Keep yourself secure.

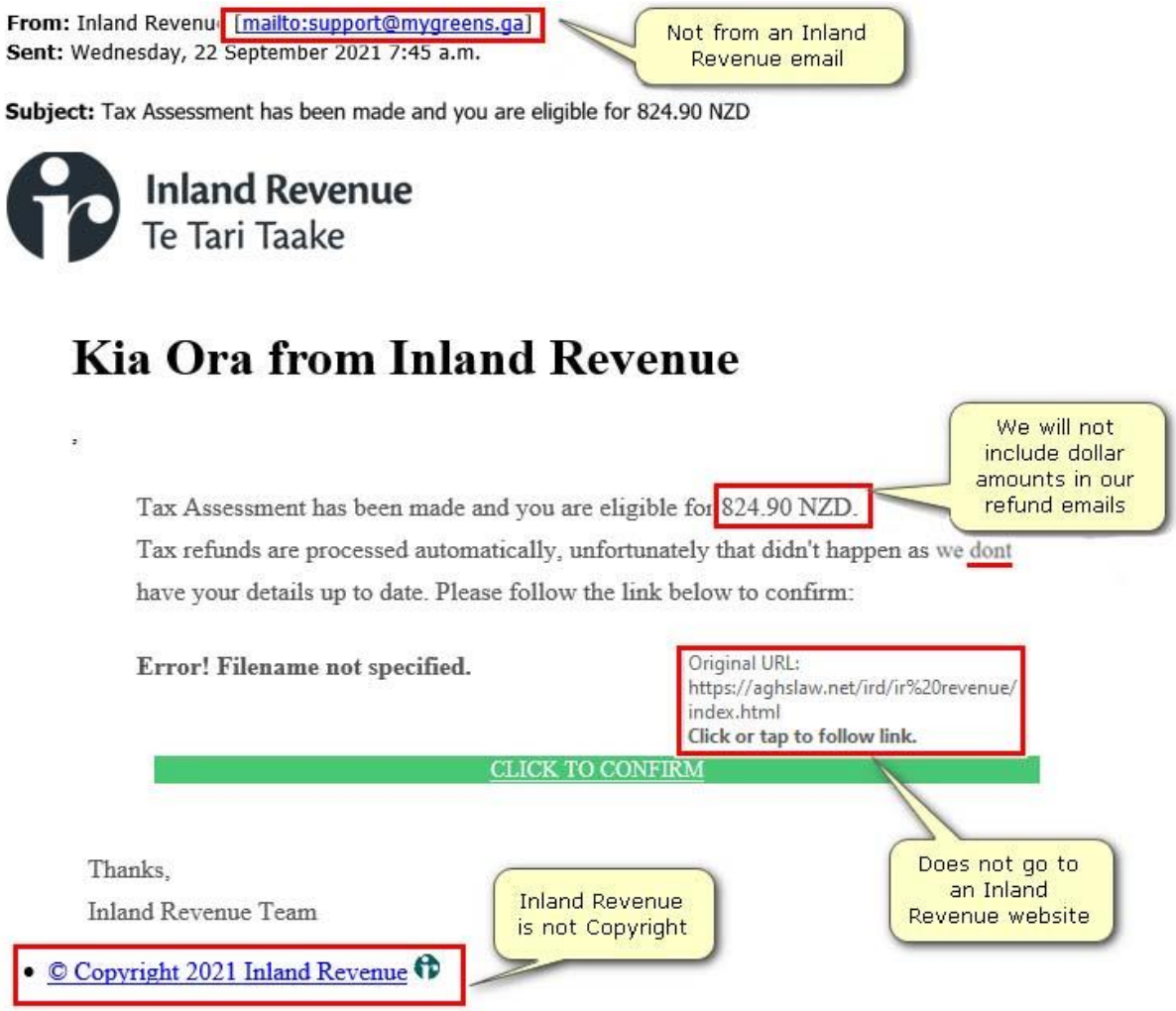
While in lockdown and having a greater reliance on technology to stay connected, it is important to keep yourself safe from internet scammers.

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.



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.

