News Release
ANZ Scam Safe

For Release: 4 April 2024

Don’t let them in: ANZ encourages customers to know the signs of a remote access scam

Scamwatch reported more than 8,000 incidents of remote access scams in 2023, resulting in more than $15 million of financial losses for Australians.

In remote access scams, criminals make unsolicited contact with victims, usually by text, phone, or email. They impersonate a legitimate company or government agency, such as a telco, bank, police or software provider, to gain remote access to a customer’s device for a fictitious reason, such as to fix a technical issue or to prevent their account being hacked.

The scammer may instruct the customer to download apps or software to allow access to the customer’s bank accounts and transfer funds or persuade the customer to do so.

ANZ encourages customers to be vigilant to all scam types, and to always stop, pause and consider any unsolicited request to access your personal computer, phone, or device.

ANZ Scams Portfolio Lead, Ruth Talalla said: “Scammers play on human emotions and use them to their advantage. They know a lot of people don’t understand the ins and outs of their technology, and so they use this to exploit the fear that their security, or finances, are in danger.”

“It’s important to be sceptical of any unsolicited contact, particularly if it is accompanied by a request to download an app, gain remote access to your device or ask for your banking details. If ever you’re unsure, cease the conversation, hang up the phone and instead contact the organisation through a legitimate channel found through their website.”

How to spot a remote access scam:

- **Unsolicited contact**: Be cautious of unexpected contact claiming to have detected issues on your device or with your bank account. Legitimate companies don't initiate contact in this manner.

- **A sense of urgency**: Scammers want you to act quickly and may claim an issue requires immediate resolution. Genuine tech support or financial or government institutions should always include identity and security checks and you should always be able to ring them back on a number you’ve independently sourced from the organisation’s legitimate website.

- **Request for remote access:** While many genuine tech companies do use remote access technology, it’s unlikely they would initiate contact with a customer directly.

- **Unconventional payment requests:** Be suspicious if a technician asks you to buy software or sign up for a service to fix your computer, or a bank or government agent tells you they’re putting funds into your account to help ‘catch a hacker’. Be suspicious of any requests to transfer funds they say they’ve credited to your account. Legitimate companies or government agents will not ask you to do this.

- **Request access to your banking**: While the scammer is using your device remotely, they might ask you to log in to your online banking so they can make a test payment or refund. They may also ask you to leave the room or put down your

phone – this is so they can access passcodes sent to you to make transactions from your account. Genuine companies will never ask you to do this.

- **Be aware of unexpected One-Time Passwords (OTPs):** If you see passcodes being sent to your mobile phone or device by your bank when you are not making or authorising anyone else to make transactions from your account, hang up the phone, delete any app or software you have been asked to download and contact your bank immediately.

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

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.

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 *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.