News Release

For Release: 11 July 2025

Could you spot a bank impersonation scam?

With a recent spate of impersonation scams across Australia, ANZ is urging customers to stay alert and ask themselves: *Could you spot a bank impersonation scam?*

Scammers are increasingly posing as banks, using sophisticated tactics to trick people into handing over personal information, transferring money, or clicking on malicious links. These scams often look and sound convincing – making it harder than ever to tell what's real and what's not.

According to Scamwatch, Australians reported over 10,800 online banking scams, with losses reaching $11 million in 2024 alone.

ANZ Head of Customer Protection, Shaq Johnson, says it's important to be cautious of unsolicited contact, and is urging customers to understand the warning signs of what a typical bank impersonation scam might look like.

"Scammers are experts at creating a sense of urgency and fear, and their methods are getting smarter – they will often use official-looking logos, language, websites, and caller ID spoofing to appear genuine.

"Learning how to spot a scam is your first line of defence, and there are common red flags that indicate someone is impersonating your bank - including asking you to click on a link via SMS, prompting you to download software, or pressuring you into an urgent decision.

"Remember there is always time to pause and think. When in doubt, call your bank directly, and if you've been met with a scam, report it to your bank to keep yourself and other customers safe."

Common signs of a bank impersonation scam include:

- A text, call or email claiming to be from your bank, asking you to verify or update your account.
- Urgent language designed to create panic – such as threats of account suspension or fraud alerts.
- Requests for login details, passwords, or remote access to your device.
- Messages with links that look legitimate but lead to fake websites.

How to protect yourself:

- Never share your banking details or passwords with anyone.
- Never share an OTP 'One-Time Password' with anyone.
- Don't click on links or download attachments from unexpected messages.
- Contact your bank directly using official contact details – not the ones provided in the message.
- Report suspicious activity to Scamwatch and your bank immediately.

For media enquiries contact:

Alexandra La Sala
Public Relations Advisor
Tel: +61 499 292 554

Kate Power
Public Relations Manager
Tel: + 61 481 547 556

Australian and New Zealand Banking Group Limited
833 Collins Street Docklands Victoria 3008 Australia
ABN 11 005 357 522

ANZ's customer protection teams and systems operate 24/7. Customers who believe they may have been a victim of a scam should contact us immediately, on 13 13 14 or visit us at http://www.anz.com.au/security/report-fraud/ for more information.

For more information on the types of scams and how to protect yourself visit http://www.anz.com.au/security/types-of-scams.

About ANZ Scam Safe: To assist the community in remaining aware and alert to the constantly changing scams and fraud environment, ANZ has launched *Scam Safe*.

Scam Safe highlights the latest cyber security and fraud issues impacting the community and what ANZ is doing to help protect our customers.

To stay *Scam Safe,* ANZ encourages customers to learn their security ANZ's:

A: Always be wary
N: Never share personal information, with anyone
Z: Zoom in on the details, they matter