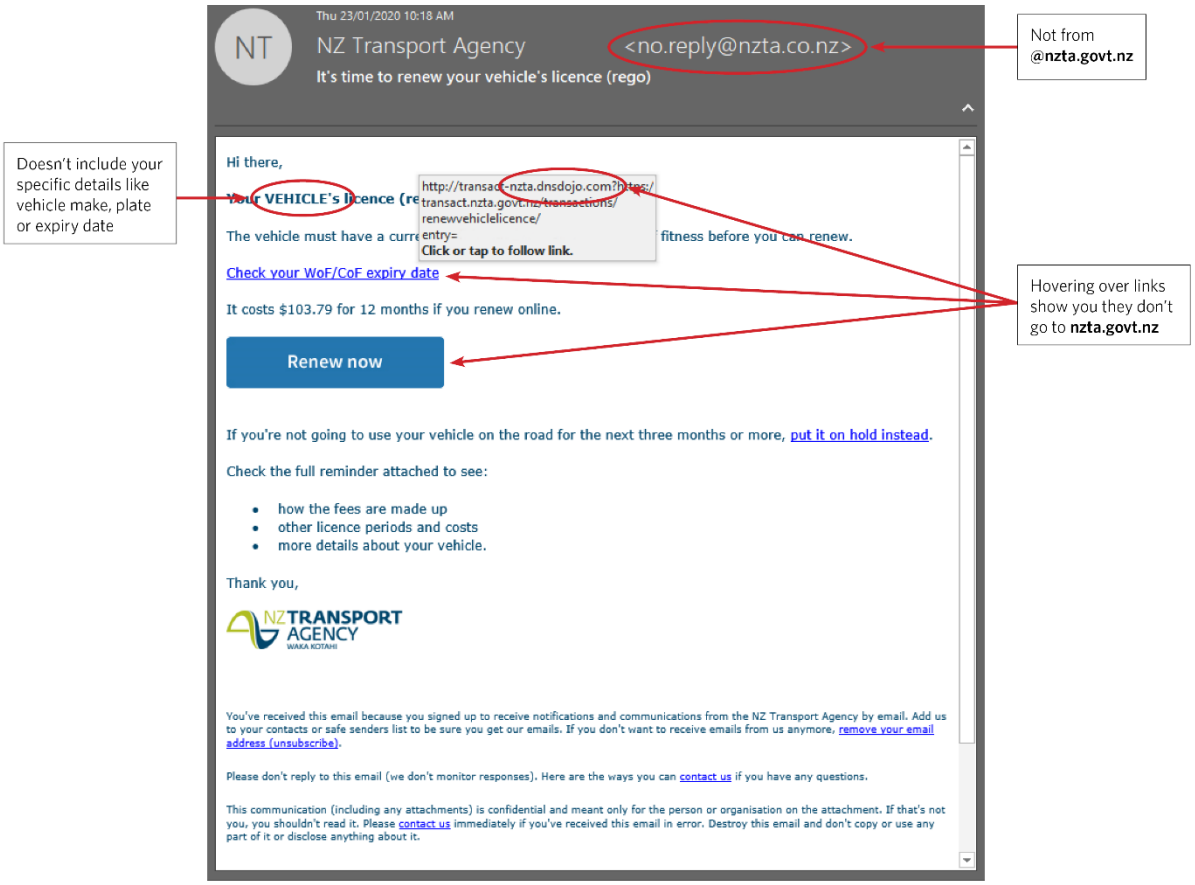
JONES ROAD AUTO

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.



NZ POST

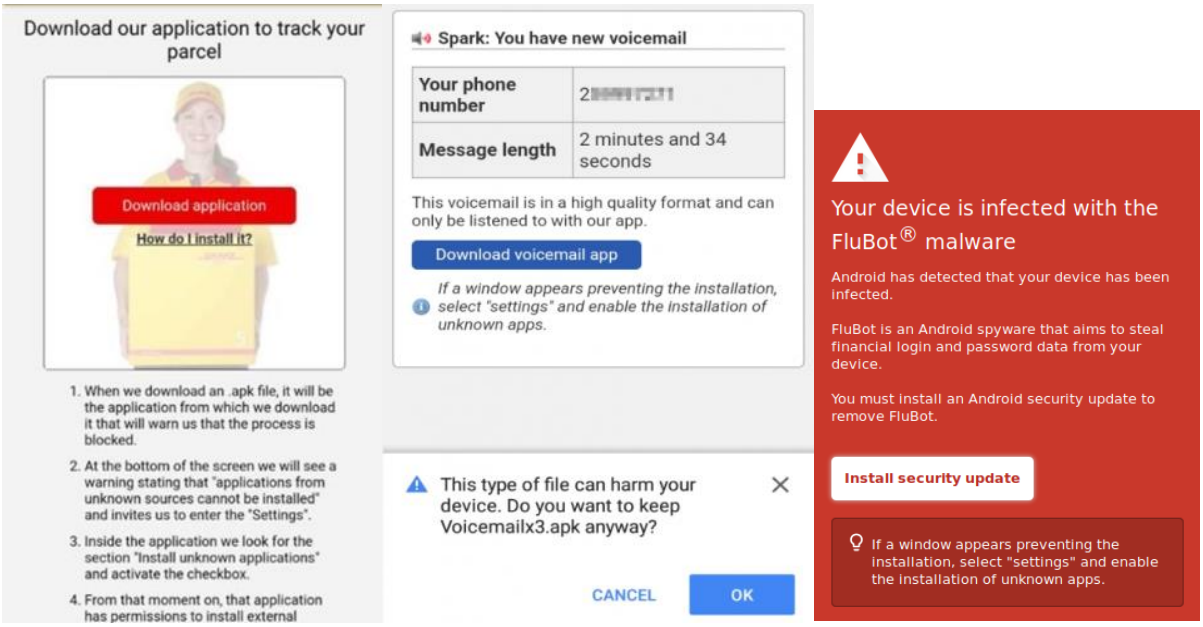
NZ post has reported a Phishing email (an email made to look like the genuine article in hopes of getting your details) telling customers

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

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.



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 advices 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 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