THE COMPLETE GUIDE

Scam-Proof Your Parents

...and yourself

Protect their money, identity and independence — with one calm habit you can set up together over a cuppa.

STOP **CHECK** **CALL**

WHAT'S INSIDE

01 **12 scams to recognise**
From fake investments to AI voice clones

02 **Talking without lecturing**
Including when they don't believe it's a scam

03 **The 15-minute phone checklist**
Plus stronger protection for later

04 **If it's already happened**
Exactly what to do, by what was lost

05 **Three practice exercises**
Rehearse it together before it's real

06 **Fridge card and contacts**
Every trusted Australian number in one place

Figures: National Anti-Scam Centre, Targeting Scams 2025 · Updated October 2026

WHY THIS MATTERS

Scams don't prey on a lack of intelligence. They prey on trust.

Your parents grew up in a world where a polite caller was usually who they said they were. Where the bank knew your name. Where you helped someone who sounded worried.

Scammers know this. They borrow a trusted name, then add a rush: **act now, or something bad happens.** Under pressure, anyone can be caught out — doctors, lawyers, tech workers and grandparents alike.

So this isn't about making your parents "better with technology". It's about giving them one simple habit: **pause, then check.**

THE AUSTRALIAN PICTURE, 2025

$88.8m
lost by Australians aged 65+, as reported to Scamwatch

26.5%
of all Scamwatch losses — though people 65+ are about 17% of Australians

$50.8m
of that came from investment scams — the costliest type for people 65+

$2.18b
reported lost by all Australians across five reporting agencies

Source: National Anti-Scam Centre, Targeting Scams 2025 (March 2026). The $88.8m is part of the $2.18b, not extra. Many scams are never reported, so real losses are higher.

The biggest losses don't come from dodgy texts. They come from **fake investments, people pretending to be the bank, and slow-building online friendships**. This guide covers all of them.

This guide is

A short, kind plan you can do together over a cuppa this weekend.

This guide isn't

A way to take over their phone, their money or their choices.

HOW SCAMS WORK

Every scam, whatever the story, uses the same three tricks

1. They pretend to be someone you trust

Your bank, myGov, the ATO, Australia Post, a grandchild, a well-known celebrity. The name, logo and even the phone number can all be faked.

2. They create a rush

"Within 24 hours." "Don't hang up." "Your account will be closed." A deadline stops you from thinking and checking.

3. They stir up strong feelings

Fear (fraud, fines, arrest), excitement (big returns, a prize), love or worry for family. Strong emotions push careful thinking aside.

Then comes the ask: keep it secret, move money, pay in an odd way (gift cards, crypto, a "safe" account), share a code, or let someone onto your device.

FOUR MYTHS TO RETIRE

"Scams are full of spelling mistakes."
Many are now flawless — often written with AI tools.

"It showed my bank's real number."
Caller ID can be faked. So can text message names.

"It was my grandson's voice."
Voices can be copied from a short clip online.

"I'd never fall for one."
Confident people check less. Everyone needs the habit.

The one rule that beats them all

Never act on the contact you received. Hang up or close it, then reach the person or company **yourself** — using a number or app you already trust.

Scams that go after savings

1 Investment and super scams BIGGEST LOSSES 65+

"Our clients are earning 18% guaranteed. Your account dashboard already shows a profit — just top up to unlock withdrawals."

Red flag Guaranteed or high returns, pressure to move super, a slick app showing profits. A fake dashboard is not proof real money exists.

What to do Check the company on Moneysmart's Investor Alert List and the adviser on the Financial Advisers Register. Talk to family first.

2 The fake bank "fraud team"

"This is your bank's fraud department. Your account has been compromised. Move your savings to this safe account while we investigate."

Red flag A "safe account", a request for a code sent to your phone, or being told to keep it from bank staff.

What to do Your bank will never ask you to move money to keep it safe. Hang up and call the number on the back of your card.

3 "Our bank details have changed"

"Hi, it's the builder. Please note our new account for the final payment — the old one is closed."

Red flag New payment details by email or text, even in a real conversation with a real business.

What to do Before paying, ring the business on a number you already had — not one in the message.

4 Romance and online friendship

"I feel like I've known you forever. My uncle taught me a crypto strategy — let me help you try it. Just between us for now."

Red flag Feelings move fast, they can never video call or meet, then a money problem or an investment tip.

