

An investment scam usually involves promises of big payouts, quick money or guaranteed returns. Always 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, then it probably is.

# How to spot an investment scam

An online contact that you've never met in person starts talking to you about investing.

Emails, websites or ads with testimonials or celebrity endorsements with exaggerated promises of big returns.

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.

The advisor who is helping you claims they don't need an Australian Financial Services (AFS) license.

You are asked to promote the scheme to friends and family to earn commission.

# How to protect yourself

- Never take investment advice from anyone you've met online, or provide them with personal or financial details.
- Verify the legitimacy of the individual and organisation you are working with using contact details you have sourced independently.
- Ensure the person who is trying to sell you a product or give you advice has an Australian Financial Services license.

- Confirm the address and contact details for the company match public listed directories.
- When considering a cryptocurrency investment, always speak with a qualified legal and/or a financial advisor first.

Scams continue to evolve and grow more sophisticated in their attempts to gain personal, banking information or access to devices. Remember to:



#### **STOP**

Take a moment to stop and assess the request. Most scams will aim to generate a sense of panic and urgency. Don't share personal or banking information if you're unsure.



## THINK

Ask yourself if the request makes sense. If you provide the requested information will you be granting access to your devices, accounts or money?



## **CHALLENGE**

Refuse to provide information, access and ignore requests. Hang up and call the organisation directly.

People's Choice will never contact you to request your passwords, VISA card/rediCARD or account details. We will not send you SMS containing links. Never share your password or Internet Banking login credentials.

If you have been contacted or are concerned about your privacy, please call us directly on 13 11 82 or visit a branch.

Scan the QR code to learn more about digital banking security.

