

News Release

For Release: 1 May 2025

ANZ encourages families to talk about scams this Mother's Day

ANZ is encouraging Australians to remain hyper-vigilant against scams **this Mother's Day**, urging families to have an open conversation with each other to ensure they know how to spot the warning signs.

In particular, the bank is reminding mothers to be wary of "Hi Mum" scams; fraudulent text messages or calls from 'loved ones' claiming to need urgent financial help.

Impersonation scams such as "Hi Mum," where criminals prey on mothers by pretending to be their child in need of money, are becoming increasingly sophisticated – with scammers contacting potential victims via text message, social media and phone calls **sometimes able to copy the way the target's child communicates** to make their approach more convincing.

ANZ Scams Portfolio Lead, Ruth Talalla encourages Australians to regularly check in with family members to stay on top of the ever-changing scam environment.

"As scam tactics become more advanced, it's vital Australians know how to recognise the warning signs."

As well as a heightened risk of "Hi Mum" scams, ANZ is reminding families to be on the lookout for online shopping scams when purchasing gifts for mum, which typically target shoppers during peak retail periods.

"Scammers are especially opportunistic in the lead up to special occasions like Mother's Day. Whether by posing as relatives or brands and sellers online, **we're reminding Australians** to ensure the whole family knows how to watch out for red flags such as inconsistent or unfamiliar contact information, significantly cheaper offers compared with other sellers, or any deal that seems too good to be true," Ms Talalla concluded.

Warning signs of impersonation scams and how to avoid them:

- Unknown contact: Cybercriminals may send messages from unknown numbers claiming to be loved ones who urgently need help. This is a tactic to put pressure on victims to send money or sensitive information. Always independently verify where the message is coming from by contacting the source via a method you already trust.
- Unexpected contact: **If a phone call or message from a 'loved one' is unexpected or strange behaviour** for this person, stop to verify their identity independently.
- Urgent action: If a scammer is urgently requesting payment and asking a victim not to tell anybody, this could also be a sign the call is a scam. Slow down, take a moment to check if the message is legitimate, and if in doubt, do not send any funds.

Warning signs of online shopping scams and how to avoid them:

- Inconsistent domains: Cybercriminals may use email and website domains that appear similar to the legitimate sender. Compare the domains to the company's official domain online.
- Uncommon payment methods: Fake sites may ask for unsecure methods of payment such as direct transfers or gift card payments when shopping online.
- Overly positive reviews: Search for independent reviews of an online trader to ensure legitimacy, particularly if the brand is unfamiliar to you.

As scam technology becomes more advanced, so too does ANZ's approach to prevention and customer education.

In March ANZ announced the launch of [Digital Padlock](#), a new feature allowing customers to 'lock down' access to their accounts if they suspect they are being targeted by cybercriminals.

So far in 2025, ANZ has issued more than 90,000 personalised warning messages on Internet Banking transactions or activity considered high risk. And, since the inception of the ANZ First Responder team – a dedicated team of specialists to directly support customers who may have been targeted by cybercriminals – 140,000 calls have been answered, with approximately 93% of these calls resolved at the first point of contact.

For media enquiries contact:

Sophie Clausen
Public Relations Advisor
Tel: +61 481 244 823

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

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