What to do Never send money to someone you haven't met in person. Shame keeps people quiet, so lead with kindness.

Scams that pretend to be someone you trust

5 myGov, Centrelink, Medicare or the ATO

"myGov: your account is suspended due to unusual activity. Verify your details within 24 hours: mygov-verify.au"

Red flag A link to sign in, threats of fines, arrest or cancelled payments, or a demand to pay a tax debt now.

What to do Don't tap the link. Open the myGov app or type my.gov.au yourself. Unsure? Call Services Australia or the ATO (page 15).

6 "Mum, it's me" — family emergencies

"Hi Mum, I dropped my phone in the sink, this is my new number. Can you help me pay a bill today? I'll pay you back."

Red flag A new number, an urgent payment, a reason they can't talk. On calls, the voice may sound exactly right — it can be AI.

What to do Don't reply to the new number. Call your family member on the number you've always had.

7 Remote "tech support"

"We've detected hackers on your internet. Please download AnyDesk so our technician can fix it while you log in to your bank."

Red flag An unexpected call or pop-up about a virus, a request to install an app, or to open banking while they watch.

What to do Hang up. Never give an unexpected caller control of your phone or computer. Close pop-ups and restart.

8 Parcels, tolls and fines

"AusPost: your parcel is on hold. Pay a $2.95 redelivery fee to release it." · *"Unpaid toll — pay today to avoid a $250 penalty."*

Red flag A small fee with a link. The real goal is your card details.

What to do Open the official app or website yourself and check there. If nothing is waiting, delete the text.

Scams in everyday life and online

9 Fake ads and celebrity endorsements

A video on Facebook shows a well-known TV presenter saying "This is how I built my retirement fund. Spaces close tonight."

Red flag Famous faces promising easy money. Videos, voices and reviews can all be made with AI.

What to do Celebrities don't sell investments in ads. Don't click or fill in a "call me back" form.

10 Online shopping and Marketplace

"I'll take the armchair! I've paid you through PayID — just pay the $50 upgrade fee shown in this email so the money releases."

Red flag Prices too good to be true, a buyer who won't come in person, "payment confirmation" emails, fees to release money.

What to do Check your own bank app — not an email — to see if money arrived. Meet in person and pay on collection.

11 Charity and door-to-door

"We're collecting for the flood victims. Could you donate by card right now? Every minute counts."

Red flag Pressure to give on the spot, no ID, a charity name you can't find.

What to do Say "I'll donate online". Look the charity up on the ACNC Charity Register and give through its own website.

12 "We can get your money back"

"I'm a lawyer working with the police. We've traced the funds you lost. Pay a $900 release fee and we'll return everything."

Red flag Contact after a scam, offering recovery for an upfront fee. They often already know what happened.

What to do Real help is free: your bank, IDCARE and the services on page 12. Never pay to recover money.

AI AND MODERN SCAMS

Seeing and hearing is no longer believing

New tools let scammers copy voices, faces and websites cheaply. The fix isn't spotting the fake — it's checking through a second, trusted route.

Copied voices

A few seconds of someone's voice from a video can be enough to fake a phone call that sounds just like them.

→ Hang up and call them back on their usual number.

Fake videos and photos

Celebrities, news readers, even "investment experts" can be made to say anything on screen.

→ Treat any video selling money-making as an ad, not news.

Perfect copycat websites

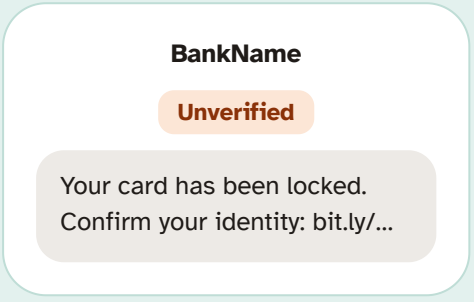
Fake bank, shop and government sites can look identical, and may appear at the top of search results as ads.

→ Use saved bookmarks or the official app.

Faked numbers and names

A call or text can display your bank's real number or name, and sit in the same thread as genuine messages.

→ Who it says it's from proves nothing.



NEW IN AUSTRALIA FROM JULY 2026

Texts may now be marked "Unverified"

Under Australia's SMS Sender ID rules, a text using a business name that isn't registered can be labelled **Unverified**. Treat it with extra suspicion — but remember a text *without* the label can still be a scam, and the label doesn't apply in WhatsApp, iMessage or Messenger.

