

## Keep yourself secure.

While in lockdown and having a greater reliance on technology to stay connected, it is important to keep yourself safe from internet scammers.

A useful resource is cert.govt.nz, a government website that responds to cyber security threats in New Zealand. It has guides on internet safety and keeps up to date with the latest scams.

Here are some of the recent attempts by scammers to get their mitts on your details and finances from Certnz well as some from the IRD and NZTA websites.

### IRD SCAM

22 September IRD has reported a Tax assessment refund scam. An example of a fake message and details of how to tell is below.

**From:** Inland Revenue <mailto:support@mygreens.ga>  
**Sent:** Wednesday, 22 September 2021 7:45 a.m.

Not from an Inland Revenue email

**Subject:** Tax Assessment has been made and you are eligible for 824.90 NZD



## Kia Ora from Inland Revenue

Tax Assessment has been made and you are eligible for **824.90 NZD.**

We will not include dollar amounts in our refund emails

Tax refunds are processed automatically, unfortunately that didn't happen as we don't have your details up to date. Please follow the link below to confirm:

**Error! Filename not specified.**

Original URL:  
<https://aghslaw.net/ird/ir%20revenue/index.html>  
Click or tap to follow link.

CLICK TO CONFIRM

Thanks,  
Inland Revenue Team

Inland Revenue is not Copyright

Does not go to an Inland Revenue website

• © Copyright 2021 Inland Revenue

A reminder that the IRD will never include dollar amounts in their refund emails or request your credit card information. If you are in any doubt as to whether you applied for a tax refund, contact the IRD directly through their official website or phone number. Do not use contact information from an email you are unsure of.

## JONES ROAD AUTO

Recently an email informing people that “Your vehicles licence (rego) expires soon” supposedly from the NZTA has been making the rounds.

This is a very convincing looking email, however the major tell is that the sender, which reads as NZ Transport Agency office@jonesroadauto.co.nz

Any mail from the NZTA will end in @nsta.govt.nz

An example of a scam email from the NZTA is shown below along with the tell tale signs of a scam.

The image shows a screenshot of an email interface with several red annotations pointing to suspicious elements:

- Sender:** The sender is identified as "NZ Transport Agency" with the email address "<no.reply@nzta.co.nz>". A red circle highlights the sender's name, and a red arrow points to the email address with a callout box stating "Not from @nzta.govt.nz".
- Subject:** The subject line is "Your **VEHICLE's** licence (rego) expires soon". A red circle highlights the word "VEHICLE's", and a callout box notes "Doesn't include your specific details like vehicle make, plate or expiry date".
- Link:** A blue link is provided: "http://transact.nzta.dnsdojo.com/inter/transact.nzta.govt.nz/transactions/renewvehiclelicence/". A red circle highlights the link, and a callout box states "Hovering over links show you they don't go to nzta.govt.nz".
- Call to Action:** A blue button labeled "Renew now" is present. A red arrow points to it from the same callout box as the link above.
- Content:** The email body contains text such as "The vehicle must have a current entry= fitness before you can renew.", "Check your WoF/CoF expiry date", "It costs \$103.79 for 12 months if you renew online.", and a list of details: "how the fees are made up", "other licence periods and costs", and "more details about your vehicle." The NZ Transport Agency logo is also visible.

## NZ POST

NZ post has reported a Phishing email (an email made to look like the genuine article in hopes of getting your details) telling customers

They remind you that any official mail from the NZ Post will end with [@nzpost.co.nz](mailto:nzpost.co.nz) or [@courierpost.co.nz](mailto:courierpost.co.nz) and advise you to not click any links in any suspicious emails and to delete them immediately.



**New Zealand Post** 

**There's a package waiting for your confirmation!**

**Dear**  
We from New Zealand Post would like to celebrate our success with you and therefore we have a special action where our customers can receive a free package!

Confirm your package by answering 3 questions on the next page, which only takes a few minutes, and we deliver the surprise package directly to you!

**Note:** *Only (32) packages left!*

**I WANT A PACKAGE!**

If you'd prefer not to receive occasional emails from us, you can [unsubscribe](#).

## TEXT MESSAGE SCAM

Certnz is warning people of a text based scam that can infect android phones with a flubot, a malicious app made to record login details.

According to Certnz, The wording of the text messages may be about a parcel delivery or that photos of the recipient have been uploaded or a voicemail. In all cases there will be a link, asking you to install an app or a security update. Below are some examples of what these messages may look like.

The image displays three screenshots illustrating a text message scam. The first screenshot shows a message titled "Download our application to track your parcel" with a photo of a delivery person and a "Download application" button. Below the message is a numbered list of instructions for installing the app. The second screenshot shows a "Spark" voicemail notification with a table of details: "Your phone number" (288991721) and "Message length" (2 minutes and 34 seconds). It includes a "Download voicemail app" button and a warning to enable installation of unknown apps. The third screenshot is a red system warning titled "Your device is infected with the FluBot® malware" with an "Install security update" button and a tip to enable installation of unknown apps.

**Download our application to track your parcel**

Download application

How do I install it?

1. When we download an .apk file, it will be the application from which we download it that will warn us that the process is blocked.
2. At the bottom of the screen we will see a warning stating that "applications from unknown sources cannot be installed" and invites us to enter the "Settings".
3. Inside the application we look for the section "install unknown applications" and activate the checkbox.
4. From that moment on, that application has permissions to install external

**Spark: You have new voicemail**

Your phone number	288991721
Message length	2 minutes and 34 seconds

This voicemail is in a high quality format and can only be listened to with our app.

Download voicemail app

If a window appears preventing the installation, select "settings" and enable the installation of unknown apps.

**This type of file can harm your device. Do you want to keep Voicemailx3.apk anyway?**

CANCEL OK

**Your device is infected with the FluBot® malware**

Android has detected that your device has been infected.

FluBot is an Android spyware that aims to steal financial login and password data from your device.

You must install an Android security update to remove FluBot.

Install security update

If a window appears preventing the installation, select "settings" and enable the installation of unknown apps.

It is important that you do not click any links in these types of messages and delete them.

If you have clicked the link, it is advised that you change your passwords and contact your bank as a precaution.

If you clicked the links and downloaded anything it is advised you do a factory reset on your phone, this will remove any apps that do not come factory standard with the phone, you change your passwords and contact your bank to check any suspicious activity.

## **PAYPAL (YOU'RE A WINNER!!!)**

Emails claiming to be from Paypal, either warning of an account closure or that you have credit waiting are still very common. The Paypal website advises customers that they will never ask for you to enter your password unless it is at the official paypal.com login page.

If you have been advised you have been paid into your paypal account or that you owe money (and if you actually have a paypal account in the first place) go to the official website [www.paypal.com](http://www.paypal.com) and check for yourself. Do not click any links in the email.

As always remember to check the sender. Hovering your mouse over the sender name will bring it up in full. Remember to err on the side of caution. If it looks too good to be true, it probably is.

### **Things to remember**

**CHECK THE SENDER**

**CHECK THE SPELLING AND GRAMMER**

**DON'T CLICK THE LINK**

**GO THROUGH OFFICIAL CHANNELS**

**IF IT'S TOO GOOD TO BE TRUE, IT IS**