



SCAMS



HOW TO SPOT THEM AND STOP THEM

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. 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, 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.





Remember

Scammers pretend to be from organisations you know and trust like businesses you deal with, government agencies or a fraud service. They 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 usually have a small amount of information on you or something that can be vaguely linked back to you but they need you to fill in the blanks. The information they already have is usually information that is readily available, for example, things that you may have posted on your social media.

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; or
- Transfer funds or send money overseas.

Scammers are getting increasingly sophisticated in their attempts to get your money or personal details.

So, while the internet can be a wonderful place to explore, it pays to be cautious!





TYPES OF SCAMS



INVESTMENT SCAMS

If it sounds too good to be true, chances are it is!

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, 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; or
- Investment seminars (often via online video, Zoom, or similar) that are free or charge high attendance fees.

So please be aware of these tricks!





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.

