Stay One Step Ahead:
Your Essential Guide to Scam Protection

Commonwealth Bank

National Seniors AUSTRALIA

Introduction

CommBank, in partnership with the National Senior Australia, is dedicated to raising awareness and preventing scams targeting seniors.

Scams and Fraud are evolving constantly and it's essential to stay informed to protect yourself and your finances. This guide will help you recognise common scams, learn how to avoid them, and understand what to do if you fall victim to one.

Types of Scams

1. Investment (including Crypto):

Scammers entice individuals with the promise of high returns, often involving crypto or other investment opportunities. Scammers may attempt to contact you via phone, email, or social media platforms.

Tips to protect yourself:

- If it sounds too good to be true, it probably is.
- Be cautious of unsolicited offers and pressure to invest or act quickly.
- Verify the legitimacy of the company or broker on the ASIC website first.

2. Business Email Compromise

Scammers can target businesses with emails from a compromised address, or emails made to look like they came from a trusted contact such as: your assistant, customer, lawyer, manager or supplier.

Tips to protect yourself:

- Before making first-time payments or a change of payment details, call the organisation on their official contact number to confirm the details first.
- Be wary of unsolicited requests for personal or financial information.
- Businesses are encouraged to train employees to recognise and report phishing attempts

PREVIOUS
NEXT

3. Remote Access

Where a scammer calls you and attempts to obtain access to your accounts or device, pretending to be from a trusted company or organisation.

Tips to protect yourself:

- Never download remote access software at the request or under pressure from a third-party caller.
- You can always call an organisation back on their legitimate contact details, found on their official website.
- Scammers can obtain your number fraudulently, so you may still receive scam calls even if you have a private number or are on the Australian Government's Do Not Call Register.

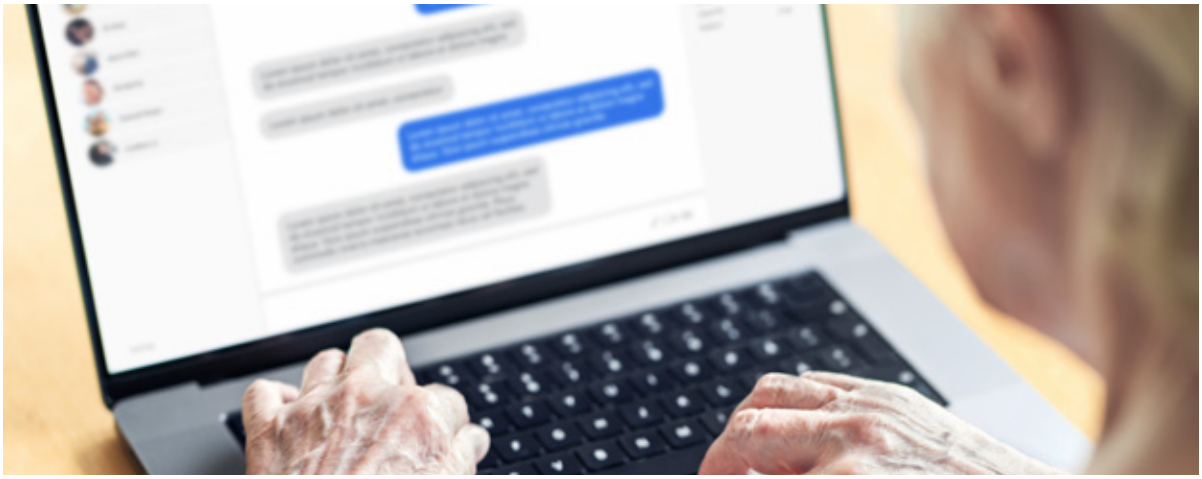
4. Phishing and Smishing

Scammers use deceptive emails or text messages that might include a link directing you to a fraudulent website or ask for sensitive personal information.

Tips to protect yourself:

- Don't click on links in suspicious emails or SMS.
- You can confirm the authenticity of a message by contacting the organisation directly, using their official contact methods available.
- Utilise multifactor authentication when you can.

