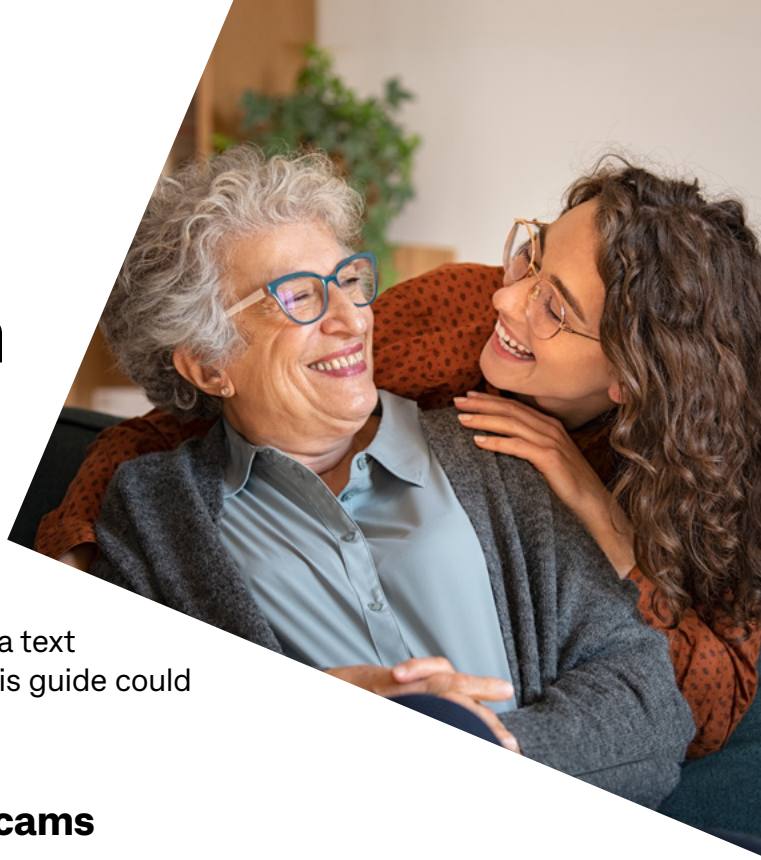
Have a conversation with your loved ones about scams.



Whether it's a suspicious phone call or a dodgy link in a text message, a simple conversation about scams using this guide could be key to helping keep your loved ones safe.

Step 1: Explain the common types of scams

Romance or relationship scams

Scammers gain your trust by developing a relationship that seems genuine. Often meeting online, you may believe you're speaking with a romantic partner, friend, or relative. However, their true goal is to steal money or personal information.

Tip: Never send money or gifts to someone you've only met online and never show yourself on camera - be on alert!

Impersonation scams

Scammers may pretend to be from organisations like banks, technology companies or government agencies. They might call, email or even visit your house in person, asking for identification documents, cards, cash, PINs, passwords or cheque books.

Tip: CommBank will never ask you to provide your passwords or NetCodes.

Investment scams

Scammers entice you with the promise of high returns, often involving cryptocurrency, term deposits, bonds or other investment opportunities.

Tip: If an investment opportunity seems too good to be true – it probably is. If you're unsure, double check with someone you trust, like close family or friends.

Remote access scams

A scammer may contact you, pretending to be from a well-known company and then attempt to access your accounts or device. They usually ask you to download software on your computer or mobile device so they can gain control.

Tip: If you receive an unexpected phone call, text or email asking to provide remote access to your device, hang up or delete the message immediately – even if they mention a well-known company.

Step 2: Share the common tricks scammers use

Tricks scammers use	Tips and what to look out for
They create a sense of urgency	• An urgent call to action, such as asking you to verify an account, transaction or make a payment. • Always be cautious about clicking on links in an SMS or email.
They pretend to be someone you trust	• An unexpected phone call or message claiming to be from a reputable company like a bank, telco or even a family member or friend. • Never trust a call or message asking for sensitive information, payments or access to your devices.
They ask for money or payments in an unusual way	• Be wary of any request to pay for something with cash, gift cards or through money transfer businesses.
They trick you in to providing sensitive personal information	• Look out for emails or messages that contain links to provide personal information like your banking info, card numbers or identity details.

Step 3: Explain some simple ways to stay safe

1. Stop

Does a call, email, text or person seem off? The best thing to do is stop. Take a breath. Real organisations won't put you under pressure to act quickly.

2. Check

Ask someone you trust to get a second opinion or contact the organisation the message claims to be from. If available, always use a trusted method to contact the organisation (for example: the CommBank app).

3. Reject

If you're unsure; hang up on the caller, delete the email or text, block the phone number and change your passwords.

Step 4: Share what to do if your loved one thinks they have been scammed

- Stop all communications with the suspected scammer immediately.
- Change your passwords, PINs and lock your cards in the CommBank app or NetBank.
- Contact us on 13 2221 as soon as possible, or message us securely in the CommBank app 24/7.

CommBank is committed to helping keep our customers safe from scams and fraud.

More resources are available at **commbank.com.au/scam-tips**

CommBank Safe

008-144 050325