Investment scams

NICOLE HEALES FINANCIAL

Reduce the risk of investment scams

www.nicolehealesfinancial.com.au →

Be suspicious of anyone offering you easy money. Scammers are skilled at convincing you that the investment is real, the returns are high and the risks are low. There's always a catch.

If you think you've been targeted by scammers, act quickly.

How investment scams work

There are many ways investment scams may appear. Three main examples are:

- The investment offer is completely fake.
- The scammer is pretending to offer a legitimate investment but keeps any money given to them.
- The scammer says they work for a well known company that is offering a legitimate investment – but they're lying.

In any case, the money you 'invest' goes straight into the scammer's bank account and not towards any real investment. It is extremely hard to recover your money if it goes to a scammer based overseas.

Anyone can be scammed and every scam is different. Scams are often hard to spot and can feel legitimate in the moment. Scammers can use professional looking websites, advertisements and apps and impersonate legitimate companies.

Scammers are using deepfake technology to create fake celebrity videos promoting Quantum AI.

Quantum AI is a fake online investment program. It claims to use artificial intelligence (AI) technology and quantum computing to generate high returns for investors. Fake trading results are displayed on a website manipulated by scammers.

If you see a celebrity spruiking an investment, search online to see if the person has posted warnings about being impersonated.

Spot the signs of a deepfake video:

- The person speaks with unusual pauses, odd pitches or different accents.
- Mouth movements aren't in time with their speech.
- Facial expressions and movements don't match the speaking tone.
- The video is low resolution.

Do not click on any links promoting Quantum AI, or similar scams such as Immediate Edge and Quantum Trade Wave.

How scammers contact you

Scammers can come from anywhere. The most common approaches are:

- **Unexpected contact** – they may contact you by phone, social media, email or text message. They might pretend to be someone you know, such as your bank, financial adviser, fund manager, or even a friend. They'll offer guaranteed or unrealistic high returns on an investment.
- **Fake investment trading** – they use real investment trading platforms to set up fake accounts. Then they will help you trade via an account manager or offer to trade on your behalf. Once you deposit your money it's gone for good.
- **Fake investment comparison websites** – scammers will get you to enter your personal information into their fake website, then contact you to sell their scam investment.
- **Websites with fake ASIC endorsements** – slick websites with fake investing information and performance figures. They may claim to be endorsed or approved by ASIC, and may show the ASIC logo.
- **Dating apps** – using romance to form a relationship with you, then offering you an 'investment opportunity'. (This is also known as 'romance baiting').
- **Paid advertising** – scammers often pay big money for advertisements, to appear high in online search results. They also advertise through social media. Advertising a scam is illegal.
- **Fake news articles** – scammers will promote fake articles on social media or news websites, linking to their scam websites.
- **Deepfake celebrity endorsement videos** – scammers use a deepfake celebrity video to promote fake investments.

What scammers may offer you

A scammer may tell you they're offering:

- guaranteed, quick and easy investment returns and sometimes tax-free benefits
- investments in shares, cryptocurrency, mortgage, real estate or virtual investments, all with 'high returns'
- a (fake) trading platform to trade foreign currency, gold, options or futures
- commissions for building their client base and getting others to invest
- an opportunity with no risk or low risk, because you will:
  - be able to sell anytime
  - get a refund for non performance
  - have insured or 'guaranteed' transactions
  - be able to swap one investment for another
- inside information on initial public offerings or discounts for early bird investors, often falsely impersonating real companies to pitch their offer.

How scammers convince you

Scammers will look at the latest market and investment trends for opportunities. They often use well known company names, platforms, and terms (such as 'crypto') to lure investors in and appear credible.

This may include fake:

- crypto (virtual currency) investments
- trading companies, getting you to invest with them through real apps and trading platforms
- offers of inside information on public company floats, often naming ones that have been hyped in the media or on social media
- offers to get your money back from a sharemarket fall or previous scam
- references to well known Australian companies or regulators, often using the Australian Coat of Arms or Government logos
- offers to keep your money safe in well known Australian banks.

Beware of scammers offering investments or asking for payment using crypto. A legitimate financial services firm is unlikely to ask you for payment in crypto. Crypto-assets (for example, cryptocurrency) are largely unregulated in Australia and are high risk, volatile investments.