PREVIOUS
NEXT



5. Relationship

Scammers create fake profiles to form relationships and manipulate victims into sending money or personal information.

Tips to protect yourself:

- Never send money to anyone you haven't met. Additionally, never share your card details or provide your physical cards, passwords, and PIN to anyone. Research your potential partner online via Google or social media apps. Try a reverse image search to identify if someone else owns the photos you've been sent.
- Speak to your family and friends about your online relationship. They may be able to offer perspective and identify warning signs that you may not have noticed

6. Employment Opportunity

Where a job offer appears to require little to no effort for a high financial gain, or promises to make quick money

Tips to protect yourself:

- Verify the company and offer through official channels and do research on the company to ensure they are legitimate and currently trading.
- Be wary of job offers via social media, encrypted chat, email, phone or letter from people you haven't met or companies you don't know.
- A legitimate company would never require you to make an advance payment or use your personal banking information to facilitate company funds or trade

PREVIOUS
NEXT

7. Online Shopping

Scammers create online stores or ads to lure shoppers into purchasing non-existent or fake products.

Tips to protect yourself:

- Shop only on reputable and secure websites and be wary of any offer that seems too good to be true.
- Use secure payment methods and avoid direct transfers to sellers.
- Don't rush or be pressured by 'limited offers' or end of sale 'countdowns'.

8. Threat and Penalty

Scammers impersonate authorities or trusted organisations to extort money through threats of fines or legal action.

Tips to protect yourself:

- Hang up on threatening callers and contact the organisation directly.
- A legitimate organisation will never ask you to pay by unusual methods such as by gift or store cards, iTunes vouchers, wire transfers or Bitcoins.
- If you're concerned for your safety, contact the police assistance line.

PREVIOUS
NEXT

Password and Personal Information:

Never share passwords or PINs and be cautious when sharing personal information. Your financial institution will never ask for your login passwords.

Avoid anything that can be easily guessed such as your address or birthday, or common quotes and phrases.

Make them unique – reusing a password multiple times makes it less secure, as it only requires one breach to compromise all the accounts with the same password

Create strong passwords and change them regularly. For tips on password creation and to test the strength of your password, visit Passwords | NSW Government

Remember if you are confronted with any of the mentioned scams to:

1. Stop. Check. Reject.
2. Stop. Does something seem off? If in doubt, the best thing to do is stop. Take a breath.
3. Check. Ask someone you trust or contact the organisation directly, using their official details.
4. Reject. Hang up on the caller, delete the email, block the phone number. Change your passwords.

PREVIOUS
NEXT

What to do if have been scammed:

If you've fallen victim to a scam and lost money or personal information, you are not alone. Every year countless Australians experience similar situations.

There are a few important things you should do straight away to limit the damage and protect yourself from further loss.

1. Stop all communications with the suspected scammer
2. Act fast to prevent loss! Contact your bank or card provider immediately to report the scam.
3. If you believe your personal information has been compromised contact IDCARE on 1800 595 160 or visit their website to find out more.
4. Report the scam to help others avoid falling victim in the future. You can report to scam reporting bodies such as Scamwatch and ReportCyber.

PREVIOUS
NEXT

Stay one step ahead of scammers by arming yourself with knowledge and taking proactive measures.

Everyone has a part to play in shutting down criminal scammers. By talking to each other, we can make sure no one is alone in the fight against scams. Remember, spreading awareness is the first line of defence against scams and fraud.

Visit Commbank Safe to learn more on how to spot and protect yourself from scams and fraud.

Visit the website

PREVIOUS

NEXT

National Seniors Australia
ABN 89 050 523 003

GPO Box 1450,
Brisbane QLD 4001

P: 1300 76 50 50
E: general@nationalseniors.com.au

1300 76 50 50 **nationalseniors.com.au**

National Seniors AUSTRALIA

0720245664STP