Aussies are losing millions to financial scams: Here's how to spot one

Scams and cybercrime are booming in the wake of the COVID-19 pandemic, leaving thousands of people out of pocket. Investment scams in particular have surged, costing victims more than $26,000 on average.

What is an investment scam and why are they booming?

An investment scam involves being conned into parting with money on the promise of a good financial return. With more people than ever interacting online due to the pandemic, whole new sections of the community have become a target for scammers.

The ACCC says it appears to be increasingly difficult for people to identify legitimate investment opportunities from scams. Scammers no longer just rely on professional looking websites. They now have the ability to contact people through phone, apps, social media and other means.

In the past, people aged 45 to 64 were most likely to fall victim, with men targeted at twice the rate of women. However, scammers are now using new methods to target younger people, as well as minority groups and people with disabilities.

So far in 2021, the highest number of reports has come from those aged 25 to 44, while those aged over 65 years have lost the most money.

What is 'romance baiting'?

The ACCC says 'romance baiting' is a new form of scam that emerged last year targeting sections of the community who haven't typically fallen victim to investment scams.

In a romance baiting scam, victims are contacted on a dating app, typically moved off the app and then lured into an investment scam, often involving cryptocurrency.

Unlike traditional dating and romance scams, which tend to target older Australians, people aged 25 to 34 lost the most money ($7.3 million) to this new type of scam last year.

What does an investment scam look like?

Financial scams are often extremely sophisticated, featuring fake platforms, websites, phone lines and social media accounts. They can appear very legitimate, with scammers posing as financial professionals or 'experts.'

Here are a few things to look out for:

- The scammer may contact you repeatedly, encouraging you to make a quick decision or risk losing out.
- They may offer you quick returns, or a 'no risk' investment opportunity.
- Hot stock market tips or 'inside information' about shares that are going to increase in value are also common.
- Other scams involve invitations to investment seminars, or the ability to gain early access to your superannuation.

Victims are most commonly contacted by phone, email or online. Scammers may also reach out to you on social media, or by text message. On social media they may pose as someone you know or are connected to. They may post messages about 'hot investment opportunities' as comments on social media posts or in online forums.

Most people who lose money do so through bank transfers, which are impossible to recover. However, losses via cryptocurrencies like Bitcoin and other digital forms of payment are increasing, with $50 million lost last year.

How can I avoid being taken in by an investment scam?

Scammers are professionals and work very hard to convince you of their scam. So how can you validate whether an opportunity is legitimate?

Before handing over any funds or personal details, you should always:

1. Ask the name of the person you're speaking with, the name and address of their company, and whether the investment scheme is registered with ASIC.
2. Check the Financial Advisers Register on the Moneysmart website to see if the person you're speaking with is authorised to provide financial advice.
3. Ask for the company's Australian Financial Service licence number and verify it by checking the ASIC Connect Professional Registers.

4. Check ASIC Connect to see if an investment scheme is registered with ASIC. Investment schemes (generally those with more than 20 members) must be registered with ASIC and will have an Australian Registered Scheme Number that you can search.

5. You can also check the list of unlicensed companies you should not deal with on Moneysmart.

6. It's also worth checking the Financial Planning Association's Find a Planner tool to find out if the person is a registered practitioner member of the FPA.

To avoid becoming a target in the first place, be vigilant about your online (and offline) security. Don't open emails or accept friend requests online from people you don't know. Don't respond to messages about investment opportunities left in comments or in forums.

Always seek independent financial advice from a financial planning professional before making any investments.

What should I do if I've been scammed?

If you think you've been the victim of an investment scam, you can lodge a report of misconduct with ASIC.

If scammers have your credit card or bank account details, contact your bank or financial institution straight away. In some cases, they may be able to freeze a transaction or reverse charges fraudulently added to your credit card.

Source: Money and Life