Our family check: if a call, video or message asks for money, codes or access, we confirm it through a different route — every time, even when it seems real.

STARTING THE CONVERSATION

Talk with them, not at them

Your parents have handled far bigger things than a dodgy text. Treat this as swapping notes, not a lecture.

OPENERS THAT WORK

"I got the strangest text this week. Have you had any like this?"

"A friend at work nearly got caught by one. Can we set up a few things on both our phones?"

"If anything ever feels off, ring me. You'll never be bothering me."

"Shall we agree how we'll check it's really us if one of us asks for money?"

TRY NOT TO SAY

✕ "You need to be more careful."	✓ "These are getting really convincing."
✕ "Give me your phone, I'll do it."	✓ "Want me to show you, or shall we do it together?"
✕ "How could you fall for that?"	✓ "I'm glad you told me. Let's sort it out."

When they don't believe it's a scam

Investment and romance scams build real trust over months. Arguing usually pushes people closer to the scammer. Instead:

1. **Stay curious.** "Tell me about them. How did you meet? What have they promised?"
2. **Suggest one check, not a verdict.** "Before sending more, shall we look them up on Moneysmart together?"
3. **Ask for a pause.** "Could we wait a week and see if they're still happy?" Real friends and investments can wait.
4. **Bring in a neutral voice.** Their bank, a financial counsellor or Scamwatch's family resources.

DO IT THIS WEEKEND

The 15-minute phone checklist

Sit side by side and let them hold the phone. Tick each one off as you go.

Bank and money

- [ ] **Save the bank's real fraud number** in Contacts, copied from the back of the card or the bank's official website.
- [ ] **Turn on bank alerts** for every payment in the banking app, so surprises show up straight away.
- [ ] **Agree the code rule:** a code sent to your phone is never read out or shared with anyone — not even "the bank".

Phone safety

- [ ] **Check there's a screen lock** — a PIN, fingerprint or face unlock.
- [ ] **Turn on automatic updates.** iPhone: Settings › General › Software Update. Android: Settings › System › Software update.
- [ ] **Look through installed apps together.** Remove any they don't recognise, especially remote-access apps like AnyDesk or TeamViewer.

Calls and texts

- [ ] **Turn on spam call and text filtering.** iPhone: Settings › Apps › Phone, and Messages. Android: Phone app › Settings › Caller ID & spam. Check it won't hide calls from the doctor or hospital.
- [ ] **Optional: join the Do Not Call Register** at donotcall.gov.au. It's free and cuts telemarketing, but scammers ignore it — it's not fraud protection.

Family plan

- [ ] **Save your number as "Family — call me first"** so it's easy to find in a hurry.
- [ ] **Agree on a trusted person** to ring before any unexpected payment, and a **family safe word** as an extra check (written somewhere private, not on the phone).

Done? Brilliant. When you have another hour, page 10 adds stronger protection for email, myGov and banking.

WHEN YOU HAVE AN HOUR

Stronger protection for the accounts that matter

Email is the master key — whoever controls it can reset almost every other password. Start there.

Meet passkeys: sign in with your face or fingerprint

A passkey replaces the password with the phone's own lock. There's nothing to type, so nothing a scammer can trick you into giving away. myGov, Google, Apple and Microsoft all offer them.

Accounts

☐ Add a passkey or two-step verification to **email** first

☐ Set up a **passkey for myGov** and review its sign-in options

☐ Use a different password for every account — a **password manager** makes this easy

☐ Check recovery phone and email are current

Banking

☐ Ask the bank about **daily transfer limits** that suit how they bank

☐ Ask about extra checks for **new payees** and large payments

☐ Remove old cards and payees no longer used

☐ Consider naming a **trusted contact** with the bank, if offered

Devices

☐ Turn on **automatic backups** (iCloud or Google)

☐ Turn on **Find My** so a lost phone can be locked

☐ Check which apps can control the screen or read messages

☐ Update the home computer and Wi-Fi router too

Privacy

☐ Set Facebook and other profiles to **friends only**

☐ Hide birthday, phone number and address from public view

☐ Be careful with posts about travel plans and grandkids' names

☐ Fewer public voice videos means less to copy

Based on the Australian Cyber Security Centre's Personal Cyber Security Handbook and myGov security advice. Menu names vary by phone and bank.

