scams might ask if you can talk somewhere else, like a private chat or email.



They might also say they will:

- buy something from you without seeing it first
- sell something to you without letting you see it first.



You can read our document about social media and app scams on our website.

www.scamwatch.gov.au/types-of-scams

Scams that happen a lot



We explain some of the scams that people experience a lot on the following pages.

Impersonation scams



Impersonation is when a person pretends to be someone else.



People who do this type of scam will pretend to be:

- someone you know
- or
- a well-known organisation or business you trust.

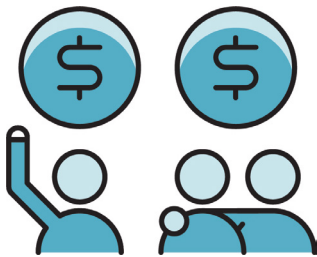


They will make it seem like they are calling or texting you from an official phone number.

Investment scams



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



This can be:

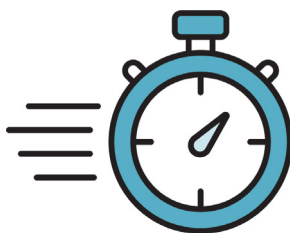
- your money
- someone else's money.



People who do this type of scam will make their investment sound:

- really good
- safe.

For example, they will:



- make you think you need to make an investment right now



- promise that you will get a lot of money without much risk.

Job scams

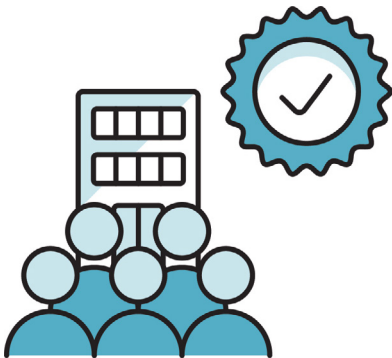
People who do this type of scam will offer you a job that:



- is easy



- pays a lot of money.

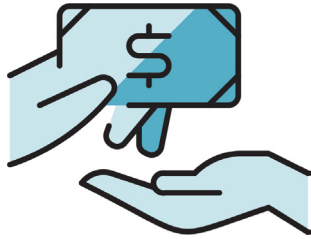


They will pretend to offer you a job at a well-known organisation or business.



Or they might pretend they hire people for other organisations and businesses.

Shopping scams



People who do this type of scam will pretend they want to:

- buy something from you
- sell something to you.



They will create a website or social media account that looks like a real business.

For example, they might pretend to be:

- an online music shop.
- selling expensive guitars at a very cheap price.



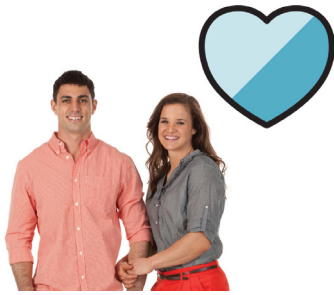
They will sell products or services that:

- sound really good
- are cheap
- seem too good to be true.



They might also send you a fake bill.

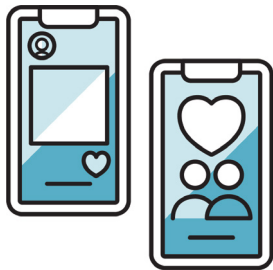
Romance scams



A **romance scam** is when someone pretends to have loving feelings for you.



People who do this type of scam will pretend to have a romantic relationship with you.



They might connect with you on:

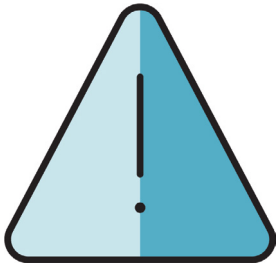
- a social media app
- a dating app.



When you trust them, they will:

- pretend that something bad has happened
- and
- ask you for money.

Threatening scams



A threatening scam is when someone says they will do something bad to you if you don't give them what they want.

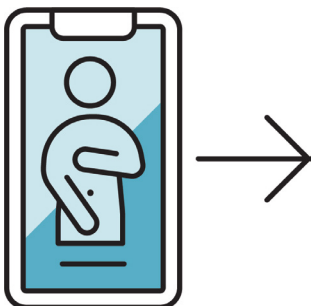
People who do these scams might threaten to:



- arrest you or make you leave Australia



- physically hurt you



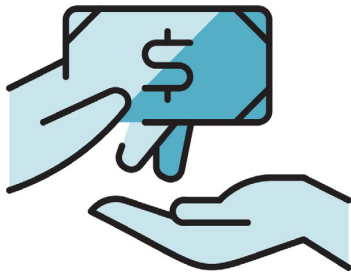
- share a private photo of you.

Unexpected money scams



People who do this type of scam will say you have won some money.

Before they send you the money, they will ask you to:



- pay money or a fee



- give them personal information, like your banking details.

How to protect yourself from scams



If you think something might be a scam, you should:

- go directly to the official website or app and make sure the contact details are the same
- only use the contact details on the official website or app.

If a text message or SMS tells you that someone you know has changed their contact details, you can:



- call the person on a phone number that you already have for them



- send a question to the new phone number that only the person you know can answer.



You should never reply if:

- you don't know the person
- the person threatens you.



If someone offers to send you a payment, you should never:

- give your personal information to them
- pay them money.



