News Release

14 November 2022

ANZ urges under-40s to be on watch for online scams

Younger people are falling victim to a surprising amount of online fraud, according to analysis of ANZ customer data.

The data shows younger people are more likely to fall victim to email or text phishing scams that target their digital banking, whereas retirees are more likely to fall victim to scams that start with a call to a landline.

The data shows that sixty per cent of digital banking phishing victims are under the age of 40, and in many cases, the fraud originates from a text message.

ANZ Senior Manager for Fraud Strategy Natasha McFlinn said younger people might feel more confident with their ability to detect scams and were more trusting of information presented to them on their devices.

"It's a reminder that any of us can fall victim to a scam.

"We all use technology in different ways and the way we interact online now means personal information like email addresses, mobile phone numbers and social media account details are often publicly available.

"While this type of information would be insufficient by itself to access a customer's banking, it is the type of information that can be used by scammers to target individuals," Ms McFlinn said.

The data also reveals that 45 per cent of the victims of cold call and remote access scams were over the age of 70.

A quarter of all scams involved customers who were 70 years or older, another 25 per cent were aged between 55 and 70 years old.

ANZ has also seen a 72 per cent increase in cases of card fraud, compared to the same time a year ago, with more than 35,000 cases reported.

"Often the fraudsters pretend to be from legitimate and well-known companies like banks, telcos and government departments," Ms McFlinn said.

"You'd be amazed at how convincing they can be. They win people over, and convince them to give them their card details.

"They'll often start with a phishing attack and then follow up with a phone call. The phone call seems extra convincing because they already have information about the customer from the previous attack."

Sometimes, while the fraudster may not have the physical card, they can make use of a customer's details, including their card number, card expiry, PIN, CVV number and two factor authentication codes to commit fraud.

In these cases the card details may be obtained through data breaches, phishing, skimming, or scams in which people give away their card details over the phone, or on a fake website.

"Where a customer reports to us that they have lost money to a scam we will make every effort to recover funds," Ms McFlinn said.

"However the speed that transactions often move, combined with the fact that fraudsters will generally remove funds as soon as they hit the recipient account, means this can be very difficult."

That is why ANZ is reminding customers to be careful with their private information.

"It is not a good idea to write passwords or other sensitive information down or share it with anyone, including family members and friends," Ms McFlinn said.

"It's really important to make sure you protect your bank cards by only using them in places you trust, whether that is online or in the real world.

"People should also avoid saving their details on websites or browsers; as well as making sure you don't leave them somewhere the cards or the information on them can be stolen."

ANZ Managing Director for Personal Banking Ben Kelleher said people should not feel embarrassed or ashamed if they have been scammed.

"It's really important to let us know if you think you have been the victim of a scam, or if you spot anything that seems suspicious."

Scam incidents reported to ANZ rose 19 per cent in the twelve months to September 30 2022, compared to the previous financial year.

However, despite the increase in incidents, ANZ's Customer Protection team increased the amount of fraud it prevented or detected by 45 per cent meaning the amount of money lost by customers was at the same level as the previous year.

Mr Kelleher said the bank has increased the resources available to its dedicated fraud team, who review banking activity around the clock for anything potentially suspicious or fraudulent.

"We have expanded our team by 25 percent in the past year and will soon be implementing new technology that will enable us to automate our fraud alerts so they can be resolved more quickly," Mr Kelleher said.

ANZ is implementing a new system where if the bank spots a suspicious transaction an alert can be sent to the customer; they can then respond with a "Y" if they made the transaction and "N" if they didn't.

ANZ has released the data as part of Fraud Awareness Week, a global effort to minimise the impact of fraud by promoting fraud awareness and education.

"Fraud Week is a good reminder to all of us to remain vigilant, be alert to scams, and careful with our private information," Mr Kelleher said.

Staying safe from scams

- Avoid using your internet banking password for anything else and make sure you do not save it to your browser.
- Keep your device operating system, apps and anti-virus software up to date and ensure all your devices are protected with a PIN, password or biometric.
- Report any scam calls you receive directly to your telecommunications provider.
- Always access Internet Banking through the banks website, not from links in text messages or emails.
- Never allow anyone who calls you out of the blue to have remote access to your devices
- Never provide or confirm your credit card details, Internet Banking log in details, PINS and two factor authentication codes in response to a phone call you've received out of the blue, even if they say they are from the bank or the Police
- If you think you have been the victim of a fraud or scam contact your bank immediately.

For media enquiries contact Briar McCormack 021 2801173

Where we talk about people having their digital banking targeted this refers to where people had something happen through their online accounts. For example, they may have been tricked into giving away their Internet Banking login details, or manipulated into making a payment from Internet Banking or goMoney to a scam.

Card fraud is where the transaction occurs on the card. For example someone giving away their card details, card details being accessed through a data breach and used without your permission, card skimming, etc.