News Release

For Release: 1 April 2026

Small businesses urged to stay alert to scams over the Easter break

ANZ is urging its business customers to stay alert to the threat of scams, ahead of the Easter break.

As some businesses prepare to close for an extended period to make the most of the celebrations, cyber criminals often try to take advantage of hardworking small business owners who may let their guard down over the consecutive public holidays.

ANZ General Manager of Transaction Banking for Business & Private Banking, Cosi De Angelis, said: “We know many small business owners across the country will shut down over Easter and use the multiple public holidays for a well deserved break.

“Because of this, busy business owners tend to get their affairs in order before they finish up, which may involve paying suppliers, salaries and holiday pay early – meaning a significant increase in the flow of funds.

“This is an opportune time for cybercriminals to attack and exploit business owners when they least expect it.”

Sophisticated tactics used by scammers to try to exploit vulnerabilities in email systems and financial processes include hacking into internal small business systems to change invoice payment details and asking for payments to instead be sent to a new or updated bank account the scammer controls.

Scammers may 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.

These types of scams are known as business email compromise or impersonation scams and typically rely on trust and urgency to succeed.

Last year, ANZ observed a spike in attempted business email compromise scams resulting in fraudulent transactions in May, in the weeks following the Easter break.

“Easter is an important time for us to remind businesses about the kinds of scams out there, and how they can help keep their staff and finances safe,” Mr De Angelis said.

“We know how hardworking our business customers are and we don’t want to see any of them being taken advantage of by cybercriminals.

“I urge our customers to double check all communication and if in doubt, contact your vendors and suppliers direct via a channel you trust,” Mr De Angelis concluded.

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.

ANZ is serious about helping businesses stay safe, combining robust fraud protections with 24/7 support.

Practical education like the 'Stop. Check. Protect' approach is also available, and encourages busy business owners to slow down and be wary of threats, helping them identify red flags and stay one step ahead of scammers.

For media enquiries contact:

Emily Arnold
Public Relations Advisor
Tel: +61 413 610 338

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