

For Release: 6 October 2026

ANZ urges businesses to stay vigilant as AI-enabled scams and identity fraud evolve

Australian businesses are being urged to remain vigilant as cyber criminals adopt increasingly sophisticated tactics, with Business Email Compromise (BEC), impersonation, investment, and invoice (payment redirection) scams posing significant risks to organisations of all sizes.

Cyber scams are becoming harder to detect, with criminals impersonating trusted brands, compromising suppliers and exploiting businesses and individuals aided by AI-enabled deception techniques and legitimate digital platforms.

The Australian Signals Directorate's [Annual Cyber Threat Report 2024-25](#) found more than 84,700 cybercrime reports were submitted nationally during FY25, with BEC and identity fraud among the top reported cybercrimes impacting businesses.

ANZ General Manager Specialist Sales, Cosi De Angelis, said: "Business Email Compromise, payment redirection and impersonation scams remain among the most significant threats facing businesses today. Tactics such as impersonating banks and trusted suppliers, sending fake invoices, and creating a sense of urgency are all too common, as scammers prey on time-poor business owners.

"As AI evolves, criminals are adopting more sophisticated tactics to manipulate customers into approving payments.

"Financial crime is becoming harder to detect because it is often hidden within legitimate businesses, trusted relationships, and everyday transactions. In many cases, criminals are exploiting trust as effectively as they are technology."

One of the most significant emerging threats identified by ANZ is the use of stolen identities and mule accounts.

The bank has observed coordinated criminal activity involving accounts opened using stolen identities and subsequently used for scam activity, money mule operations, micro-laundering, and the movement of scam proceeds through the financial system.

ANZ continues to strengthen its fraud and scam prevention capabilities, focusing on behavioural biometrics, fraud analytics, and enhanced onboarding controls.

Between October 2025 and June 2026, ANZ customer scam losses fell by 24 per cent compared with the same period the previous year. During that time, ANZ also prevented and recovered more than \$100 million in scam and fraud-related funds.

"Scam prevention isn't only about stopping customers from sending money to criminals. It's also about preventing criminals from establishing accounts that can receive and move scam proceeds in the first place," Mr De Angelis said.

Alongside investing in scam detection and prevention measures, ANZ is supporting customers through education initiatives including enhanced cyber security education resources, customer webinars, high-risk payment controls, and reminding customers to Stop. Check. Protect.

With October marking Cyber Security Action Month, ANZ is encouraging businesses to review their cyber security practices and ensure staff understand the warning signs of cyber-enabled scams and fraud.

"Periods of increased transaction volumes and customer activity can create opportunities for cyber criminals to exploit rushed decision-making. As Black Friday and the festive season approach, now is a good time for businesses to review their cyber security controls and ensure employees understand the warning signs of scams.

"Technology will continue to evolve, but human judgement remains one of the strongest defences against scams. Recognising red flags such as unexpected changes to payment instructions, unusual requests, or pressure to act quickly can be the difference between stopping a scam and becoming a victim," Mr De Angelis said.

Tips to protect your business:

- **Your bank will never ask you to share sensitive banking details like passwords, PINs, ANZ Shield Codes, or one-time passcodes.** If someone requests this, hang up immediately.

- **Seek confirmation by phone** rather than email if you receive a change of banking details from a supplier or a new supplier you have not paid before.
- **Request two authorisations for payments** to create an extra level of security, particularly for large transactions or those that are sensitive or urgent.
- **Review how you update supplier details** making sure employees are aware of the new or updated policies.

ANZ encourages all businesses and their employees to continue building their awareness through available education opportunities and information on the [ANZ Business Cybersecurity Hub](#).

For media enquiries contact:

Sophie Clausen
Public Relations Advisor
Tel: +61 479 033 226

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

ANZ is committed to helping protect customers from scams and fraud through layered security, education and specialist support. Its fraud protection teams and systems operate 24/7, supported by ANZ Falcon, the bank's flagship fraud detection and prevention technology.

ANZ's scam protections include First Responders, CallSafe, Scam Safe, enhanced biometrics and Confirmation of Payee, giving customers more tools and support to bank securely.