Broad Wealth Management

Creating Protecting Retiring

Protect yourself from Cyber Scams

Introduction

Personal cyber security is not just about changing settings, it's also about changing your thinking and behaviours.

Cybercriminals are known to use email, messages, social media or phone calls to try and scam Australians. They might pretend to be an individual or organisation you think you know, or think you should trust.

Their messages and calls attempt to trick you into performing specific actions, such as:

- Revealing bank account details, passwords, and credit card numbers,
- Giving remote access to your computer,
- Opening an attachment, which may contain malware,
- Sending money or gift cards.

How to recognise scam messages

It can be difficult to recognise scam messages. Cybercriminals often use certain techniques to trick you. Their messages might include:

- **Authority.** Is the message claiming to be from someone official, such as your bank?
- **Urgency.** Are you told there is a problem, or that you have a limited time to respond or pay?
- **Emotion.** Does the message make you panic, hopeful or curious?
- **Scarcity.** Is the message offering something in short supply, or promising a good deal?
- **Current event.** Is the message about a current news story or big event?

Unexpected money scams

There are different types of unexpected money scams, but they all promise the lure of some greater reward.

Unexpected money scams:

- usually promise you a significant share of a large sum of money, or other reward, in return for a small up-front payment
- request your personal financial details, and
- are also known as 'advance fee fraud' scams.

What to look out for

There are different types of unexpected money scams, but they all promise the lure of some greater reward, which could be:

- an unexpected lottery win
- an inheritance
- payment to assist with transferring money out of a country ('Nigerian' scams)
- a share in profits from a business investment.

Other signs to look out for:

- You receive an unexpected message by email, text message or other online method that promises an extraordinary reward or opportunity (for example, you've won a lottery that you don't remember entering or you're offered an unbelievably good business opportunity).
- You're told that you need to pay an up-front fee or provide personal details to receive a much greater reward.
- The email looks convincing and may use official looking letterhead and logos but it isn't addressed to you personally. The offer pressures you to make a decision quickly, and it may also contain spelling and grammatical errors.
- You're asked to provide your bank account details, copies of identity documents as verification and to pay a series of fees, charges or taxes to help release or transfer the money out of the country, through your bank.

Tips to protect yourself from money scams

There are a number of different things you can do to protect yourself:

- Understand that scams exist and use caution online. Be wary of messages that arrive out of the blue, whether on email, social media or other means. Remember there are no legitimate get-rich-quick schemes.
- Do an internet search using the names, contact details or exact wording of the message to see if it has been used as a scam on other people. Many scams can be identified this way.
- Don't open messages or click on links if you don't know the sender or if you're not expecting the message. Watch out for messages that promise you money or present hard luck or exotic stories offering you a share in millions of dollars.
- Use a spam filter to catch fake messages before they get to your inbox and delete spam that gets through without opening it.
- Don't accept friend or contact requests on social media from people you don't know. Scammers may use your information on social media, to make their messages more appealing or appear more genuine.

Anyone can be scammed and every scam is different. Scams are often very hard to spot and can feel legitimate in the moment.

Investment scams

If you're looking to invest money, make sure you're aware of the warning signs of investment scams online so you don't lose your hard-earned money.

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.

How investment scams work

There are three main types of investment scams:

- The investment offer is completely fake.
- The investment exists, but the money you give the scammer doesn't go towards that investment.
- The scammer says they represent a well-known company – 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.

Beware of scammers offering investments or asking for payment using crypto-assets (ie cryptocurrency). Crypto-assets are largely unregulated in Australia and are high-risk, volatile investments. Payments using crypto are very difficult to trace and recover.

How scammers get you to invest

1. The set up

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 fund manager, financial adviser, bank, 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 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 by showing the ASIC logo.

Dating apps

Using romance to form a relationship with you, then offering you an investment opportunity.

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, impersonating other news outlets and linking to their scam websites.

2. The offer

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'
- options trading or foreign currency trading
- 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 (IP0)* or discounts for early bird investors, often falsely impersonating real companies to pitch their offer.

3. The hook

Scammers will look at the latest 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-asset (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, often using losses resulting from the COVID-19 pandemic as bait.

**An IPO is when a company lists on a stock exchange and offers shares to the public for purchase. Also known as a float.*

How to spot an investment scam

The investment offer may be a scam if the person:

- does not have an Australian financial services (AFS) licence or says they don't need one
- constantly contacts you (phone calls or emails) and pressures you to make a quick decision
- uses the name of a reputable organisation to gain credibility (for example, NASDAQ, Bloomberg)
- has an investment prospectus that isn't registered with ASIC
- offers you very high investment returns

If you spot any of these signs, hang up the phone or delete the email. If you manage to record any of the scammer's details, report them to the Australian Securities and Investments Commission (ASIC).

Other tactics used by investment scammers

Operate from overseas

Overseas-based scammers target Australians because ASIC does not have international jurisdiction to prosecute them and they are very difficult to track down. They may ask you to deposit into different bank accounts every time you make a payment.

Investing in overseas companies can be risky. If you invest and something goes wrong, you won't be able to get help from ASIC.

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 out of victims.

'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.

How to check an investment is real

Ask questions and request information

Check the legitimacy of the person offering the investment by asking them:

- What is your name and what company do you represent?
- Who owns your company?
- Does your company have an AFS licence and what is the licence number?
- What is your address?
- Is your investing prospectus registered with ASIC?

If they try to avoid answering these questions, their investment offer is probably a scam. Hang up the phone, do not respond to the email. Stop dealing with the person or delete and block them if it's through social media.

However, even if they can answer these questions, it doesn't always mean the investment is legitimate.

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.

Tips to avoid investment scams

If you think you have encountered a scam:

- Talk about your concerns with a friend, family member or colleague. This can help you do a quick sanity check and reframe your thinking, because some scams work by playing on your emotions.
- Check the scam's legitimacy directly with the organisation it claims to be from, by using contact details sourced separately from the business' official website (and not using any contact details from the message itself).

Signs that often indicate it's a scam:

- It asks you to click on a link to 'confirm' your details.
- It's not addressed to you personally.
- There's a sense of urgency about the message.

In searching for a business's official website or other pages, have a look online for any reviews from other people that may confirm it's a scam.

You can also create a 'not sure' folder in your mailbox, where you drag suspicious messages to go through at a later time, perhaps with the help of someone you trust.

Remember some scams attempt to hijack your logical thinking by telling you to act urgently. Reframe your thinking by reviewing these messages the day or week after you receive them.

Help is available

If you think you've been scammed, don't feel embarrassed or helpless. Help is always available.

Follow these steps to protect yourself from further harm:

- Stop sending money to the company.
- Report it to your bank or financial institution.
- Be wary of falling for a follow-up scam or offers to recover your money.
- Report it to ASIC or your local police.
- Get support if you need it from Lifeline (13 11 14) or the National Debt Helpline (1800 007 007).

Contact us

If you have any further concerns, please feel welcome to get in touch.

Anthony Broad

Broad Wealth Management

PO Box 24

Waratah NSW 2298

P: 0431 062 243

E: anthony@broadwealth.com.au

Broad Wealth Management
Creating Protecting Retiring