Spotting scams before they cost you

Who this is for: older Australians and the families who worry about them
Reading time: about 6 minutes
In one line: every scam, no matter how sophisticated, relies on the same three pressures, and all three can be beaten with one habit.

Let us start with the facts, because they are confronting. Australians reported more than two billion dollars in scam losses last year, and people over 65 carry a far bigger share of those losses than their share of the population. Scammers target older Australians deliberately. Not because older people are foolish, but because they are more likely to answer the phone, more likely to be polite to strangers, and more likely to have savings worth stealing.

So if you have ever been targeted, you are not gullible. You are on a list, along with practically every other adult in the country. The goal of this guide is to make sure being on the list never costs you anything.

The three pressures behind every scam

Scams change costumes constantly. The Tax Office one becomes the toll road one becomes the parcel delivery one. Underneath the costume, every scam applies some mix of three pressures:

Urgency. Something terrible will happen right now unless you act. Your account will be closed, a warrant issued, your grandson left stranded. Urgency exists for one reason: to stop you thinking and checking.

Authority. The message claims to be from someone you would normally obey or trust. The bank, the police, the ATO, Microsoft, your energy company, even a family member.

Secrecy. You are told not to tell anyone. The "investigation" is confidential, the surprise will be ruined, the family should not be worried. Secrecy exists to keep you away from the people who would spot the scam in five seconds.

When two or three of these arrive together, the alarm should be deafening. Real organisations almost never combine them. Your actual bank does not ring you, demand immediate action, and ask you to keep it secret. Only scammers do that.

The big ones doing the rounds

The bank impersonation call. Someone from your bank's "fraud team" says your account is compromised and you must move money to a "safe account". This is the most expensive lie in Australia. Banks never ask you to move money to keep it safe. Never. Hang up and call the number on the back of your card.

Remote access. A caller from "Telstra", "NBN", or "Microsoft" needs to fix a problem with your computer and asks you to install something so they can help. The software gives them control of your machine, and then your banking. No legitimate company cold-calls to fix your computer. None.

The text from the toll road, parcel company, or government agency. A small fee owed, a delivery problem, a link to tap. The link leads to a fake site that harvests your card details. Real organisations do not resolve fees by text message link.

Romance and friendship scams. A connection forms online, often over months. They are warm, attentive, and eventually in trouble that only money fixes. The cruelty of these is hard to overstate, and the losses run to nine figures nationally. The rule is hard but simple: someone you have never met in person who asks for money is a scam, with no exceptions.

Investment offers. Professional websites, fake celebrity endorsements, early "returns" you can actually withdraw to build trust. Investment scams are the single largest category of losses in the country. If an investment found you, rather than you finding it, walk away.

The grandparent call. A young voice in distress: "Grandma? I'm in trouble, please don't tell Mum." Money needed urgently for bail, a hospital, a flight. AI can now mimic a specific person's voice, so trust the situation, not the sound. Hang up and ring the grandchild's actual number.

The one habit that beats all of them

Here it is: **stop, and check through a different door.**

Whatever the message or call claims, end the contact, then verify using contact details you found yourself. Ring the bank on the number printed on your card. Check the toll account through the official app. Call the grandchild on the number you have always had. Ask the company through their real website, which you typed in yourself.

Scammers can fake a caller ID, an email address, a website, and now a voice. The one thing they cannot fake is what you find when you go through a different door. Every

pressure a scammer applies, the urgency, the authority, the secrecy, is designed to stop you doing exactly this. Which tells you everything about how well it works.

And the second half of the habit: **tell someone.** Scams die in daylight. A thirty-second mention to a family member or friend, "I got an odd call today", is often all it takes. You are never bothering anyone. The people who love you would far rather hear about ten harmless calls than one expensive silence.

If one gets through

It happens, including to sharp, careful people. Speed matters more than embarrassment.

1. **Call your bank immediately** and tell them. Fast action can sometimes stop or recover transfers.
2. **Report it to Scamwatch** (scamwatch.gov.au) so the patterns get tracked and others get warned.
3. **Contact IDCARE** (idcare.org) if personal details were taken. They are a free, government-supported identity recovery service.
4. **Tell your family.** Not as a confession. As intelligence. The same scam is probably heading their way.

Nobody worth knowing will think less of you. The shame belongs entirely to the thief.

What we do about this in homes

When Gray Matter Solutions sets up technology for clients, scam resistance is built into the setup: call screening where available, spam filtering, safe defaults, and a plain-language, large-print "is this a scam?" checklist that lives next to the phone. We also walk through real examples together, because seeing a scam in advance is the best vaccination there is.

Worried about a parent, or about your own setup? Start with a free call. Email phil@graymatter.team or visit graymatter.team.

Gray Matter Solutions Pty Ltd, ABN 24 678 904 231. In-home technology support across Sydney's Northern Beaches, North Shore, and Inner West.

Want a hand with this? Gray Matter Solutions provides patient, in-home technology support across the Northern Beaches, North Shore, and Inner West of Sydney, funded through NDIS,

Support at Home, or privately. Start with a free 15-minute call: (02) 5761 0386, or phil@graymatter.team. More free guides at graymatter.team/insights/.