Payments made using crypto are very difficult to trace and recover.

Other tactics used by investment scammers

Operate from overseas

Investing in overseas companies or through brokers based outside Australia can be risky. If you invest and something goes wrong, you may not have access to important consumer rights and protections under Australian laws.

Convincing you not to pull out of the investment

They may try to swap your current investment for another one, convincing you the value will increase, or threaten you with legal action or fees.

A common tactic is to ask for 'insurance' or 'taxes' before funds invested can be released. This is just another method to extract more money from you.

'Pump and dump' scams

Scammers use social media and online forums to create fake news and excitement in listed stocks to increase (or 'pump') the share price.

Then they sell (or 'dump') their shares and take a profit, leaving the share price to fall. Any other investors are left with low value shares and will lose money. This may be market manipulation which is illegal.

Protect yourself from investment scams

Investment scams can look very convincing. It may be hard to tell if they're genuine investments or not.

Always use a licensed Australian financial services provider when you invest. Check they are listed on AFCA's financial firm directory, https://www.afca.org.au/make-a-complaint/findafinancialfirm.

Before you invest your money, check basic facts about what you are investing in and who with.

Banking and credit scams

If someone asks you to verify or give your personal details or offers you a loan, it could be a scam. Scammers can use your personal information to steal your money and run up debts in your name. If someone contacts you about an investment that you think could be a scam, report it to help warn others, https://moneysmart.gov.au/check-and-report-scams/report-an-investment-scam.

How banking and credit scams work

Scammers may target you online or on social media, by phone, text or email. Know what to look for so you can spot a scam and protect yourself.

Phishing scams

A scammer pretends to be your bank, internet provider, Government department, business, law enforcement, or even friends and family.

They may give you some information that seems genuine, such as personal details. This is to try to convince you they are who they claim to be and gain your trust.

The scammer may say there is a problem they need to fix. For example, an issue with your computer or online banking account, an overpayment or suspicious activity on your account.

The scammer could ask you to:

- verify or update your login details, passwords or other personal details
- confirm your banking details so they can give you a 'refund'
- supply them with banking verification codes
- click on a link they send you
- download software they provide
- give them remote access to your computer so they can 'fix' a problem (that doesn't exist)
- make a payment.

Signs of a phishing scam

- The email address doesn't match the company name or is from a free provider (such as hotmail, gmail or outlook).
- There are spelling mistakes or the information doesn't make sense.
- You're asked to take an action, such as click on a link, supply a code or download software.

While your bank may contact you if they suspect a suspicious transaction, they will never ask you:

- for sensitive information such as online banking passwords or codes
- to download software
- to transfer money
- to log in to online banking through a link sent via text or email.

Signs of a credit card scam

- There are unusual transactions on your credit card statement.
- Someone contacts you by phone, text or email and asks you to make an urgent credit card payment. They may claim to be a relative or friend.
- Or they could ask you to 'verify' your card details.

Check your credit card statements regularly, especially if your card is lost or stolen. If you see something you don't recognise, tell your bank straight away.

Loan scams

Scammers may contact you by email or text saying you're approved for a loan you never applied for. Or after you've filled out an online loan enquiry form.

Signs of a loan scam

- The loan seems too good to be true (for example, a really low interest rate).
- There's no credit check or you're guaranteed approval.
- They ask for an up front deposit or your bank details.
- They say the offer is ending soon and pressure you to act now.
- The lender claims to be from Australia but doesn't have a website or has an international phone number.
- The email address doesn't match the company name or is from a free provider (such as hotmail, gmail or outlook).
- They ask you to make a payment for insurance or tax before they can release the loan funds.

If you don't recognise the lender, check the company details online and read reviews. Check that it's not on the investor alert list, https://moneysmart.gov.au/check-and-report-scams/investor-alert-list.

What to do if you've been scammed

If you think you've been targeted by scammers, act quickly.

Call your bank as soon as possible to let them know about the scam.

