



SCAM CALL? STOP. THINK. PROTECT YOURSELF.

Simple steps to keep you safe from scammers.

1 RED FLAGS TO WATCH FOR

-  Caller claims to be from a bank, government or police.
-  Talks about urgent problems (fraud, loans, suspicious activity).
-  Uses real personal details to gain trust.
-  Asks you to:
 - open your banking app
 - share your balance
 - confirm transactions
-  Pushes you to act immediately.

2 STOP THE CONVERSATION



- Do NOT provide any information.
- Do NOT follow instructions on your phone.
- Hang up immediately.
- Stay calm – pressure is part of the scam.

3 CHECK BEFORE YOU ACT



- Call your bank using the official number.
- Never trust numbers given by the caller.
- Log into your account independently.
- Ask a trusted person if unsure.

4 STAY SECURE



- Enable bank alerts.
- Use strong, unique passwords.
- Keep personal information private.
- Be cautious with unexpected calls.

5 REPORT IT



- Report to [Scamwatch.gov.au](https://www.scamwatch.gov.au)
- Tell your bank immediately.
- Warn friends and family – it could save them from being scammed.



NO BANK WILL EVER ASK FOR YOUR DETAILS OVER THE PHONE.



If in doubt, **hang up.**
It's okay to stop the conversation.



Contact your bank directly using their official number.
Don't use numbers from suspicious calls or texts.



Talk to someone you trust.
A second opinion can make a big difference.



Report scams at [Scamwatch.gov.au](https://www.scamwatch.gov.au)
Help stop scammers and protect others.