Can you spot a scam?

On the internet, we cannot always be sure that people are who they say they are. Being aware of internet tricksters is one of the most important steps towards avoiding them. Once you are aware of their tricks, it should be easier to spot a scam when you see one.

Phishing scams

'Phishing' scams are the most common form of scam on the internet. They can appear to be from a trusted organisation and are designed to trick you into giving out your personal details such as your bank account, credit card number, username and passwords.

They can appear in many forms:

- unexpected emails, text messages or phone calls that ask you to confirm, update or re-enter your personal details
- urgent or threatening messages telling you something unusual is happening with your account, or that your account will be closed so you need to click on a link to rectify it
- unexpected emails that ask you to open or download an '.exe' or '.zip' file.

Tip: If you are unsure about a message you have received, do an internet search for the company it appears to be sent from and contact them directly.

Slow down. Re-read the message.

- Who is the sender? Is it an official email address or a strange looking one?
- Who is it addressed to? Be suspicious if it is to 'Dear customer' instead of your name.
- Does it contain poor grammar or spelling? This can be a sign that it is from a scammer.

Don't:

- click on any links
- open any attachments as they may download a computer virus
- use the contact details provided in the message, they could be fake.

Tax & Medicare scams

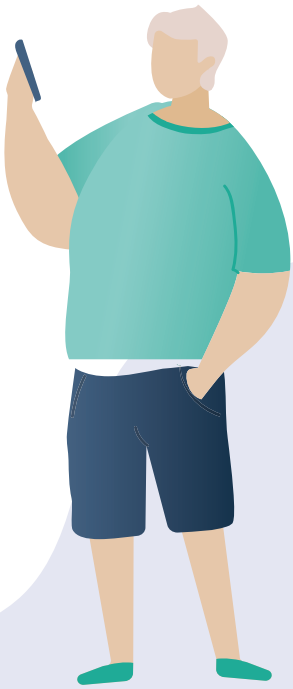
Scammers are impersonating the Australian Taxation Office, Medicare and other government organisations to gain money and personal information from victims through fake websites, emails, text messages and phone calls.

It's important to remember, the Australian Tax Office (ATO) will never:

- send you an email or text message asking for your personal information including your TFN, credit card or bank details
- ask for you to pay a fee to receive your tax refund, or to get out of being arrested for tax evasion
- send you an email with a link to an online service that asks for your personal details
- send you downloadable files or tell you to install software.

What can you do to be savvy and safe?

- Don't click on any links or download any attachments.
- Don't give out personal details such as your tax file number (TFN), date of birth, bank account or credit card details.
- If you are unsure whether a phone message is real, do not use the contact details provided, instead do an internet search for the organisation's number.
- Know the status of your tax affairs – is it likely that you are due a tax refund or owe payment?
- Log in to your official myGov account by manually typing the address instead of clicking a link.
- Check whether the email you have received is from the ATO's real address ending with @ato.gov.au
- Even if it looks like you are on the ATO or myGov website, check the address ends in .gov.au (instead of .com.au, .org.au or .net.au for example).
- Look out for poor grammar and spelling.
- Be suspicious of messages not directly addressed to you.



Romance and dating scams

Scammers are creating fake online profiles on social media or dating sites to make contact with victims. Their aim is to gain your trust before asking for money.

What can you do to be savvy and safe?

Look out for:

- people who express deep affections for you very quickly before asking for money, or a 'loan'
- people who avoid meeting face to face and make excuses as to why they can't travel to see you
- people whose online profile does not match what they have told you about themselves.

Do:

- check whether their images are really theirs or if they have been taken from somewhere else on the internet by doing a Google image search. 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'.

Don't:

- transfer any money to somebody you have only spoken to by phone or email
- send personal information such as your date of birth, bank or credit card details.

Tech support scams

These scams usually start with a call or email that appears to be from a large, well known organisation to tell you that you have a computer or internet problem and they can fix it.

What can you do to be savvy and safe?

- Don't provide remote access to your computer.
- Don't provide them with 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.

Large organisations expect you to call them when there's a problem with your internet or computer. They will not call you.

Help, I suspect I'm being scammed

If you think you have been 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 and stop any further payments to the scammer
- report the scam to the Australian Competition and Consumer Commission at scamwatch.gov.au - they can help you with further advice
- raise awareness. If there's anybody else you know who might be a victim, let them know.

If you are unsure whether a message you have received is really from the ATO, or you have been the victim of a tax related scam, call the **ATO Scam Hotline** on **1800 008 540**.

Keep up to date on ATO scams by visiting ato.gov.au/scams

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

Remember:

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

Scams are intended to take advantage of your good nature, but the internet can be a safe place to explore if you are careful about sharing personal information online, use common sense about who you send money to and keep your guard up.

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