News Release

For Release: 10 April 2025

ANZ warns customers to be vigilant to business email compromise and fake invoice scams

ANZ is urging customers to be on alert for the warning signs of business email compromise (BEC) and fake invoice scams, also known as payment redirection scams, as cybercriminals look to take advantage of businesses and individuals by exploiting vulnerabilities in email systems and financial processes.

Small and medium sized businesses are the most common targets for cybercriminals running payment redirection scams, as their technology infrastructure is typically less complicated to infiltrate than larger corporations. Once scammers have hacked into a business's internal system, they can update invoice payment details and ask for payments to be sent to a new or updated bank account.

The Federal Government's Annual Cyber Threat Report stated the total self-reported BEC losses were almost $84 million over the 2023-2024 financial year across Australia, with the majority of cybercrime reports lodged by small businesses.

ANZ Scams Portfolio Lead, Ruth Talalla said: "Scams remain an ongoing challenge for Australians, with cybercriminals increasingly adopting sophisticated practices such as BEC and fake invoice scams to exploit consumers.

"We encourage business owners and individuals to be on high alert and double check all details before making any payments. If you receive an unusual or unexpected payment request, notice updated details on an invoice, or are making a payment to a new account, it's important to verify the details directly with the legitimate company or person before sending funds."

How to spot these scams:

- **Unexpected contact method or requests:** Be cautious if someone you don't usually communicate with via email or social media asks for personal information or payment (e.g., on WhatsApp).
- **Modified payment details on an invoice:** Verify payment details against previous invoices and confirm any changes directly with the company or person you're paying.
- **Dodgy domains:** Cybercriminals may use email domains that look similar to the real sender's. Compare the email domain to the company's official domain online.
- **Poorly written text or inconsistent message formats:** Look for grammar or spelling mistakes and unusual tone. Even well-written messages can be fake.
- **Missing or faked email signature:** Typically, cybercriminals will lack the legitimate company's or individual's email signature. Check for any inconsistencies with the real company's or individual's signature.

How to avoid these scams:

- Never call the phone number provided in a suspicious email or message. Instead, use a phone number you have independently verified and speak to someone you have previously dealt with if possible.
- Verify new or updated account details with the legitimate company using a phone number you have sourced independently before transferring any funds.
- If an email or message creates a sense of urgency, don't rush. Take your time to verify its authenticity.
- Use PayID for payments when available, so you can confirm the identity of the recipient.
- For large payments, send a small amount first and confirm it has been received by the legitimate company or individual before sending the full amount.

For media enquiries contact:

Alexandra La Sala
Public Relations Advisor
Tel: +61 466 258 343

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.

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

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