

February 2024

Own Your Online

Online Security Basics for Business

Who are we?



Sam Leggett
Senior Analyst, Threat
and Incident Response



Hadyn Green
Senior Advisor, Engagement,
Communications and Partnerships

About CERT NZ

CERT NZ is the government's public-facing cyber security agency. We run the Own Your Online website – a resource for individuals and businesses to raise understanding of cyber security.

CERT NZ also provides the following services.

- Helping businesses (and individuals) affected by cyber incidents.
- Scam prevention initiatives with industry partners to detect and prevent cyber crime at the source.
- Regular stats about cyber security, which help us see the threats coming up.

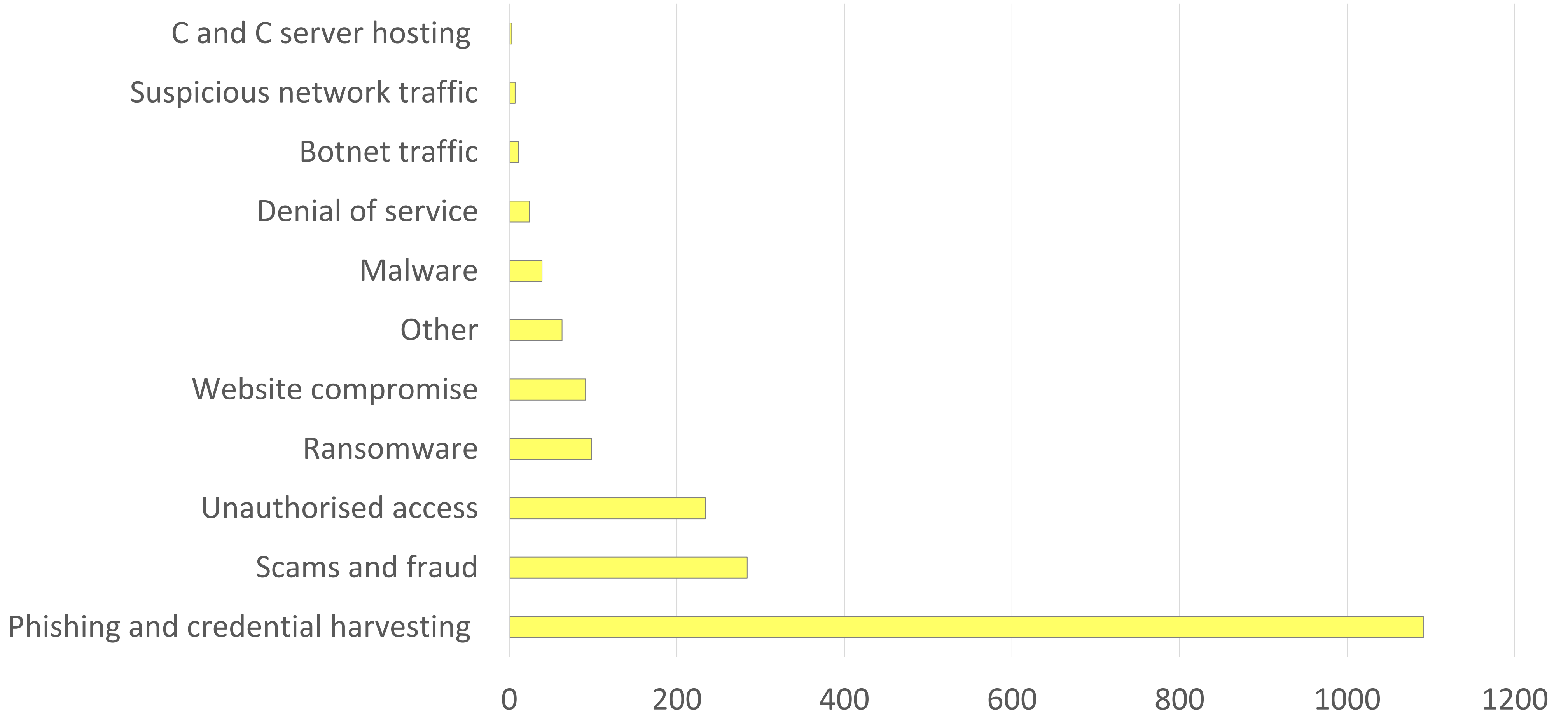
Today's agenda

We're going to cover off:

- Common threats for businesses
- Practical tips
- How to implement the basics

Common threats

Breakdown of incidents affecting organisations 2021 - 2023



'Phishing'

Phishing is the practice of sending messages – via email or text message – pretending to be from someone reputable. The intent is to trick you into revealing personal or financial information, or doing something which compromises your security.

