News Release

For Release: 19 December 2022

ANZ encourages customers to stay cyber-smart this silly season

ANZ is encouraging customers to be vigilant to scam activity during the festive season as scammers take advantage of busy schedules, an increase in online shopping, giving and travel.

ANZ saw a 22 per cent increase in scam-related activity this year, and similarly the Australian Cyber Security Centre observed a 13 per cent increase in the number of reported cyber incidents. Scams are most commonly delivered via phone call, text and email with more than 90 per cent of cyber attacks reported to begin as a phishing email.

ANZ Head of Customer Protection, Shaq Johnson said: "This busy time of year can leave Australians more susceptible to scams and cyber-attacks."

"Individuals, organisations and businesses are often distracted by holidays, shopping and other end of year events.

"As people prepare for the festive season, it's important to be cyber safe and cyber resilient. Ensure cyber resiliency plans are up to date and encourage conversations with friends and loved ones – perhaps around the Christmas table – about the evolving scams and cyber environment."

There is nothing festive about Christmas scams. Things to prepare for this festive season:

Bank Impersonation Scams. Cyber criminals are taking advantage of Australians' heightened awareness to scam activity and are cold calling, or texting customers claiming to be from their bank's Fraud Prevention team. The scammers try to panic the victim by telling them their account is at risk of fraudulent activity and often share personal information to support their claims before requesting sensitive account details, like internet banking registration information, passwords, card and PIN numbers. ANZ will never ask for personal information over the phone. If you're unsure if a call is legitimate, ask where the call is coming from and call them back on a number listed on official websites.

Business email compromise (BEC) & requests to update payment details. Falsely modified invoices are a popular approach for deceiving businesses out of funds throughout the year, but the signs can be easily missed during the busy lead up to Christmas. Ensure all requests to change payment details are checked before submitting payments, including those from your builder, conveyancer or supplier.

Fake parcel delivery. It's the most popular time of the year for online shopping and cybercriminals are quick to take advantage by impersonating popular courier services and sending tracking links by SMS or email. Never click a link or pay additional delivery fees and always visit a business website directly to track online shipping.

Fake e-gift cards. E-gift cards are an increasingly popular method of gifting. Cyber criminals take advantage of this by sending fake gift cards to trick customers into clicking on a link and handing over their personal information, including banking details. Never click on a link and always visit the retailer's official website to check if a gift card is legitimate.

"Hey Mum" scams. Impersonating family members, often under the guise of a lost phone, is a popular method for scammers to gather personal information and convince recipients to urgently transfer money. Stop and think twice when anyone, even someone you trust, asks for urgent funds.

Travel scams. Christmas is one of the busiest times of the year to travel. Cyber criminals take advantage of this by setting up fake websites and tricking people into a great deal for travel or related services, like insurance. Another way cyber criminals take advantage of increased travel is by offering 'compensation' for disrupted travel. Never give personal information or share travel plans with anyone you don't know. Always ensure correspondence with an organization is through their official website. If it's too good to be true, it probably is.

ANZ encourages customers to make a PACT to protect their virtual valuables, which means placing the same emphasis on keeping information safe and secure online as one would with physical valuables, such as a house, car or wallet.

PACT is a simple message:

Pause before sharing your personal information (address, date of birth, passwords etc);
Activate two layers of security (voice ID, SMS notification etc);
Call out suspicious messages (emails, text, calls that are urgent, emotive or unusual); and
Turn on automatic software updates (on your phone and other devices).

For media enquiries contact:

Claudia Filer, +61 401 777 324

Visit ANZ.com for more information on staying cyber-safe this festive season.

Check out ANZ's guides for individuals and businesses.