

# Staying Safe Online – INVESTMENT SCAMS

An investment scam usually involves promises of big payouts, quick money or guaranteed returns.

## 3 Common Types of Investment Scams

**Cryptocurrency scams** – These scams generally encourage you to invest in digital currencies like Bitcoin. Scammers advertise or post on social media and offer great returns from cryptocurrency trading.

**Unsolicited investment advice** – Scammers often pose as stockbrokers or investment portfolio managers. They will call, email or contact you via social media offering financial or investment advice. They will offer low-risk investments that promise a high and quick return.

**Superannuation** – These scams offer to give you early access to your super fund, often through a self-managed super fund for a fee. The scammer will often pose as a financial adviser and ask you to agree to a story to ensure the early release of your money.

Then, acting as your financial adviser, they deceive your own superannuation fund into paying out your super benefits directly to them leaving you with nothing.

**STOP.  
THINK.  
CHALLENGE.**



### 3 warning signs

- 1 Contact comes out of the blue, from someone you don't know – you receive a call, email or message on social media from someone offering you advice you didn't ask for on investments. This often comes with high-pressure tactics – repeatedly contacting you, and telling you to act quickly and invest or you will miss out.
- 2 Use of a celebrity or high profile person as an endorsement – these are often fake, and their name and image are used without the individual's permission.
- 3 You are asked to deposit funds into different accounts for each transaction – scammers may claim this is for security reasons or because they are an international company.

### 3 ways to protect yourself

- 1 Get professional advice. That should be independent legal advice, or financial advice from a financial advisor registered with ASIC.
- 2 If it is cryptocurrency investment always speak with a qualified legal and/or financial adviser first.
- 3 Do your research and do not let anyone pressure you into an investment. Never commit to anything on the spot.
  - a. Check if a financial advisor is registered via the ASIC website. Any business or person that offers or advises you about financial products must hold an Australian Financial Services (AFS) licence.
  - b. Check ASIC's list of companies you should not deal with. If the company that contacted you is on the list – do not deal with them. Even if they are not on this list it could still be a scam.



**Be suspicious of any investment opportunity that promises you a high return with little or no risk – if something seems too good to be true, it probably is, and is likely a scam.**

## Think you've been scammed?



If you think you have been a victim of a scam it's important to call **Heritage on 13 14 22 (available 24/7)** promptly to limit any further loss and to see if the transactions can be reversed or disputed. If you are overseas please call +61 7 4694 9000.

**DO NOT** make further payments to the scammer.

Please ensure you change your passwords to secure your account and report the scam to [ACCC \(www.accc.gov.au\)](http://www.accc.gov.au) via the report a scam page. For more information on how to protect yourself from scam visit the [Scamwatch website \(www.scamwatch.gov.au\)](http://www.scamwatch.gov.au).



Go to our website to download more information about scams: [www.heritage.com.au/scams](http://www.heritage.com.au/scams)

**Heritage Bank**  
*People first.*