News Release

For Release: 17 December 2024

ANZ encourages shoppers to be on alert for scams this festive season

December marks the busiest time of the year for Australian shoppers and as people turn their attention to the holidays, cyber criminals often find ways to take advantage of festive celebrations and customs.

ANZ has urged Australians to be alert to scams this holiday season, as cyber criminals look to benefit from the increase in online shopping, parcel deliveries, and travel.

ANZ Head of Customer Protection, Shaq Johnson, said: "During peak shopping periods, such as the December rush, customers are spending more time and money online so it is crucial that they remain vigilant about cyber safety.

"It's important to be aware of common scams. These include fake parcel delivery or 'parcel stuck' messages, bank impersonation and business email compromise attempts, 'Hey Mum' scams, fake e-gift cards, and travel-related scams."

In 2024, ANZ saw a 46 per cent reduction in customer losses incurred by scams. Over this period, the bank's customer protection team prevented more than $140 million going to cyber criminals.

"Cyber criminals employ various tactics to attempt to trick people into providing their personal and financial details," Mr Johnson said.

"A common scam at this time of year is the 'parcel stuck scam', where scammers trick individuals into paying additional fees or providing personal information by claiming that their package is stuck in transit. These can be difficult to detect, especially since many are expecting deliveries," Mr Johnson said.

"As always, but particularly in busy shopping periods, it's important to remember if it seems too good to be true, it probably is. Take the steps to safeguard yourself and your loved ones and be aware of the various tricks cyber criminals use online, to enjoy a cyber safe holiday season."

Key ways to stay safe online:

- Be wary of enticing offers: If something seems too good to be true, it probably is. Be cautious of offers that pressure you to make a quick purchase.
- Be cautious of new online stores: New online stores with extremely low prices can be tempting. Check the website's registration date using the ICANN Lookup search; if it was recently registered, it might be a scam.
- Avoid clicking on unexpected or unusual links: Don't click on unexpected or unusual links in emails, text messages, or pop-up messages on social media - they might lead you to a phishing website.
- Be alert for any SMS or phone call claiming to be from ANZ: The bank will never ask you to share your passwords, Shield Codes or PIN. If you receive a request for sensitive information, it could be a bank impersonation scam. Only call ANZ on phone numbers found in the ANZ app or on its website.
- Check the website URL carefully: Scam sites often use URLs that closely resemble those of official sites. Look for dashes, symbols, or typos in the URL.
- Verify information independently: Instead of relying on the communication you received, contact the shipping company directly through their official website or phone number to confirm your delivery status.
- Use secure payment methods and always check payment details: Use secure payment methods like PayID or BPAY, and verify the name matches the recipient. Always confirm invoice details directly with the business, especially if they have changed from previous ones. Be wary of unusual payment methods, such as vendors who only accept gift cards.
- Inspect items in person: Whenever possible, physically check items before purchasing. Seeing an item in person significantly reduces the risk of falling for a scam.

For media enquiries contact:

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

Amanda Schultz
Media & Public Relations Manager
Tel: +61 401 532 325

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 a new *Scam Safe* series.

Scam Safe will highlight 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