You should think about protecting your:

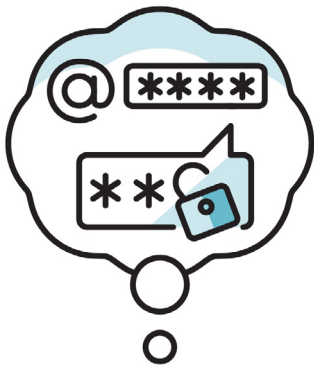
- email account
- phone.



This includes using **multi-factor authentication**.

Multi-factor authentication is when you must use 2 different ways to log in to your account every time.

For example, setting up your email account so a different number is sent to your phone every time you want to log in.



This means that people who do scams can only use your email account if they know:

- your email password
- and
- the number that is sent to your phone.



This also includes keeping your:

- phone and computer updated
- apps updated.



You should never download a program or app that lets someone use your computer or phone.

You should also never:

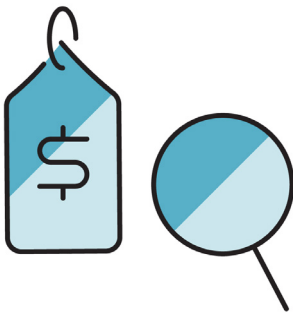


- select a warning or error message that pops up on your screen

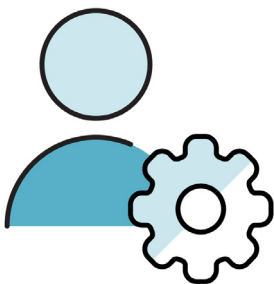


- open a link that someone has sent you in an email or a text message, without checking that it is real first.

If you think a website might be a scam, you should:



- check how much the same items cost on other websites



- find out more about who runs the website.



You should also:

- block the account
- contact the social media platform.

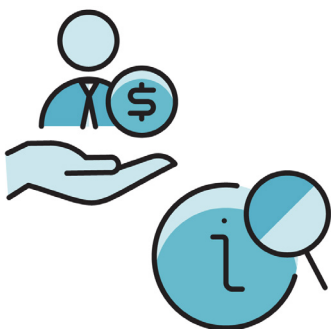
If you have only met someone online,
you should never:



- pay them money



- send them private photos of yourself.



If an organisation or business offers you a job,
you should always learn more about them.

An organisation or business should always ask:



- if you have the right skills for the job



- to **interview** you.



When someone interviews you, they ask you questions about:

- other jobs you have had
- your skills.



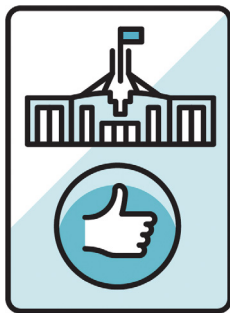
You should never agree to take a job if they don't ask you for these things.



You should also never pay anyone to get a job.



You should only get advice about money from someone who has a **license** from the Australian Government.



A license is a document that says the Government trusts that you know how to do something the right way.



Only someone with a licence can ask you for a payment.

What to do if you think you've been scammed



Anyone can be scammed.



It might have happened to you or someone you know.



If you think you have been scammed, it is important to get help as soon as you can.



If you have lost money to a scam, you should contact your bank.



If people who do scams are trying to use your personal information to hurt you, you should contact IDCARE.



You can call IDCARE.


1800 595 160



You can visit the IDCARE website.

www.idcare.org

Where to report a scam

 **SCAMWATCH** You can report a scam to Scamwatch.



Scamwatch works to keep people in Australia safe from scams.



When you report a scam, you help Scamwatch protect more people.



You can fill out the form on the Scamwatch website.

www.scamwatch.gov.au/report-a-scam



You can ask for help to fill out this form.

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

More help and support



Lifeline is a service for people at risk of suicide.

This is when someone ends their own life.



You can call any time.

13 11 14



Beyond Blue is a service that can support you with your mental health.



You can call any time.

1300 224 636



Kids Helpline is a service that supports young people between 5 and 25 years old.



You can call any time.

1800 55 1800

Support to manage your money



Scams can make it hard to manage your money.



The National Debt Helpline has **financial counsellors** you can talk to.

Financial counsellors can help you manage your money.



You can call them.

1800 007 007



You can call from:

- 9:30 am to 4:30 pm
- Monday to Friday.



You can also chat with a financial counsellor online.

www.ndh.org.au

Word list

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



Employer

An employer is a person who hires other people to work for them.



Financial counsellors

Financial counsellors can help you manage your money.



Hacked

When someone has hacked your accounts, it means they can use your account without you wanting them to.



Impersonation

Impersonation is when a person pretends to be someone else.



Interview

When someone interviews you, they ask you questions about:

- other jobs you have had
- your skills.



Investment

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

This can be:

- your money
- someone else's money.



License

A license is a document that says the Government trusts that you know how to do something the right way.



Multi-factor authentication

Multi-factor authentication is when you must use 2 different ways to log in to your account every time.



Romance scam

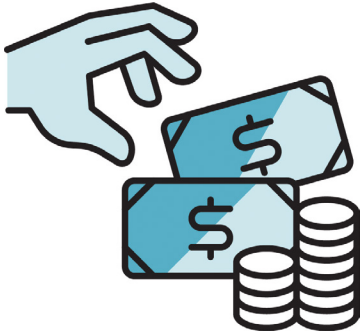
A romance scam is when someone pretends to have loving feelings for you.

Scam

We call it a scam when someone:



- lies to you



- tries to take your money



- tries to get your personal information.



The Information Access Group created this Easy Read summary 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 5461-F.



Australian Government



National
Anti-Scam
Centre

www.scamwatch.gov.au