Phishing is often the first thing scammers do before moving to more disruptive attacks.




**Don't
expose
your life
online.
Own it.**

Whatever you're doing online, you can be exposed to a cyber attack. Visit ownyouronline.govt.nz and learn how to protect your life online.

Phishing emails

What to look for

From: Inland Revenue <xatosi@krf.biglobe.ne.jp>
Sent: Monday, May 15, 2023 9:22 AM
Subject: [SPAM] Your refund tax are now av... (0-000061-393534-008)



COMMUNICATION OF INCIDENCE IN THE 2021-2022 INCOME STATEMENT.

In relation to the resolution issued by this Provincial Directorate of the Inland Revenue Department, we have recalculated your last taxable income declaration (Model 100. Personal i...)

This resolution informs that it has pending receipt of \$596.09 NZD.

You must request it within 10 business days confirm... ent Billing Address by email at review-office@refund-update-ird-govt-nz.com.

You must confirm your Current Address and also attach photocopies of your Passport and Driver Licence in order to confirm account ownership.

After said term, the corresponding resolution will be issued.

The Inland Revenue Department, in accordance with the provisions of article 21.3 of the aforementioned Law 39/2015, of October 1, after said period according to article 25.I.b of the same law, the expiration of the procedure will occur and the file of proceedings.

Not from an Inland Revenue email address

We do not put bill or refund amounts in emails

This is not an Inland Revenue email address

Thu 23/01/2020 10:18 AM

NT NZ Transport Agency <no.reply@nzta.co.nz>
It's time to renew your vehicle's licence (rego)

Hi there,

Your VEHICLE's licence (re...

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.


[Renew now](#)

If you're not going to use your vehicle on the road for the next three months or more, [put it on hold instead](#).

Check the full reminder attached to see:

- how the fees are made up
- other licence periods and costs
- more details about your vehicle.

Thank you,



You've received this email because you signed up to receive notifications and communications from the NZ Transport Agency by email. Add us to your contacts or safe senders list to be sure you get our emails. If you don't want to receive emails from us anymore, [remove your email address \(unsubscribe\)](#).

Please don't reply to this email (we don't monitor responses). Here are the ways you can [contact us](#) if you have any questions.

This communication (including any attachments) is confidential and meant only for the person or organisation on the attachment. If that's not you, you shouldn't read it. Please [contact us](#) immediately if you've received this email in error. Destroy this email and don't copy or use any part of it or disclose anything about it.

