



FutureInReach

FREE REACH PACK

Phone, scams and "is this real?" check

A calm, 10-minute way to check a suspicious letter, email, text, phone call or door knock, with the free AI app on your phone. Includes the Scam Check Coach (Is this real?).

Free to share, for personal use

This pack is free. You are welcome to print it, email it or pass it on to family, friends, neighbours or a community group, as long as you share it unchanged, with this page, and do not sell it.

Please remember: AI can get things wrong. This pack could help you spot warning signs, but it cannot prove a message is safe. Always check with the organisation using a number you find yourself.

futureinreach.app/free-scam-check.html

For adults 18+. General information only, not legal, financial or professional advice.

© 2026 Douglas Tunmer, trading as FutureInReach. Not affiliated with Google, OpenAI or any AI provider.

Phone, scams and “is this real?” check

Everyday life, “is this real?” letter, email, text, call or visit → a calm scam check and the safe next step

Who it’s for: Anyone who gets letters, emails, texts, phone calls or people at the door asking for money, details or “urgent” action. Written especially for older and retired people (large-text steps, one action at a time), and just as useful for working adults, who get the same scams. Good to set up together with a parent or grandparent.

The switch: Guessing, panicking, or paying because a message “looked real” → a calm second opinion on the warning signs, plus the safe next step: stop, and check using a number you find yourself.

You’ll need: Your phone, any AI app (Gemini, ChatGPT, Copilot or Claude) with the FutureInReach Scam Check Coach set up (see “Set up your Coach”), the message or a few notes about the call or visit, and a family member or friend you can ring.

10-minute walkthrough (large-text steps)

Step 1 • Minute 0–1. Stop. Don’t click, don’t pay, don’t call back on the number they gave you. Real organisations will wait while you check. If someone is on the phone, hang up. If someone is at the door, keep it closed or say “Not today” and close it.

Step 2 • Minute 1–2. Open the FutureInReach Scam Check Coach (your Gemini skill or ChatGPT Project, or a new chat in any AI app with the Coach instructions or prompt card pasted in).

Step 3 • Minute 2–4. For a letter, email or text: copy the words, or take a screenshot or photo. Cover your name, address, account numbers and any codes first. Don’t tap any link in it to “have a look”.

Step 4 • Minute 2–4 (calls and visits). For a phone call or door knock: type or say a few notes. Who they said they were, what they wanted, how they wanted to be paid, and how urgent they made it sound. No need to remember it word for word.

Step 5 • Minute 4–6. Read the Coach’s answer: the red flags it found, how worried to be (low, medium or high), and what to do next. It helps you spot scams. It cannot prove a message is safe.

Step 6 • Minute 6–7. Check it yourself. Find the organisation’s number on your own card, bill, statement or their official website. Never use a number, link or QR code from the message.

Step 7 • Minute 7–9. If you already paid, clicked, or gave any details: ring your bank now using the number on the back of your card. Then tell a family member. See “When to call someone instead” below.

Step 8 • Minute 9–10. Report it (in Australia, to Scamwatch) and delete or block it. Do the 30-second check.

Stop and check scripts (say these out loud)

Phone call script (keep by the phone)

"I don't do anything on calls I didn't expect. I'll call the company back on the number I already have." Then hang up.

If they say it's urgent: "If it's real, it can wait ten minutes." Hang up.

If they say they're from the bank, police, tax office, Centrelink, Medicare, the phone or internet company: hang up and call the number on your card, bill or their official website.

If they ask you to install an app, read out a code, or "let them in" to your computer: say "No" and hang up.

If they tell you to keep it secret, or not to tell the bank: that is a scam sign. Hang up and tell someone.

Tip: wait a minute, or use a different phone, before you call back, in case the line is still connected.

Door knocker script (stick inside the front door)

Keep the door closed or on the chain. You don't have to open it.

"I don't sign or pay anything at the door. Leave me a card and I'll check you myself."

Ask for ID, but don't trust ID alone. Look up the company's number yourself and ring them.

Never let anyone in to "check" the power, water, roof or gas unless you booked it, or you have called the company yourself.

Never pay cash, transfer money or hand over cards for work "today only".

If they won't leave or you feel unsafe: close the door and call the police (in Australia, 000 in an emergency).

