Australian Government

Be Connected
Every Australian online.

Can you spot a scam?

Being aware of scams and how they work is one of the important steps towards avoiding them. Each year older Australians lose millions of dollars through scams. While the internet is a wonderful place to explore and connect with others, we cannot always be sure that people are who they say they are. Once you know a scammer's tricks, you're more likely to be able to spot a scam.

Phishing scams

Phishing scams are attempts by scammers to trick you into believing they are from a trusted organisation or a person you know to get you to give out personal information such as your bank account numbers, passwords and credit card numbers.

Phishing messages are designed to look genuine and often copy the format used by the organisation the scammer is pretending to represent including their branding and logo. These scams can appear in many forms including emails, text messages or phone calls. For example, you might receive:

- a text message from your bank asking you to confirm your password
- an email from your internet provider asking you to update your details
- a text message from a family member using a new phone number telling you they have lost their phone and need you to send money urgently
- a phone call from your financial institution to alert you to an 'unauthorised or suspicious activity on your account', or that your account will be closed if you don't update your details
- a Facebook notification from a person you know recommending a website.

Tax and Medicare scams

Scammers impersonate the Australian Taxation Office (ATO), Medicare and other government organisations to try and trick you into paying money and sharing personal information. These scammers create fake websites and will send you emails, text messages and call you pretending to be from a government organisation.

The ATO will never email, text or call asking you to:

- provide personal information such as your tax file number, credit card or bank details
- pay a fee to receive your tax refund, or to get out of being arrested for tax evasion
- click a link to enter your personal details
- download files or install software.

If you are unsure whether the communication is from the ATO, call the ATO Scams hotline 1800 008 540 or visit ato.gov.au/scams.

How to protect yourself

- Slow down. Re-read the message. Ask yourself could the message or call be fake?
- Is it an official email address or is it not quite right?
- Who is it addressed to? Be suspicious if it is to 'Dear customer' instead of your name.
- Does it contain typing errors or grammatical mistakes? This can be a sign that it is from a scammer.
- Don't use the contact details provided in the message, they could be fake. Do an internet search for the organisation's phone number and official website.
- Don't click on any links or open any attachments as they may download a virus to your device – just press delete.
- Don't give out personal details such as your tax file number (TFN), date of birth, bank account or credit card details.

Remember: Scammers may try to play with your emotions to get you to react and not take time to think carefully about the situation. Their tactics may include using threats or fines, telling you that there has been unauthorised spending from your account or pretending to be a family member that needs help.

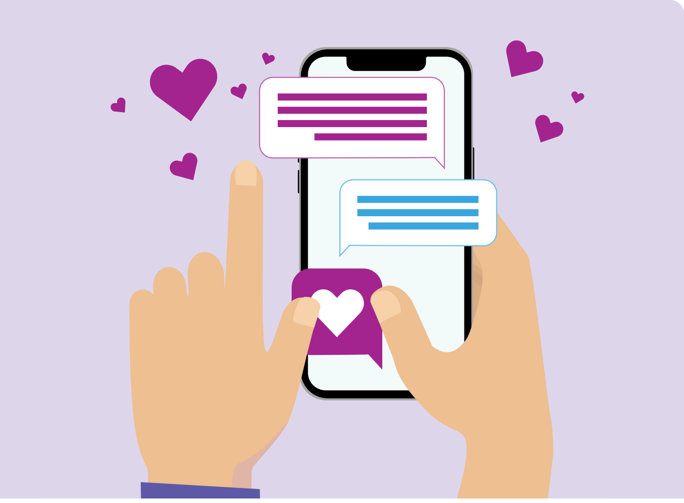
Friendship and romance scams

Scammers take advantage of people looking for friends or romantic partners, often via dating websites, apps, social media or even online games by pretending to be prospective companions. Their aim is to gain your trust to get you to provide money, gifts, intimate images or personal details.

What can you do to be savvy and safe?