Doesn't include your specific details like vehicle make, plate or expiry date

Not from @nzta.govt.nz

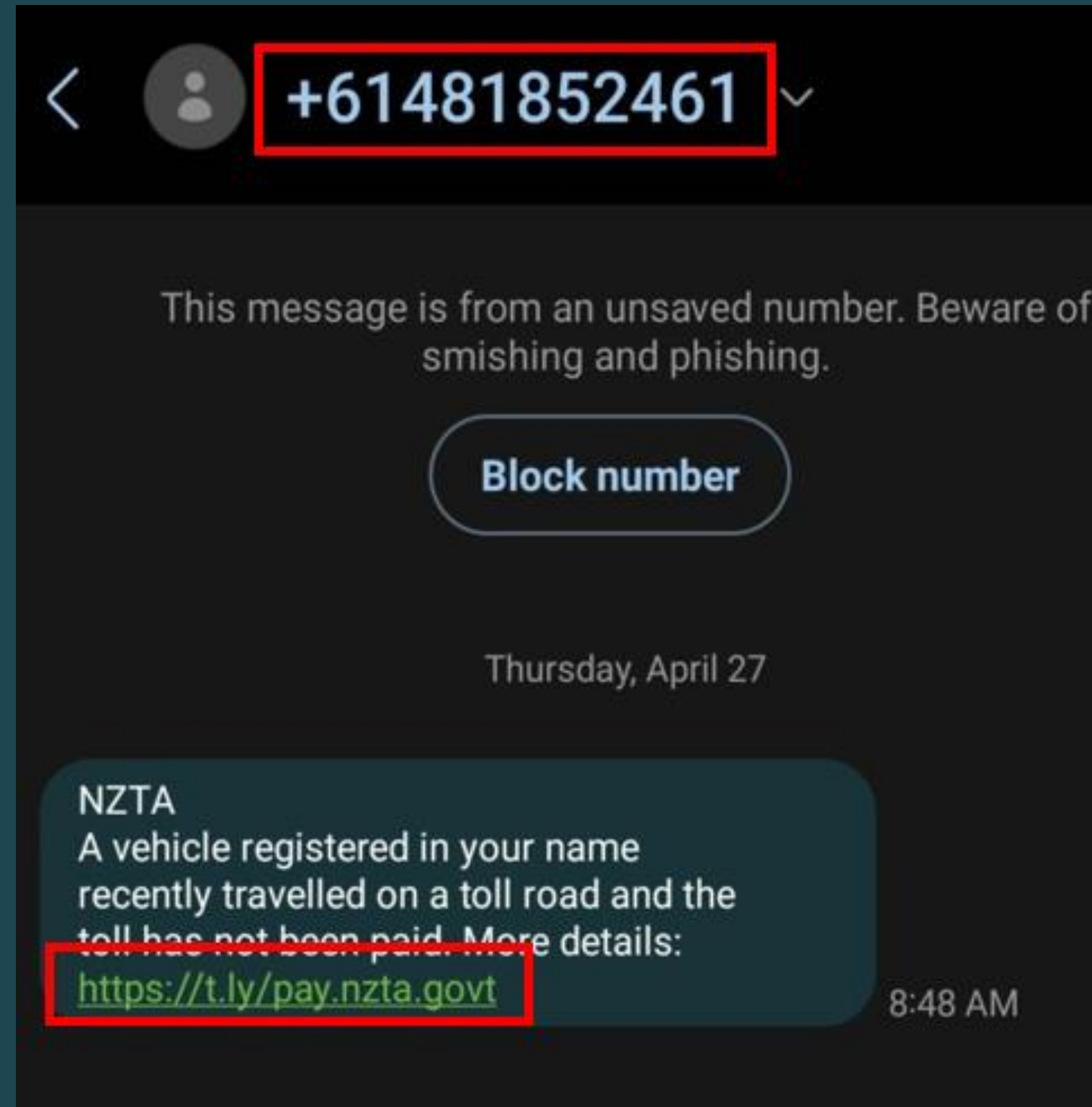
Hovering over links show you they don't go to nzta.govt.nz

