Online presentation summary

Australian Government

Be Connected
Every Australian online.

Protect yourself against scams

Scammers are getting increasingly sophisticated in their attempts to get your money or personal details. Scams target people of all backgrounds, ages and income levels across Australia. Online scams are usually run by someone with a fake profile or business or they pretend to be from a well-known organisation. So, while the internet can be a wonderful place to explore, it pays to be cautious! Be alert and protect yourself from being scammed by following our tips.

Protect your personal information

Scammers pretend to be from organisations you know and trust like businesses you deal with, government agencies or a fraud service to try and get you to reveal important personal and financial information. They may contact you via a phone call, email, text, or through social media. Scammers will use your personal details to steal your money or commit another crime.

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

- verify who you are or update your details
- click on a link
- give them remote access to your computer
- pay a debt
- buy a voucher to pay a fine
- transfer funds or send money overseas.

Signs that it may be a scam

- 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.

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.

How to protect yourself

- Be alert to the fact that scams exist and always consider the possibility that a message, email or phone call may be a scam.
- Know who you're dealing with. If you are unsure if 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.
- Don't provide personal of financial information.
- Don't open suspicious texts, pop-up windows or click on links or attachments in emails – delete them.
- Don't respond to phone calls about your computer asking for remote access – hang up – even if they mention a well-known company such as Telstra.

Be careful when making friends online

Scammers contact people, usually via social media, a dating site, or even via an online game. They'll be very friendly and interesting and keen to build a friendship or relationship with you. Scammers can be surprisingly patient. The fake relationship might continue for weeks, or even a year, so they can gain your trust and ask you for money, personal information, intimate images or trick you into doing something illegal.

Signs that it may be a scam

Look out for people who:

- express deep affection quickly and contact you often
- can't meet in person, or ask for money so they can travel to meet you
- try and move you off the platform or app where you met to a more private communication channel, such as direct messaging or emailing
- claim to be financially stable but ask you for money
- tell you elaborate stories about financial troubles
- ask about your financial status
- become desperate, persistent, more direct or even aggressive when you don't send money
- seem to have inconsistencies in their stories and online profile – for example, their photo looks different to their description
- have spelling and grammar mistakes
- tell you they are working overseas (e.g. aid worker or working in the military).

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 an image search to help determine if they really are who they say they are. 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, inconsistencies in their stories.
- Don't agree to carry packages internationally or transfer money for someone else, as you may be committing a criminal offence.
- Don't share intimate pictures or videos. Scammers are known to blackmail their targets using compromising material.
- Stop all communication if a person starts asking you for a favour or money.
- Avoid any arrangement with a stranger that asks for a payment via money order, wire transfer, international funds transfer, pre-loaded card or electronic currency, like Bitcoin. It is rare to recover money sent this way.

Watch out for investment scams

Investment scams involve promises of big payouts, quick money or guaranteed returns. Always be suspicious of any investment opportunities that promise a high return with little or no risk.

Australians lose more money to investment scams than any other. They can be hard to spot, as scammers put a lot of effort into creating convincing stories and making professional websites and promotional materials. Before investing always seek independent legal advice or financial advice from a financial adviser who is registered with the Australian Securities and Investments Commission (ASIC).

Some of the most common ways investment scams can work include:

- contacting you via email or phone with a special opportunity to get a fast or guaranteed return
- using fake celebrity endorsements to make a scam seem legitimate
- convincing you to access your superannuation early or in a lump sum
- investment seminars (often via online video, Zoom, or similar) that are free or charge high attendance fees.

Superannuation

Superannuation scams offer to give you early access to your super fund, often through a self-managed super fund or for a fee. The offer may come from a scammer posing as a financial adviser.

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. For more information visit: moneysmart.gov.au/how-super-works/superannuation-scams

Share promotions and hot tips

Scammers may contact you by email, social media or post a message in a forum to encourage you to buy shares in a company they predict is about to increase in value. The message looks like an inside tip and will usually stress that you need to act quickly. The scammer is trying to get you to buy shares to boost the price of stock so they can sell shares they have already bought and make a huge profit. The share value will then go down dramatically.

Celebrity endorsement scams

Scammers use the image, name and personal characteristics of well-known celebrities without their permission to entice you into investing as it's being backed by someone you trust. These scams often appear as online advertisements or promotional stories on social media feeds or seemingly legitimate, trustworthy websites.

Warning signs of an investment scam

You are contacted out of the blue via phone call, text, email or social media message from someone offering unsolicited investment advice and they:

- use high pressure tactics, including contacting you repeatedly and pressure you to make a quick decision.
- promise low risks with high or guaranteed returns.
- don't have an Australian financial services (AFS) licence or say they don't need one.
- have an investment prospectus that isn't registered with ASIC.
- use celebrity endorsements or images: These are usually fake. Celebrities rarely discuss their investments or financial decisions in public.
- direct you to a fake website.
- try to stop you pulling out of the deal.

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 adviser and their company is registered via the ASIC website asic.gov.au/online-services/search-asic-s-registers/
  - you have checked ASIC's list of companies you should not deal with moneysmart.gov.au/companies-you-should-not-deal-with

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.