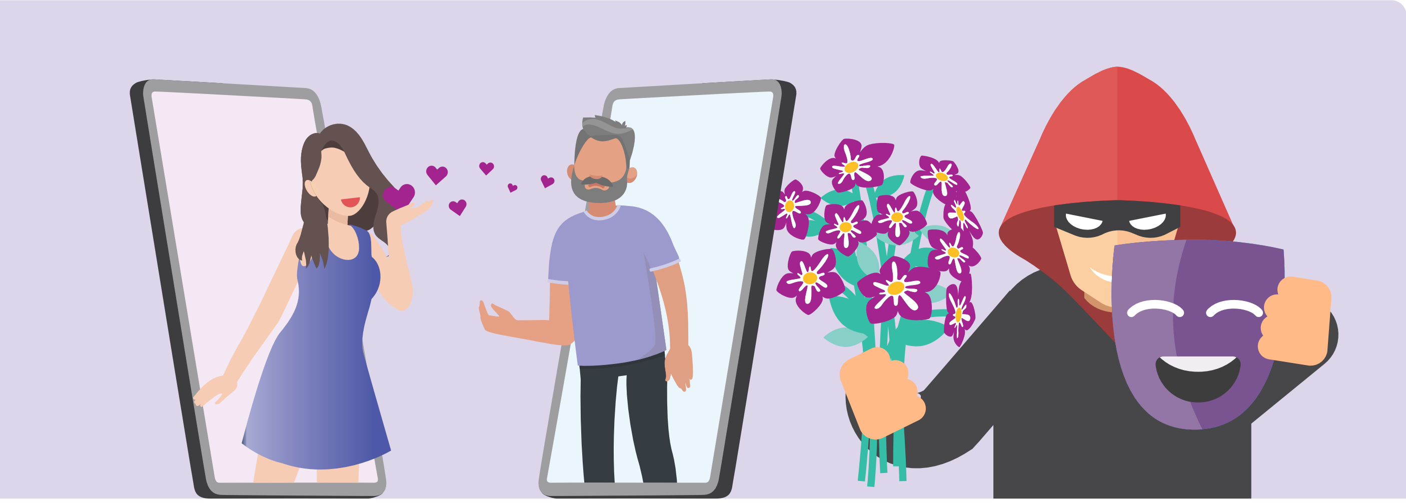
Look out for people who:

- express deep affections for you very quickly
- after gaining your trust – often waiting weeks, months or even years – tell you an elaborate story and ask for money or a loan, gifts or your bank account/credit card details
- avoid meeting you in person and make excuses as to why they can't travel to see you
- have an online profile that is not consistent with what they tell you about themselves.



How to protect yourself

- Never send money or give credit card details, online account details, or copies of important personal documents to someone you haven't met in person.
- Do a Google image search of the person's photos to help determine if they really are who they say they are or if the photos have been taken from somewhere else on the internet. Go to images.google.com and click on the camera icon.
- Be suspicious when they start mentioning money problems or needing money for an emergency.
- Be alert to things like spelling and grammar mistakes and inconsistencies in their stories.
- Don't share intimate pictures or videos. Scammers are known to blackmail their targets using compromising material.



Tech support scams

These scams usually start with a call or email that appears to be from a large telecommunications or computer company, such as Telstra, the NBN or Microsoft to tell you that you have a computer or internet problem and they can fix it. They will then request remote access to your computer to 'find out what the problem is' or try to talk you into buying unnecessary software or a service to 'fix' the computer.

How to protect yourself

- If you receive an unexpected phone call about your computer and remote access is requested – hang up.
- Don't provide an unsolicited caller remote access to your computer.
- Don't share your personal information such as your bank account or credit card details.
- Don't buy software from an unsolicited call or email.
- Ignore pop-up messages telling you to call tech support.

Top tips for avoiding scams

Stop

- Take your time before giving money or personal information to anyone.
- Scammers will offer to help you or ask you to verify who you are. They will pretend to be from organisations you know and trust like a business you deal with, or police, government or fraud service.

Think

- Ask yourself could the message or call be fake?
- Never click a link in a message and ask a trusted friend or family member what they would do. Only contact businesses or the government using contact information from their official website or through their secure apps. If you're not sure say no, hang up or delete.

Protect

- Act quickly if something feels wrong.
- Contact your bank immediately if you lose money or personal information or if you notice some unusual activity on your cards or accounts. Seek help from organisations like IDCARE and report online crime to ReportCyber. Help others by reporting scams to Scamwatch.

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 or financial institution immediately to stop any further payments to the scammer.
- If you have experienced cybercrime and lost money online, you can report it to the police via ReportCyber or visit: cyber.gov.au
- If you are concerned that your personal information has been exposed and misused, contact Australia's National Identity and Cyber Support Service IDCARE on 1300 432 273 or idcare.org
- report the scam to the ACCC via the scamwatch.gov.au/report-a-scam page. This helps to warn people about current scams, monitor trends and disrupt scams where possible.
- Spread the word to your friends and family to protect them.

Remember: There's always someone who can help – whether it's the folks at cyber.gov.au or scamwatch.gov.au, a technically minded friend or family member, or even a local computer club

To keep up to date with the latest scams to avoid, subscribe to Scamwatch email alerts.

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.

visit beconnected.esafety.gov.au

Australian Government | eSafety Commissioner

This program has been developed by eSafety as part of the Be Connected initiative.

beconnected.esafety.gov.au