



The fight against scams never stops.

To defend **you**, Australian banks have
joined forces with a major investment
in **new technology**.

Australian banks are working to protect **you**.





**AUSTRALIAN BANKS ARE COMMITTED TO
PROTECTING YOU**

**If you suspect a scam, contact your bank
immediately.**



Australian Banking Association

PROTECT YOURSELF FROM SCAMS

A BANK WILL NEVER:

- Contact you to ask for any account or personal details in an unsolicited text or email.
- Call and ask people to transfer funds to another account over the phone.
- Ask for online banking passcodes or passwords over email, text or phone.
- Ask for remote access to your devices.
- Threaten you to take immediate action on an issue.



PROTECT YOURSELF FROM SCAMS

YOU SHOULD NEVER:

- Provide banking information, passwords or two-factor identification codes over the phone or via text to anyone even if you know them – contact the bank through official channels only.
- Login to your online banking via links sent through email or text.
- Click on suspicious emails, links or texts.
- Transfer money unless you're certain it's going to the right person.
- Provide personal information to anyone you don't know personally unless you know it's for a legitimate purpose.



PROTECT YOURSELF FROM SCAMS

YOU SHOULD ALWAYS:

- Pause to question the authenticity of a text message, an email, a call or a person who claims to be from a trusted organisation. If in doubt, call back on the publicly listed phone number before taking any action.
- Register a PayID securely through your bank and not via a third party and use PayID where you can.
- Set-up two factor authentication to protect your accounts and online banking.
- Check the legitimacy of any invoices or bills and use PayID wherever possible.
- Immediately report any suspicious activity directly to your bank.





PROTECT YOURSELF FROM SCAMS

Contact your bank immediately if you suspect something's wrong.



Australian Banking Association