News Release

For Release: 20 July 2023

ANZ encourages customers to be cautious of all online transactions

ANZ is urging customers to remain vigilant to scams and fraud when completing any transaction online. The reminder comes as ANZ customer protection teams see an increasing number of sophisticated new Bond Investment and Business Email Compromise (BEC) scams.

In the last fortnight, ANZ has prevented and recovered more than $3.2 million from being transferred to online criminals from personal or business accounts in these types of scams.

Bond Investment scams typically impersonate well known Australian organisations and financial institutions and target individuals. Generally, victims will be convinced to invest in fake bond offerings. Once the scammers receive the funds, they are often filtered through trading platforms and often onto cryptocurrency – making it difficult to recover.

Business Email Compromise (BEC) scams target businesses, with online criminals posing as a trusted supplier or vendor and collecting payment for goods or services received. Often a business will receive an invoice from a supplier whose email address has been compromised advising their bank details have changed and requesting future payments be paid into a different, fraudulent bank account.

In other variations of the BEC scam, online criminals will send an email to a company's accounts team via a compromised email account, pretending to be a senior executive, requesting the urgent transfer of funds. Criminals can also request recurring salary or rental payments be directed to a new account.

ANZ Head of Customer Protection Shaq Johnson said: "We are seeing a significant increase in scams of this nature and encourage Australians to be very cautious when presented with any investment opportunity, or requests to make payments to a different bank accounts."

"Often, when we speak to customers who have been caught up in BEC or Bond Investment scams, they genuinely believe the person or vendor they have been communicating with is legitimate."

"This often requires a deeper conversation and education from our end to enable them to understand the sophistication and tactics of these criminals."

ANZ has robust technology and systems and experienced staff to monitor and block scams. It remains important for customers to double check out of the ordinary transactions or funds leaving their accounts.

To protect yourself and your business from Bond and Business Email Compromise scams:

- Ensure you have a process in place to identify and action suspicious emails, texts or phone calls.
- Pause before responding to any request for money online, no matter how frequent or ordinary the transaction. If something doesn't seem right, or is unexpected, question it.

- Use the contact details on official company websites to verify any communications from company employees, vendors, or suppliers.
- Activate two-factor authentication (2FA) as well as a strong password to protect the security of your, and your businesses email accounts.

For more information on Bond and Business Email Compromise Scams, visit https://www.anz.com.au/security/types-of-scams/ and the ACCC ScamWatch.

ANZ is continually reviewing and adjusting its capabilities to keep customers safe as new scams emerge and scammers change how they operate. In the last twelve months, our people and our systems have stopped more than $60 million going to criminals.

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 33 50 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.

For media enquiries contact:
Claudia Filer; +61 401 777 324