IF IT'S ALREADY HAPPENED

Act fast. Start here.

First, take a breath. It isn't their fault, and acting within hours makes the biggest difference.

1

Stop all contact

Hang up, stop replying, send nothing more — even if they threaten.

2

Call the bank now

Use the number on the card. Say "I've been scammed" and ask what they can stop.

3

Keep the evidence

Screenshots, numbers, receipts, dates. Don't delete the messages.

THEN, DEPENDING ON WHAT HAPPENED

Money was sent	Ask the bank's fraud team to try to recall the payment, freeze accounts and open a scam case. Note the case number.
Card details were shared	Block the card in the banking app or by phone, order a new one and check recent transactions.
A password or code was shared	Change that password (email first), sign out other devices, and turn on a passkey or two-step verification.
Someone controlled the device	Turn off Wi-Fi and data, remove the remote-access app, and change passwords from a different, trusted device. Get trusted help to check it.
ID documents were shared	Call IDCARE (1800 595 160) and the organisation that issued the document. Ask about a ban on your credit report.
They're still in touch	Stop payments and replies. If there are threats, call police on 131 444, or 000 in an emergency. Watch for "recovery" offers (scam 12).

Report it at scamwatch.gov.au to warn others, and at cyber.gov.au (ReportCyber) if money or identity was taken.

Be gentle afterwards. Embarrassment stops people speaking up next time. Thank them for telling you.

IN THE DAYS AFTER

Getting help with money and identity

If the bank says no to a refund

STEP 1

Complain to the bank in writing

Ask for its formal complaints team. Include the scam case number and your timeline.

→

STEP 2

Not happy? Go to AFCA

The Australian Financial Complaints Authority is free and independent: afca.org.au

Since March 2026, AFCA can look at some scam complaints against the bank that *received* the money, not just your own. It can't promise a refund, but it's worth asking.

If personal details were taken

IDCARE — 1800 595 160

Free, one-on-one help making a recovery plan after identity theft.

Ban your credit report

Ask a credit reporting agency for a ban so no one can borrow in your name.

myGov, Centrelink, Medicare

Services Australia Scams and Identity Theft Helpdesk: 1800 941 126.

Passport or licence

Contact the issuing agency to report it and ask about a replacement.

Who does what

Scamwatch	Collects reports to warn others and disrupt scams. It can't recover money.
ReportCyber	Sends cybercrime reports to police.
Your bank	The only one who can try to stop or recall a payment.
Police	131 444 for threats or harassment · 000 in an emergency.

Look after the person, too. Losing money to a scam can bring shame, grief and sleepless nights. Free support: **Lifeline 13 11 14** · **National Debt Helpline 1800 007 007** for financial counselling.

PRACTISE TOGETHER

Rehearse it before it's real

Like a fire drill: a few minutes of practice makes the right move automatic under pressure.

A **The urgent call · 5 minutes**

One of you rings pretending to be a grandchild in trouble who needs money today. The other practises saying **"I'll call you right back"**, hanging up and ringing the real person on their saved number. Swap roles.

B **Spot the fake · 5 minutes**

Look at three recent texts or emails together. For each, ask: *Who says it's from? What does it want me to do? How would I check without using its link or number?*

C **Check an investment · 10 minutes**

Visit moneysmart.gov.au together. Search a company name on the Investor Alert List and an adviser on the Financial Advisers Register. Remember: not being on the warning list doesn't prove it's safe.

Our family verification plan

If someone asks for money, we call: _____

Before any payment over $ _____

...we check with: _____

We never share: **Codes sent to our phones, passwords, or remote access**

Our safe word is kept: _____

A safe word is a back-up, not a replacement for calling back on a known number.

Print this page and stick it on the fridge, near the phone or by the computer.

Before you click, pay or share:

STOP

Don't do anything yet. A real company will wait.

CHECK

Is someone pretending? A rush? Strong feelings? An odd way to pay?

CALL

Hang up, then ring family or a number you already trust.

Never share a code sent to my phone. Not with anyone. Not even the bank.

If in doubt, call: _____

Phone _____

My bank's fraud line _____

IDCARE (free) **1800 595 160**

Nobody real will ever be cross with you for checking.

