News Release

For Release: 15 January 2026

Banks and Telcos Use Kiwi Tech to Block Phishing Websites

Banks, telcos and digital platforms are teaming up with a New Zealand start-up to boost efforts to disrupt and block phishing websites before they can harm customers.

The initiative began as a pilot led by ANZ NZ and 2degrees, and now includes Kiwibank, TSB, One NZ, Spark and Trade Me.

“The aim is to detect, validate, block and disrupt malicious domains within the first hour of a webpage going live,” says Alan Thomsen, Head of Customer Protection at ANZ NZ.

“We want to block those sites before our customers might view them and be put at risk of being scammed.”

For security reasons, the name of the New Zealand tech company is not being made public.

The companies involved in this collaboration have already disrupted over five thousand domains in the past two months.

The technology has also helped reduce card phishing cases involving ANZ customers by 39 percent in two months, highlighting its effectiveness in protecting people from online scams.

An estimated twenty thousand New Zealanders fall victim to phishing scams every year, costing them financially and emotionally.

“That’s why we have been working so hard to combat these scams,” says Mr Thomsen.

“We’re excited to be working with a New Zealand tech company to use their technology to disrupt these malicious sites faster and across more organisations.”

“Phishing” websites are designed to trick people into revealing personal information such as a customer’s name, credit card number, or login details. Some try to install malware or remote access tools that can enable larger, more sophisticated scams.

“Cross-industry co-operation is vital to swift and accurate identification and disruption of scams,” says Ivan Reutskiy, GM Security at 2degrees.

“We are proud of the advances we have made with ANZ and others in this space, to help make people safer online.”

He would like to see more Kiwi organisations join the programme to help disrupt the scam websites quickly and more effectively.

“As scams become more complex and AI-generated attacks rise, we’re not just reacting to fraud, but disrupting the scammers before they can contact the New Zealand public,” says Mr Thomsen.

“It’s another way we’re building a safer banking experience for our customers and the wider public. Phishing websites are becoming more sophisticated. So, we all need to stay vigilant.”

Staying safe online:

- **Be cautious with unexpected messages:** Phishing scams often start with emails or texts that look like they’re from trusted sources - like banks or government agencies. ANZ warns that clicking on malicious links in these messages can lead to serious consequences, including losing your savings or having your credit card exploited.
- **Watch for impersonation tactics:** Scammers may pretend to be ANZ staff or fraud team members. They use convincing language and mimic real bank processes to trick people into transferring money or revealing sensitive information.
- **Stay updated on current scams:** ANZ regularly publishes alerts about the latest scams, including fake investment offers, mobile wallet fraud, and impersonation schemes. Keeping informed helps you recognise red flags before it’s too late.
- **Report suspicious activity immediately**: Contact us immediately if you become aware of anything that’s out of the ordinary with your banking, or you believe your accounts might have been compromised. You can call us 7 days a week, 24 hours a day on 0800 658 044. Or from overseas: +64 9 522 3010.

- **Stay up to date with the latest advice:** Own Your Online has a raft of material and the latest tips to help people stay secure online. For more information on ANZ NZ's scam and fraud prevention measures - including tips for banking safely - go here.

For media enquiries contact:

Tony Field
External Communications Manager
Tel: +64 21 220 3152