

STOP. CHECK. VERIFY.

A simple habit for suspicious emails, texts, calls and social messages.

1 STOP

Do not click, reply, pay, call, upload ID or share a security code just because a message feels urgent.

2 CHECK

Open the sender details. Inspect the real email address, link destination, account profile, attachment name and payment request.

3 VERIFY

Leave the message. Open the official app or website yourself, or call a trusted number you found independently.

Common warning signs

- The sender name looks familiar, but the full email address does not match.
- A link looks normal until you inspect where it really goes.
- You are rushed, threatened, frightened or told to keep the request secret.
- Someone asks for a one-time code, password, ID document or remote access.
- You are told to move money to a 'safe account' or pay to receive money or a prize.
- A friend or family account asks for money but blocks normal ways to verify who they are.

If you already clicked, paid or shared information

- Stop contact and do not send more money or codes.
- If money was sent, contact your bank immediately using a trusted number.
- Change affected passwords and turn on multi-factor authentication where available.
- Save messages, screenshots, receipts and account details as evidence.
- If someone is threatening or blackmailing you, do not pay. Save evidence and seek help.

The safest habit: Do not use the message to verify the message.

Australia: report scams at Scamwatch. For online sexual blackmail or image-based abuse, use eSafety. Elsewhere, use your national fraud reporting service. Educational guide only. Scam Spotter uses reconstructed examples rather than real victim messages.

theimmortalai.com/scam-spotter/