KEEP THIS PAGE

Trusted Australian contacts

These numbers and websites are the real ones. Save them now, so you never need to search in a hurry — scammers buy search ads too.

Your bank	Stop or recall payments, block cards	**Back of your card**
IDCARE	Free identity and cyber support	**1800 595 160**
Services Australia	myGov, Centrelink and Medicare scams	**1800 941 126**
ATO	Check if contact from the ATO is real	**1800 008 540**
National Debt Helpline	Free financial counselling	**1800 007 007**
Lifeline	24/7 crisis and emotional support	**13 11 14**
Police	Threats or harassment · emergencies	**131 444 · 000**

Websites worth bookmarking

scamwatch.gov.au
Report scams, see current alerts, help a family member

cyber.gov.au
ReportCyber and the Personal Cyber Security Handbook

moneysmart.gov.au
Investor Alert List and Financial Advisers Register

afca.org.au
Free complaints when the bank says no

acnc.gov.au
Check a charity is registered before giving

beconnected.esafety.gov.au
Free online safety lessons for older Australians

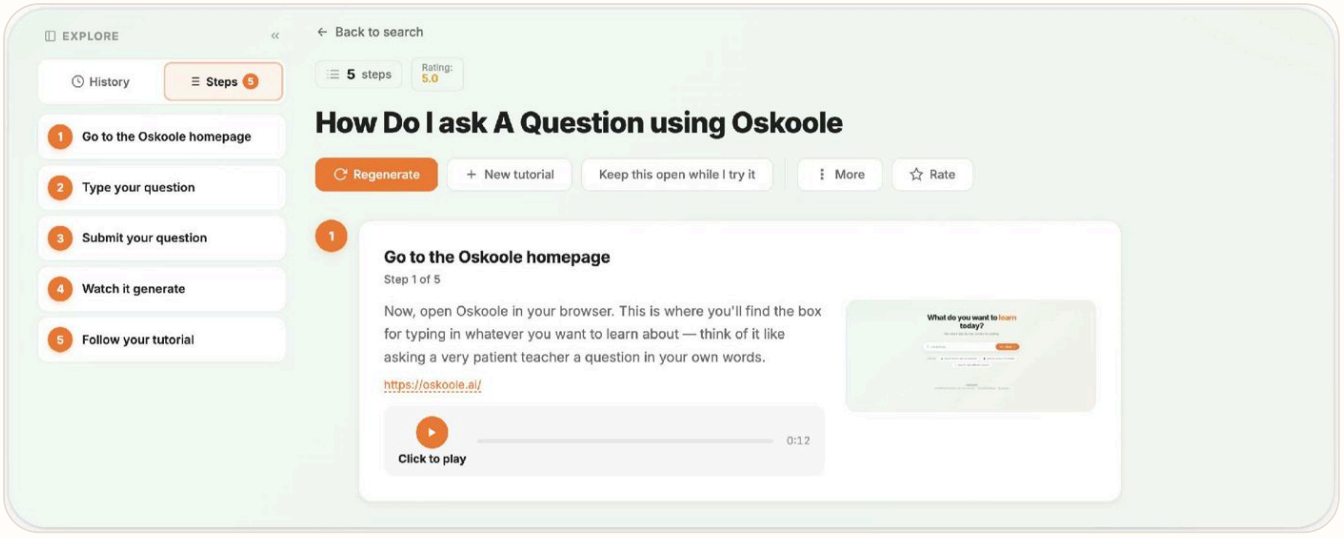
Numbers checked October 2026. Services can change — if a number doesn't work, find it on the organisation's official website.

Oskoole.ai

You can't be there for every message. Oskoole can.

Oskoole helps older Australians learn technology at their own pace. Your parents type a question in their own words, like **"How do I turn on bank alerts?"** or **"Is this text a scam?"**, and get a clear, step-by-step answer read out loud — in 76 languages.

They can ask any time, as often as they like. No one to bother, and no question too small.



Use it to learn, then still check. Oskoole can explain warning signs and walk you through settings, but it can't confirm whether a specific message is genuine. When money is involved, STOP, CHECK, CALL. And never type passwords, codes, card numbers or ID details into Oskoole or any AI assistant.

Try your first 3 questions free

oskoole.com

No card needed to start. After that, $9.99 a month. Prices in Australian dollars, including GST.