Media release

6 June 2023

DIA warns scammers over ‘toll’ scam

Stop what you’re doing and hand yourself in, is the message to scammers responsible for the ‘toll’ scam, from Te Tari Taiwhenua, Department of Internal Affairs (DIA).

The ‘NZTA toll’ phishing scam has been circulating Aotearoa New Zealand since late 2022. It presents itself as genuine SMS text messages from legitimate organisations such as Waka Kotahi – New Zealand Transport Agency, NZ Post, Inland Revenue, and numerous New Zealand-based banks. It also includes gambling and prize scams.

DIA wants scammers to know it is working closely with mobile network operators, New Zealand banks and government agencies NZ Police and CERT NZ to investigate the scam, and to stop those responsible in their tracks.

“We are seeing cases where everyday New Zealanders have lost their entire life savings to this scam, in some cases upwards of $10,000”, says John Michael, Deputy Director Operations at DIA. “We want to be clear to the scammers that by sending scam SMS messages, you are targeting fellow New Zealanders. This has to stop.

“If you are involved in sending these scam messages, you are committing a crime. Please step forward and contact us at info@antispam.govt.nz. Failure to do so will result in us pursuing our investigations, and if you are found guilty of sending scam messages, you could be fined up to $200,000.

“We work closely with NZ mobile network operators and NZ Police and are aware of scam technology currently operating in main townships and city locations in both the North and South Island. We are confident in our ability to identify the users of this technology.”

DIA reiterates that if you are involved in this scam, you may be inflicting harm on your friends, family or whānau. If you’ve been approached about a business opportunity that involves sending large amounts of SMS text messages, are thinking about it, or know someone who has, DIA needs to speak to you. Please get in contact at info@antispam.govt.nz.

If you have information relating to the persons responsible, please contact DIA at info@antispam.govt.nz. Or, to report anonymously, head to [www.crimestoppers-nz.org/police](http://www.crimestoppers-nz.org/police) or call Crime Stoppers free on 0800 555 111.

If you think you are a victim of the phishing scam relating to NZTA, Inland Revenue, NZ Post, or a bank, please contact NZ Police either by calling 105 or reporting it online via the 105 website, quoting ‘Operation Lime Green’. You can also visit your local police station.

If you receive a scam SMS text message, please report it free of charge by forwarding the message to 7726 and following the prompts.

**Advice for the public for dealing with scams**

* Remember - not all messages will look the same, as scammers change their wording over time.
* Do not engage with or click any links before you know a message is genuine.
* To check if a message is genuine, check directly with the people it came from. Go to the organisation’s website or check your online account directly.
* Scam messages commonly contain bad or irregular spelling and grammar. Use this as your first sign that this could be a scam.
* Never provide any card or personal details if you do click a bad link.
* If you have paid money already, speak to your bank as soon as possible and let them know what’s happened.
* It can be harder for people that don’t frequently use their phone to recognise a scam, such as the elderly or vulnerable. Check in with your whānau to help them learn how to avoid falling victim to an SMS scam.
* Head to our website for a step-by-step guide of how to report spam: [How to report SMS spam](https://www.dia.govt.nz/Spam-Complain-About-TXT-Spam)

Ends

Notes for media

* We have spokespeople available to interview about this topic.
* We cannot share any detailed information about ongoing investigations.

Media contact:

Media desk
Te Tari Taiwhenua Department of Internal Affairs
Mobile: +64 27 535 8639
Email: media@dia.govt.nz