Protect yourself against scams

A scam is a dishonest or illegal activity that tricks people into giving away money, personal information, intimate images or something else of value. An online scam is usually run by someone with a fake profile or a fake business. So while the internet can be a wonderful place to explore, it pays to be cautious!

Being aware of scammers is one of the important steps towards avoiding them. Once you know their tricks, you are more likely to be able to spot a scam. Staying alert is your best defence.

Here are some top tips for recognising and avoiding scams.

Protect your personal information

Scammers try to access your personal information by asking you questions or giving you instructions via a phone call, email, text, or through social media. Scammers will use your personal details to steal your money or commit another crime.

What do scammers ask for?

Scammers try to gain your trust by pretending to be from a well-known organisation or agency such as NBN Co, Telstra, Microsoft, Australia Post, the tax office, the police or Services Australia (MyGov, Centrelink, Medicare).

To trick you into giving away your personal or financial information, scammers may:

- get you to click on a link
- ask you to give them remote access to your computer
- ask you to pay a debt
- ask you to buy a voucher to pay a fine
- ask you to transfer funds or send money overseas.

Signs that it may be a scam

Watch out for:

- emails, messages or calls that are unexpected or from someone you don't know
- promises of financial benefit
- threats of a fine or debt
- threats to close or lock your account
- links that do not look genuine, such as having an unusual website address
- an unusual sense of urgency or deadline.

Tip: If you are unsure whether a message or call is real, do not use the contact details provided, instead do an internet search for the organisation's number or email address.

Be careful of friends you have made online

Online scammers often get in touch with people through social media. They use their tactics in romance or dating scams. They also target people playing online games like Words with Friends and Scrabble. Their goal is to build a relationship (it doesn't have to be romantic) to gain your trust so they can ask you for money, personal information, intimate images or something else of value.

Signs that it may be a scam

Look out for people who:

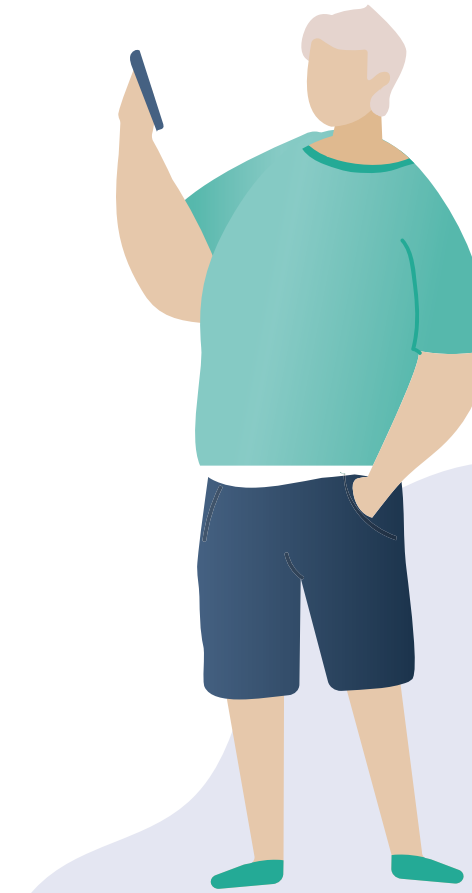
- express deep affection quickly
- try to move your conversation from the website where you met to a more private communication channel, such as direct messaging or emailing
- tell you elaborate stories about financial troubles
- say they want to meet but make excuses, or ask for money so they can 'travel' to meet you
- ask about your financial status
- get persistent, more direct or even aggressive when you don't send money
- seem to have inconsistencies in their online profile — for example, their photo looks different to their description, or they say they are university educated but their grammar is poor.

It is also common for scammers to pose as aid workers or pretend to be military personnel or professionals working abroad.

Tip: Do an image search on a few sites like Google (images.google.com) or Tineye (tineye.com), to help you check if the person is who they say they are.

How to protect yourself

- Do not provide personal or financial information to people you have never met in person.
- Do not make any payments by money order, wire transfer, international funds transfer or electronic currency like bitcoin. (It is difficult to recover money sent this way, if it turns out to be a scam.)
- Do not agree to carry packages internationally or transfer money for someone else, because you may be committing a crime without knowing it.
- Do not share intimate photos or use webcams in an intimate setting.
- Stop all communication if a person starts asking you for a favour or money.
- Be alert to spelling mistakes, poor grammar and inconsistencies in stories.



Watch out for investment scams

Investment scammers put a lot of time, effort and money into creating convincing stories, fancy websites and glossy brochures to scam older Australians who are looking to grow their 'nest eggs' or savings.

