

# Talking about scams to **help protect your loved ones**

Whether it's a suspicious phone call or a dodgy link in a text message, a simple conversation about scams using this guide could help you uncover red flags you might otherwise miss and stop a scam in its tracks.

## 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:** Verify before you act. Contact the organisation via their official website or app.

### 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.

## Common tricks scammers use

| Tricks scammers use | Red flags to look out for |
|---|---|
| **Pressure to act quickly.** | Urgent requests to verify, click a link or make a payment. |
| **Unexpected contact.** | Receiving unexpected emails, messages, or phone calls from unknown sources, especially if they ask for personal information. |
| **Requests for money in unusual ways.** | Being asked to pay using gift cards, cash or transfers. |
| **Requests for personal or banking details.** | Emails, texts or calls asking for personal information like your banking information, card numbers or identity details. |

## Easy ways to start the conversation



**Not sure what to say? Try:**

"This feels off, what do you think?"

"Can I check this with you before I do anything?"

"Does this sound legitimate to you?"

"Someone's asking me to move money quickly. Can I talk it through with you?"

"I received a suspicious message. Can you help me check it?"

**You don't need to have all the answers. Talking it through can help you spot red flags.**

## What to do if you or a loved one has been scammed

- Stop all communications with the suspected scammer immediately.
- Change passwords, PINs and lock 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.

If something doesn't feel right, remember:

**Stop. Check. Reject.**





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

Commonwealth Bank of Australia ABN 48 123 123 124 AFSL and Australian credit licence 234945.