

## SOCIAL MEDIA

Be wary of advertisements found on social media offering investment opportunities. Scammers use these platforms to lure potential victims and direct them to fraudulent websites.

## HIGH RETURNS

Always be suspicious of any investment opportunities that promise a high return with little or no risk – if it seems too good to be true, it probably is!

## REMOTE ACCESS

Never allow anyone access to your device to assist with creating accounts. Remote access apps give scammers full access to your device allowing them to steal your money and personal information.

AVOIDING

# INVESTMENT SCAMS

Investment scams involve promises of big payouts, quick money, or guaranteed returns which eventually leads to having no further contact once they have your money.

## PERSONAL INFORMATION

Do not send copies of identification such as your driver's licence, passport, or Medicare card to people or businesses that you are unfamiliar with.

## SPELLING AND GRAMMAR

Beware of poor grammar and spelling. Legitimate companies will ensure professionalism on their website and in communications.

## CRYPTOCURRENCY

Scammers use cryptocurrencies because they are not easily recovered. Crypto can be sent overseas quickly with limited oversight.

If you are the victim of a cybercrime, make a report at [cyber.gov.au/report](https://cyber.gov.au/report) or attend your local police station.

Disclaimer: This publication contains only general guidelines and strategies for dealing with scams, and no guarantees or representations are made concerning their effectiveness. SAPOL accepts no responsibility for any injury or loss resulting from the application of these strategies.



SOUTH AUSTRALIA POLICE  
SAFER COMMUNITIES



Government  
of South Australia