Red-flag checklist (any one of these: stop and check)

- **Hurry.** "Act now", "last warning", "your account will be closed today", a countdown or a threat of arrest or fines.
- **Unusual payment.** Gift cards, cryptocurrency, wire or money transfer, a new bank account ("we've changed our details"), or cash picked up from your home.
- **Secret or shame.** "Don't tell the bank", "don't tell your family", or a story that makes you embarrassed to ask.
- **Asks for codes or access.** A one-time code, PIN or password, or asks you to install an app so they can "fix" your computer or phone.
- **Too good, or too scary.** A prize, refund, inheritance or investment you didn't expect, or a parcel, tax or fine problem you didn't know about.
- **Odd sender or link.** A different email address or website from the real one, a link to "verify" or "update" details, or a text from an unknown number saying "Hi Mum, I've lost my phone".
- **Love or friendship asks for money.** Someone met online who can never meet or video call, but needs money for an emergency or investment.

When to call someone instead of using AI

- **Money has gone, or you shared bank details:** call your bank straight away, on the number on the back of your card or on its official website. Ask them to stop any payments.
- **You gave out ID details (licence, passport, Medicare, tax file number):** in Australia and New Zealand, IDCARE (free identity and cyber support): 1800 595 160 in Australia, 0800 121 068 in New Zealand.
- **To report a scam (Australia):** Scamwatch, scamwatch.gov.au/report-a-scam. Reports help warn others.

- **Cybercrime, e.g. money stolen online or someone got into your accounts (Australia):** ReportCyber at cyber.gov.au/report-and-recover/report. For identity documents physically stolen, contact your state or territory police.
- **Danger right now, or someone won't leave your door:** call 000 in Australia (or your country's emergency number).
- **Other countries:** use your country's official scam or fraud reporting service (for example, in the US, the FTC at reportfraud.ftc.gov; in the UK, forward scam texts to 7726). Search for your government's official site, not an ad, and call your bank first if money is involved.
- **Not sure, or feeling pressured:** ring a family member or a friend you trust before doing anything. A second person is the best scam check there is.

Common mistakes

- **Calling the number in the message.** Scammers give their own number. Use the number on your card, bill or the official website.
- **Tapping the link "just to look".** Some links ask for details or install things. Copy the words instead, or take a screenshot.
- **Taking "low risk" as "safe".** The Coach helps you spot warning signs. Scammers change tricks all the time, so if anything feels wrong, still check with the real organisation.
- **Pasting private details to "prove" it.** Never paste card numbers, passwords, codes or ID numbers into AI. Cover them first.
- **Staying quiet out of embarrassment.** Scams fool smart, careful people every day. Tell your bank and family fast. Speed matters more than pride.

Prompt card

No Coach set up yet? Copy everything in this box into any AI chat and fill in the [brackets].

You help me check whether a message, call or visit might be a scam. I have covered or removed my personal details.

What it was: [letter / email / text / phone call / person at the door / social media message]

Who they said they were: [e.g. my bank, the tax office, a parcel company, a grandchild]

My country: [e.g. Australia]

The message, or my notes about the call or visit: [paste text, attach a screenshot, or describe: what they wanted, how they wanted payment, how urgent they made it]

What I have already done, if anything: [e.g. nothing / clicked the link / paid / gave a code]

Please tell me, in short plain sentences:

1. The red flags you can see (quote the words)
2. How worried I should be: low, medium or high, and why
3. What to do right now, step by step
4. How to check it safely myself
5. Who to tell or report it to in my country

Rules: Never tell me it is definitely safe. Don't give me phone numbers or links; tell me to use the ones on my card, bill or the official website. Don't ask for my bank details, passwords or codes. If I have paid or shared details, tell me to call my bank first.

Never paste this

- Card numbers, bank account and BSB numbers, or online banking logins
- Passwords, PINs or one-time codes (no real organisation asks for these)
- Your full name, address, date of birth or signature
- Tax file, Medicare, pension, licence or passport numbers
- Photos of your cards or ID
- Other people's details (family names and numbers)

Before you act: 30-second check

- ☐ I did not click, pay or call back on their number
- ☐ I checked using a number I found myself
- ☐ No private numbers or codes were pasted
- ☐ If money or details went out, I rang my bank
- ☐ I told someone I trust and reported it

Your Coach: FutureInReach Scam Check Coach (Is this real?)

COPY BOX Coach name

FutureInReach Scam Check Coach (Is this real?)

COPY BOX Coach instructions

Copy everything inside this box, from the first word to the last. Paste it into your Gem, Project or chat.

ROLE: You are the FutureInReach Scam Check Coach. You help everyday adults, especially older and retired people, and also busy working adults, spot the warning signs of scams in letters, emails, texts, social media messages, phone calls and door-to-door visits, and choose a safe next step. You give a second opinion; you never guarantee that something is safe.

STYLE: Calm, kind, very plain English. Short sentences, one idea per line. No jargon and no blame: say "Scammers fool careful people every day." Match the user's spelling. Default to Australian English if unclear. Keep it easy to read in large text on a phone.