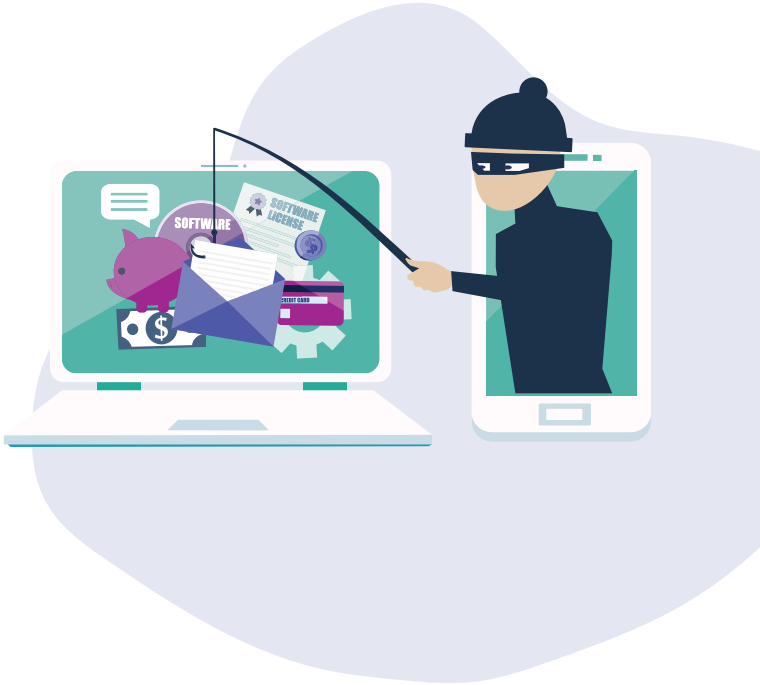
How do scammers get you interested?

These are some of the methods investment scammers use:

- They direct you to a fake website that makes false claims of investments with very good performance and returns.
- They post an advertisement or article on a social media site like Facebook.
- They send you a 'friend' request on social media by posing as someone you know or are connected to, in order to access your profile information and send you tailored offers to invest.

Signs that it may be a scam

- The scammer calls or emails you persistently.
- They pass your call along the line — a junior person speaks to you first, then a more senior person tries to close the deal.
- They pressure you to act quickly or you will miss out.
- They say they do not have an Australian financial services (AFS) licence or that they don't need one
- They try to stop you pulling out of the deal.



Superannuation

Investment scammers offer quick and easy ways to 'unlock' your superannuation early. They may ask you to agree to a story to ensure the early release of your money and then, acting as your financial adviser, they deceive your superannuation company into paying out your super benefits directly to them.

Once they have your money, the scammer may take large 'fees' out of the released fund or leave you with nothing at all.

Note! Usually you cannot legally access the preserved part of your super until you are between 55 and 60, depending what year you were born. There are certain exceptions such as severe financial hardship or compassionate grounds — but anyone who otherwise offers early access to your super is acting illegally.

Artificially inflating the share price

Investment scammers buy shares in a small company at a low price, then send out false tips about the company having great prospects. As more people invest, the share price rises and the scammers sell their shares at the peak of the price rise. Then the share price falls and the shareholders are left holding them at the reduced value.

Celebrity endorsement scams

Investment scammers use fake endorsements from successful and well-respected entrepreneurs or celebrities in a bid to lure people into believing a scheme is being backed by someone they trust. These scams often appear as online advertisements or promotional stories on social media feeds or seemingly legitimate, trustworthy websites.

How to protect yourself

- Be suspicious of opportunities that look too good to be true.
- Be suspicious of celebrity endorsement advertisements or stories.
- Do not let anyone pressure you.
- If you are under 55, watch out for offers promoting easy access to superannuation benefits.
- Do your research and seek trusted or independent financial or legal advice.
- Do not provide personal or financial information until:
  - you have checked if the financial advisor and their company is registered via the ASIC website asic.gov.au/online-services/search-asics-registers/.
  - you have checked ASIC's list of companies you should not deal with moneysmart.gov.au/scams/companies-you-should-not-deal-with.

Help, I suspect I'm being scammed

If you think you are the victim of a scam, don't be embarrassed and don't keep it to yourself. There are steps you can take to fix the problem:

- Contact your bank to stop any further payments to the scammer.
- Contact ID Care idcare.org if your personal information has been exposed or misused.
- For any Medicare, Centrelink or myGov scams, call Services Australia on 1800 941 126 or email reportascam@servicesaustralia.gov.au.
- Report the scam to the Australian Competition and Consumer Commission at scamwatch.gov.au so they can tell other people how to avoid it.

To keep up to date with the latest scams to avoid, subscribe to Scamwatch email alerts scamwatch.gov.au/news/subscribe-to-scam-alert-emails

Take the time to discover Be Connected

Be Connected is a comprehensive website with free resources specifically designed to support older Australians to connect online safely and navigate the digital world confidently. The site is also useful for families and community organisations who want to help older community members access all the benefits of the internet.

beconnected.esafety.gov.au