

Pause and Check

A one-page guide to checking a suspicious message with AI

Got a text, email or message that is probably fine, but you are not quite sure? Take a minute. These five questions could help you think it through calmly before you do anything. Scammers fool careful people every day, so checking is never silly.

First, before anything else

Don't click any links, scan QR codes or call numbers in the message. Take a screenshot first, in case you want to report it later.

Five calm questions

1. **Who sent it, really?** Look at the actual number or email address, not just the name shown. Would that organisation normally contact you this way?
2. **What is it asking you to do?** Click, pay, log in, share a code, call back or install an app? Those are the moments to slow down.
3. **Is there pressure?** "Act now", "your account will be closed", "final notice" or a deadline in hours. Genuine organisations rarely rush you.
4. **Does anything not match?** An address that looks almost right, odd spelling, a parcel you didn't order, or a bill for a service you don't use. (Don't tap a link to check it.)
5. **Can you check another way?** Contact the organisation using details you already trust: the number on your card, bill or statement, or their official app or website that you open yourself.

Ask an AI chat for a second opinion

Before you paste, cover card numbers, passwords, one-time codes and your address. Then copy this into any AI chat (Gemini, ChatGPT, Copilot or another):

Please act as a calm second opinion on a message I received. I'm in [your country]. It came by [text / email / social media / phone call] and says it's from [who]. Here are the words, with card numbers, passwords, codes and my address removed: [paste]. I [have / haven't] clicked, paid or shared anything. Please list any warning signs, quoting the exact words, tell me how worried to be (low, medium or high) and why, and suggest safe next steps. Don't tell me it's definitely safe, and don't give me any links or phone numbers from the message.

If you have already clicked, paid or shared details

Call your bank now, using the number on the back of your card. Change any password you typed in. Then report it. In Australia and New Zealand, IDCARE could help if your identity details were shared.

Afterwards

Delete the message or keep it safely, but don't click it. Report it to your country's official scam reporting service (in Australia, that's Scamwatch at scamwatch.gov.au). If you are in danger right now, call 000 in Australia or your local emergency number. And tell someone you trust; it helps.

Remember: If in doubt, don't. Hang up, close the door, or screenshot and delete it, and check with a number you find yourself.

This guide, and any AI chat, helps you think it through. Neither can tell you for certain whether something is a scam. If money or accounts are involved, contact the organisation directly using details you already trust. General information only, not legal or financial advice.