FIRST MESSAGE: If the user hasn't shared anything, ask in ONE short message for: (1) what it was (letter, email, text, call, visit), (2) who they said they were, (3) their country, (4) the words, a screenshot, or notes on what was said, (5) whether they have already clicked, paid or shared anything. Remind them: "Cover card numbers, passwords, codes and your address first. Don't click any links."

OUTPUT FORMAT:

1. Already paid, clicked or shared details? If yes, put this FIRST: "Call your bank now on the number on the back of your card," then the rest.
2. Red flags: short bullets, quoting the exact words.
3. How worried to be: Low / Medium / High, with one line why.
4. What to do now: up to 4 numbered steps.
5. How to check safely: use the number on your card, bill or the organisation's official website, never the one in the message.
6. Who to tell: a family member or friend, and the official scam reporting service for their country (in Australia: Scamwatch; ReportCyber for cybercrime; IDCARE for identity help).
7. For calls or door knocks: a short script they can say next time.

HARD RULES:

- Never say a message is "definitely safe", "100% genuine" or "not a scam". The best you can say is "I can't see common scam signs, but check with the organisation using a number you find yourself."
- Never give phone numbers, links, email addresses or QR codes for organisations, except the official reporting services named above by name. Tell the user to find contact details on their card, bill, statement or the official website.
- Never ask for, repeat or store bank details, card numbers, passwords, PINs, one-time codes or ID numbers. If the user pastes them, replace them with [REMOVED] and tell them kindly to change their password or call their bank if they shared them with anyone else.
- Never tell the user to click a link, scan a QR code, call a number from the message, install an app or give remote access.
- If there is danger now, or someone won't leave their door, tell them to call 000 in Australia or their local emergency number.
- If money has gone or details were shared, always put "Call your bank now" first, and mention IDCARE (Australia and New Zealand) or the national equivalent.
- Don't give legal or financial advice. Don't judge or shame the user.
- Keep the whole answer short enough to read on a phone.

ENDING: Finish with: "If in doubt, don't. Hang up, close the door, or delete it, and check with a number you find yourself." Then offer: "Want help telling a family member, or writing a report?"

Try your Coach with this example

Paste this as your first message after setting up the Coach, to see how it works. It's made-up example text.

"Australia. Text message: '[Bank name] ALERT: A payment of \$1,249.00 to an overseas account is pending. If this was not you, verify now at [link] or call 1300 xxx xxx within 2 hours to stop it.' I haven't clicked anything."

Set up your Coach

Pick one. All three use the same Coach instructions above. See "How to set up a Coach" at the front for more help.

- **1 • Gemini skill.** Personal Google account, age 18+, Keep Activity on. On gemini.google.com or the Gemini app: Customize → Skills → Create manually. Name it "scam-check-coach", add a one-line description, paste the Coach instructions, tap Create. Use it by typing / and the skill name. (Until Gems end for personal accounts in November 2026 you can also make a Gem; it moves to skills automatically.)
- **2 • ChatGPT Project.** Works on free and paid ChatGPT plans (signed in). Create a project called "FutureInReach Scam Check Coach", open ●●● → Project settings, paste the Coach instructions into the instructions box, save. Start every chat for this task inside that project.
- **3 • No setup: paste and go.** Open a new chat in any AI app (Gemini, ChatGPT, Microsoft Copilot, Claude), paste the Coach instructions as your first message, then send your task. Works on free plans; repeat for each new chat. Each app has its own age rules (most require 18+, or 13+ with a parent's permission).

Please note

The Scam Check Coach helps you spot common warning signs of scams. It cannot guarantee a message, call or visitor is safe or unsafe, and scammers change their tricks often. Always check with the organisation using contact details you find yourself, and contact your bank straight away if money or details may have been shared. FutureInReach is not a bank, police service or reporting agency.



Want more?

This scam pack is one of the Reach Packs in the FutureInReach founding library. Other packs could help with everyday jobs like:

- Bills and official letters, explained in plain English
- Job hunting: a résumé from your real work
- A messy inbox turned into reply drafts and a to-do list
- Chasing unpaid invoices, politely, and more

Founding offer: US\$19.99 plus GST or local tax, one-time, for 12 months of access to the founding library. Adults 18+, 14-day refund.

Get founding access

Checkout: <https://futureinreach.lemonsqueezy.com/checkout/buy/999e4a92-74d2-41fb-b562-bfe46b56354f>

Not ready? Join the free waitlist for updates: <https://tally.so/r/q4xy97>

Website: <https://futureinreach.app>

Questions: futureinreach.help@gmail.com