News Release

For Release: 2 October 2025

ANZ reminds business customers to stay scam aware this Cyber Security Awareness Month

ANZ is urging Australian businesses to stay vigilant against scam activity as cybercriminals increasingly target small and medium-sized businesses with sophisticated tactics.

Cybercriminals take advantage of businesses and individuals by exploiting vulnerabilities in email systems and financial processes, hacking into internal systems to update invoice payment details and asking for payments to be sent to a new or updated bank account the scammer controls.

This type of activity is referred to as a business email compromise (BEC). According to the Australian Signals Directorate's latest Cyber threat trends report, BEC scams are among the most common scam type, costing Australian businesses over $84 million in 2024 alone, and representing 13 per cent of the 87,400 reported cybercrime incidents.

Scammers will also attempt to target small businesses by impersonating banks or other financial institutions and government agencies, tricking people into sharing personal information, transferring money or clicking on malicious links.

Small businesses are being disproportionately targeted; the average cost of a cybercrime incident has increased by 8 per cent in 2024 compared to the previous year, costing small businesses an average of $49,000 each year.

ANZ Head of Transaction Banking, Cosi De Angelis, said: "Cyber Security Awareness Month offers an opportune time for us to remind businesses about the kinds of scams out there, and how they can help keep their staff and finances safe.

"At ANZ we're serious about helping businesses stay safe. We combine robust fraud protections with 24/7 support, and provide practical education, like our 'Stop. Check. Protect' approach, which encourages busy business owners to slow down and be wary of threats, helping them identify red flags and stay one step ahead of scammers.

"Too often, I see scammers attempt to target small business owners by impersonating trusted business partners or long-term suppliers. Business owners are often run off their feet, and cybercriminals will look to exploit this and take advantage of hardworking Australians.

"Given the sheer volume of emails, text messages, instant messages and social media messages business owners and employees send and receive each day, it's not surprising we tend to act on things straight away and sometimes overlook inconsistencies in correspondence. Scammers will take advantage of this - I implore Australians to double check all communication and if in doubt, contact your vendors and suppliers."

ANZ teams are working around the clock to help prevent cybercriminals from targeting small-medium Aussie businesses. Between October 2024 and June 2025, ANZ successfully prevented and recovered over $100 million in scam and fraud-related funds.

Melbourne-based family business, Benton's Plumbing Services, was targeted by scammers impersonating a genuine business contact. Staff were tricked into handing over remote access to their computers, unknowingly placing their business at serious financial risk.

ANZ's Falcon technology flagged suspicious activity when the business attempted to transfer a large sum of money to an overseas account. ANZ's Fraud Detection team acted swiftly - contacting Benton's Plumbing Services while staff were still engaged in a live chat with the scammers. Thanks to the rapid response, the threat was intercepted, and no money was lost.

Benton's Plumbing Services' Chief Financial Officer, Aleks Nawrocki, said: "Our team experienced a very significant scam near miss that was averted by the diligence of the ANZ team. The ANZ team was extremely quick and efficient, and the scam was thankfully, identified and prevented.

"Since the incident, our team has been more scam aware and confident in identifying when something doesn't feel right. It is extremely reassuring to know that we have been protected by the ANZ team and want to encourage other businesses just like us to operate with caution."

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.

Securing Australia Together webinar

ANZ has partnered with the National Office of Cyber Security (NOCS) along with the other major banks to deliver a Securing Australia Together webinar on Thursday, 9 October at 10am AEDT.

Register your attendance to Securing Australia Together and enter the access code **ANZ-JNEUY.**

Stay scam safe with ANZ

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

For media enquiries contact:

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

Judy Hang
Public Relations Advisor
Tel: +61 479 173 821