Phishing text messages

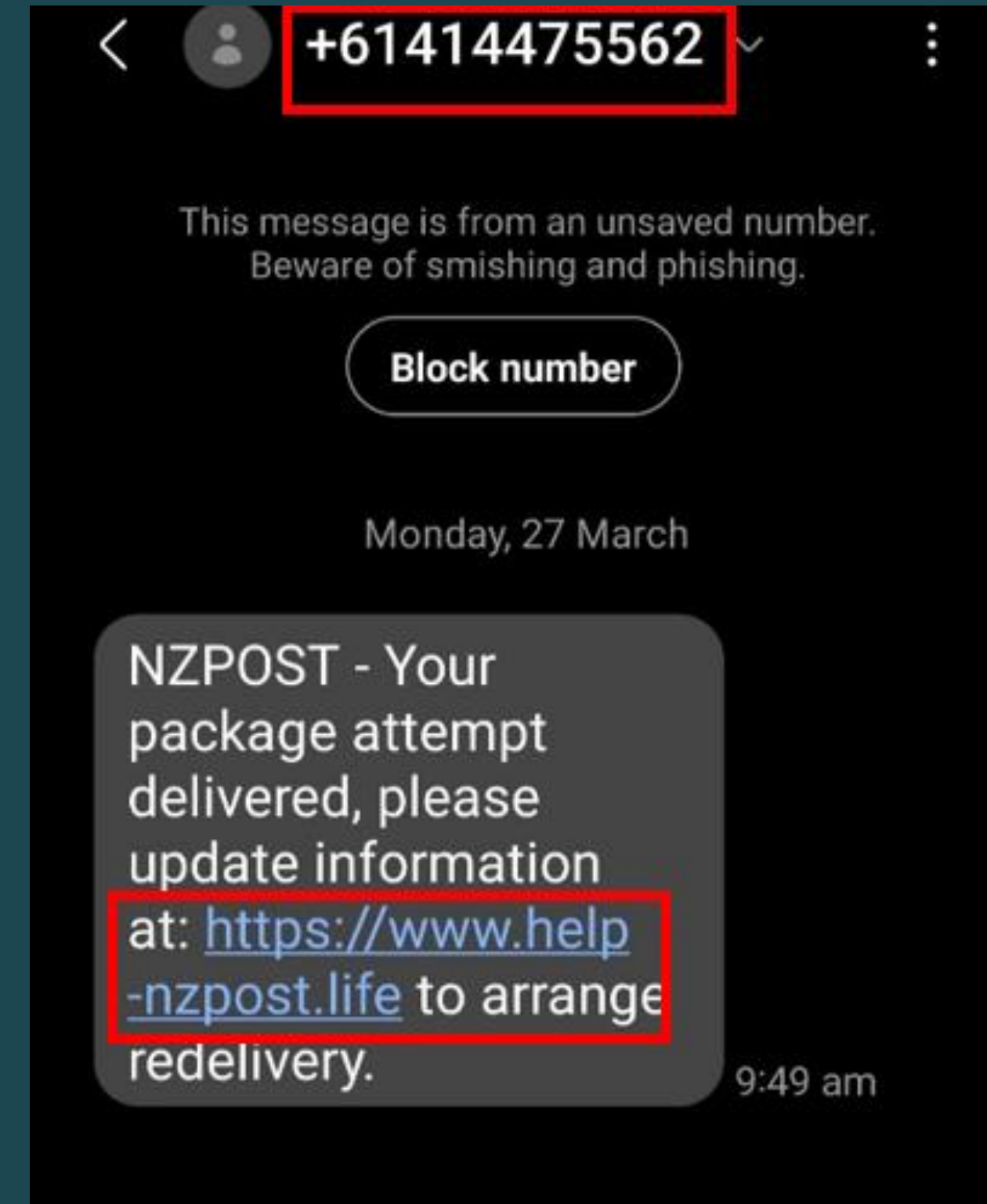
What to look for



- Sent from a phone number not a four-digit 'short code'
- Not a real BNZ website



- Sent from a phone number not a four-digit 'short code'
- Phone number uses Australian area code (+61)
- Not a real NZTA website



- Sent from a phone number not a four-digit 'short code'
- Phone number uses Australian area code (+61)
- Not a real NZ Post website



Practical tips & Implementing the basics

Practical tips:

- Asset Management
- Software updates
- Passwords
- Two-factor authentication
- Principle of least privilege
- Back ups
- Incident response plan

Asset Management

Asset Management is recording, tracking, and maintaining every system asset in your organisation. This includes software and hardware, as well as any cloud-based systems you use.

<https://www.cert.govt.nz/it-specialists/critical-controls/asset-lifecycle-management/>



Software/Services:

- Website
- Email
- Bank Account
- Social Media
- Collaboration
- Invoicing



Hardware:

- Laptops
- Mobile Phones
- Modems/Routers

Software updates

Turn on auto-updates on apps and devices

- Updating devices improves performances and fixes weakness that could let in attackers.
- The easiest way to do this is by going to settings and turning on automatic updates.
- For software that doesn't have an auto-update option, make sure to schedule regular checks for new updates.

<https://www.ownyouronline.govt.nz/personal/get-protected/guides/keep-up-with-your-updates/>





Software/Services:

- Website
- Email
- Bank Account
- Social Media
- Collaboration
- Invoicing



Hardware:

- Laptops
- Mobile Phones
- Modems/Routers



Software/Services:

- Website
- Email
- Bank Account
- Social Media
- Collaboration
- Invoicing



Hardware:

- Laptops
- Mobile Phones
- Modems/Routers



Password Policy vs Password Manager

Passwords Policy

To ensure your employees have secure logins, passwords should...

- Be at least 15 characters long, preferably with numbers symbols and capitals – you can create a passphrase by joining four or more random words together and adding numbers of symbols as needed,
- Be unique, not used for other accounts,
- Not use personal information that can be easily found online – like pet names or birthdays,
- Not use not use common patterns – for example, 1 or ! at the end, @ instead of 'a'.

Strong and unique is better than changing regularly



Password manager

The problem with passwords is that once they are lost or guessed, they're no longer secret or secure. At CERT NZ, we see a lot of unauthorised access incidents which are caused by issues related to password management.

Providing your staff with a password manager is the most effective way to enable them to use unique and strong passwords, and to enable better password hygiene.

Password managers are like a digital vault that keeps all your passwords in one place, so all you to do remember is the password to open the vault. They can also suggest passwords for you that will be almost impossible to crack.

