News Release

5 April 2024

Beware of phishing scams - they open the door to more serious crimes

Following the Easter weekend ANZ is urging people to watch out for phishing scams which open the door for fraudsters to commit serious crime.

Phishing is a way criminals trick people into giving them personal and financial information. They send fraudulent emails or text messages which include malicious links to very convincing websites.

These scams quickly escalate into something much more sinister and include callous manipulation of victims.

"Clicking on a malicious website link in a scam text message can result in a customer losing all of their savings or having their credit card exploited," says Alan Thomsen, ANZ's Head of Customer Protection.

"The criminals behind these scams are highly organised and often mimic bank processes to trick people into paying them money."

Following the holiday weekend ANZ is seeing a spike in phishing scams from criminals pretending to be from legitimate organisations. The texts can seem just real enough that people click on a fraudulent or malicious weblink and enter their credit card or bank account details.

This is often followed by a cold call from a criminal pretending to be from ANZ's fraud team to say the customers' account has been compromised, they'll use the credit card or bank details entered into the fake website to 'verify' the call is genuine.

Customers are then told they need to move money to a safe or secure account to protect their funds.

The customer is then convinced to log into their digital banking and make payments to a 'safe account' or authorise Google Pay to be provisioned to a new device. The money is actually being paid into an account owned or controlled by the criminal and the money is quickly transferred – often offshore.

"We are urging people to be vigilant. ANZ will never ask you to move money to another account to keep it safe or send you a text message that includes a link to a website.

"You should never give the two factor authentication codes your bank sends you to authorise or verify payments to anyone - even the Police," Mr Thomsen said.

ANZ has also seen a rapid increase in the number of scams originating online via social media platforms and search engines.

Over 55 per cent of recorded scams start online, with Facebook marketplace scams the most common.

"Making the payment is the final step in any scam," Mr Thomsen says.

"The majority of scams start online, via social media and search engines, including through paid and promoted content. Given this, more needs to be done to identify and shut down malicious and fake content before people pick up the phone, reply to a text or message, click on a link, or respond to an ad online.

"Greater collaboration across multiple sectors is required to better protect New Zealanders.

"While banks in New Zealand have made a start in setting up an Anti-Scam Centre, we're urging for Government Agencies, like the Police, and other relevant parties to be part of the solution, as this model has been very successful in both Singapore and Australia."

Singapore's Anti-Scam Command draws together considerable Police resources including investigation, intervention, and enforcement under one umbrella and actively involves financial and other institutions in the fight against scams. The Singapore Police announced in September last year that a single operation of the Scam Centre had successfully disrupted more than 800 scams averting potential losses of more than $17.1 million.

Australia's National Anti-Scam Centre, which takes a similar approach, has been running since mid-2023. Early reports suggest, like Singapore, a collaborative, targeted approach that engages all players is more effective at addressing scams.

"ANZ is committed to working constructively with the industry, Government, and other relevant parties to advance initiatives that could help prevent crime and further protect New Zealanders.

"Our collective focus should be on making it harder for criminals to operate in New Zealand, making it harder to target New Zealanders and preventing further harm."

ANZ will **never ask** customers:

- For their banking passwords, PINs, or two-factor authentication codes
- For their credit card details
- To transfer money to a 'safe' account, purchase gift cards or set up a crypto currency account
- To download software or allow remote access to the customer's device
- ANZ will never send you a text message that includes a link to a website

ANZ customers who have been a victim of fraud or a scam should call us immediately on 0800 269 296 (international +64 4 470 3142).

To find out more about how to stay keep safe online, as well as scams to be aware of, people can go to anz.co.nz/banksafe.

For media queries contact: Briar McCormack 021 2801173