Protect yourself against banking and credit scams

- Use strong passwords.
- Make sure your computer's antivirus software and operating system is up to date.
- Password protect all your devices. If you're using a shared or public computer, never save passwords and always log out of your accounts.
- Delete unsolicited or suspicious emails or messages straight away.
- Never click on any links.
- Go to your bank's website or their secure app to make a transaction.
- Shop on secure websites.
- Store your credit cards in a safe place.
- Avoid public WiFi.
- Shred letters from your employer, bank or super fund before you throw them out.
- Check the lender is licensed by ASIC, https://service.asic.gov.au/search/. Choose 'Credit Licensee' in the drop down menu when you search.

Scammers don't need your credit card to use it. They only need your card details.

They could get your card details if you put them into an unsecure website or use public WiFi or if your card is lost or stolen.

Superannuation scams

If someone offers to withdraw your super or move it to a self managed super fund (SMSF) so you can get the money, it could be a scam. Learn how to spot the signs of a super scam and what you can do to protect yourself.

If you've been affected by a data breach, contact your super fund to let them know. A scammer may have access to your accounts, including your super.

Spot the signs of a super scam

Scammers can target you online, by phone or email. They may use flashy advertising through social media or on websites.

Here are some ways a scammer could try to get your super.

Phishing scams for your personal details

A scammer contacts you pretending to be from a financial firm, such as a bank or super fund. They may use copied AFS licence details from a legitimate organisation to give you the impression they are genuine.

They ask for your personal or account details and may send an email with a link. When you click on the link, they will gain access to your computer, including your login details for other accounts.

With these details, a scammer can:

- create a super account in your name with another fund, or a fake SMSF, then transfer funds to this account and withdraw it
- use stolen myGov sign in details to gain access to your personal details and superannuation accounts.

Encourage you to open a self managed super fund

A scammer offers to help you 'control' your super by establishing a SMSF and transferring your super into it. They may:

- offer to help grow your super by investing with them in fake high return investments
- provide a fake investment performance app or computer program, showing false returns on your investments
- offer to 'do everything for you', advising there is no need to engage with anyone else as they will take care of it
- offer to invest your super in unusual investments such as cryptocurrencies or foreign currency bonds.

Scammers using this tactic may not be pushy and instead attempt to build trust with you over time. Eventually, they convince you to transfer your super into a SMSF or bank account that they control. They can then withdraw your super.

Offer to get access to your super early

Someone offers you a quick and easy way to access your super early, which may not satisfy a condition of release.

They may offer to help you fill out genuine documents needed to do this. This may include giving them your personal details to withdraw super from your fund or suggest transferring it into a SMSF, for a fee. They may tell you that after the paperwork is lodged, you can access the funds for personal use.

This process is illegal and you will end up paying additional tax and penalties.

Protect yourself from super scams

- Check your super balance regularly by logging into your account through your super fund's website.
- Look for any unusual transactions such as transfer requests or changes in personal details. If something doesn't look right, contact your super fund and ask them to check.
- Consider utilising multi-factor authentication if offered by your super fund or ask to 'password protect' your account.
- Make sure your super fund has an up to date mobile number, email and postal address for you.
- If someone contacts you claiming to be acting on behalf of your super fund, contact your fund to check.
- Know the rules about when you can legally access your super.
- If you're not sure about something, talk to a person you trust before you go ahead. This could be a family member, your accountant or financial adviser, or your super fund.
- Don't deal with anyone who is not licensed. You can check if someone is licensed on ASIC's Professional Registers Search, https://service.asic.gov.au/search/.

Take steps to stop indentity theft

There are simple steps you can take to help stop someone stealing your identity. For example, you can shred your personal documents, and be careful what you share on social media.

Of course, starting early can make a significant difference to your retirement lifestyle but even well planned decisions close to retirement can have a positive impact. Don't let procrastination or fear of the unknown deprive you of a financially secure, comfortable retirement.

Report a super scam

If you think you've been targeted by someone who is trying to access your super, report it to:

- Your super fund
- Scamwatch, https://www.scamwatch.gov.au/report-a-scam
- ATO – 13 10 20

Source: MoneySmart, August 2025

Capstone
FINANCIAL PLANNING

Get in touch with us, we're here to help.

0417 167 024
nicole@nicolehealesfinancial.com.au
www.nicolehealesfinancial.com.au →

Nicole Heales (T/A Nicole Heales Financial) is an Authorised Representative (No. 312479) of Capstone Financial Planning Pty Ltd. ABN 24 093 733 969. Australian Financial Services Licence No. 223135.