<https://www.ownyouronline.govt.nz/business/get-protected/guides/using-a-password-manager-in-your-business/>





Software/Services:

- Website
- Email
- Bank Account
- Social Media
- Collaboration
- Invoicing



Hardware:

- Laptops
- Mobile Phones
- Modems/Routers



Software/Services:

- Website
- Email
- Bank Account
- Social Media
- Collaboration
- Invoicing



Hardware:

- Laptops
- Mobile Phones
- Modems/Routers

Two-factor authentication

Turn on 2FA as an extra layer of protection

- 2FA is a unique code sent to your phone or taken from an app that only you have access to.
- 2FA stops attackers from accessing your accounts with your log in details and can let you know that these details have been compromised.
- Read 2FA codes carefully and only enter them if the message description matches the action you are taking.

<https://www.ownyouronline.govt.nz/business/get-protected/guides/protect-your-business-with-2fa/>



Software/Services:

- Website
- Email
- Bank Account
- Social Media
- Collaboration
- Invoicing



Hardware:

- Laptops
- Mobile Phones
- Modems/Routers



Software/Services:

- Website
- Email
- Bank Account
- Social Media
- Collaboration
- Invoicing



Hardware:

- Laptops
- Mobile Phones
- Modems/Routers

Principle of least privilege

The principle of least privilege means only having the access you need to do your job.

Restricting the level of access to only what's needed, also restricts the number of things an attacker can do if the account is compromised.

<https://www.cert.govt.nz/it-specialists/critical-controls/principle-of-least-privilege/>



Software/Services:

- Website
- Email
- Bank Account
- Social Media
- Collaboration
- Invoicing



Hardware:

- Laptops
- Mobile Phones
- Modems/Routers



Software/Services:

- Website
- Email
- Bank Account
- Social Media
- Collaboration
- Invoicing



Hardware:

- Laptops
- Mobile Phones
- Modems/Routers

Backups

If you run a business, you know how important it is to keep your data safe. If it's compromised in any way —lost, leaked or stolen — you need to make sure you have a backup copy available so you can restore it.

- Set your backup process to happen automatically, if possible.
- Store your backups in a secure location that isn't on your own systems/servers. If your servers are compromised, your backups may not be available.
- Test your backup process

<https://www.ownyouronline.govt.nz/business/get-protected/guides/backups-for-your-business/>



Software/Services:

- Website
- Email
- Bank Account
- Social Media
- Collaboration
- Invoicing



Hardware:

- Laptops
- Mobile Phones
- Modems/Routers



Software/Services:

- Website
- Email
- Bank Account
- Social Media
- Collaboration
- Invoicing



Hardware:

- Laptops
- Mobile Phones
- Modems/Routers

Incident Response Plan

An incident response plan is a step-by-step guide that documents who will do what, if a cyber security incident occurs.

Having a plan in place *before* an incident occurs will help you take control of the situation, navigate your way through and reduce the impact on your business.

Your plan will depend on the size, scale and operation of your business, but there are some standard elements to consider that will help in recovery.

<https://www.ownyouronline.govt.nz/business/get-protected/guides/create-an-incident-response-plan/>



Reporting scams keeps everyone safe

Report online scams to CERT NZ at www.cert.govt.nz/individuals/report-an-issue/ and we'll work with our partners to shut them down.

You can also:

- forward spam/scam text messages to 7726 (the Department of Internal Affairs),
- report scams on social media to the platform (for example, Facebook), and
- report unauthorised transactions and scam payments to your bank immediately.

Tiakina tō mana tuihono

own your online

Simplifying cyber security



Distributed denial-of-service (DDoS) attacks

DDoS attacks work by flooding a website with multiple false requests to overload the system. During a DDoS attack, your customers may not be able to access yo...



Artificial intelligence

Artificial Intelligence (AI) can quickly create believable scams and phishing emails in bulk.



Insider threat

'Insider threat' is a malicious threat to a business or organisation from someone who has inside knowledge. It's one of the biggest cyber security threats that...



Phishing scams

Phishing scams are one of the most common, prolific and successful attacks we see. Learn how they could affect your business.



Business email compromise

If a scammer gets access to your business email, they can use it to email your contacts to try to get money or personal details from them.



Businesses and ransomware

Ransomware is a type of malicious software that denies a user access to their files or computer system unless they pay a ransom. Attacks can cause huge...



Featured

Business basics

Create an incident response plan

We've outlined some simple steps to help you evaluate how an incident could affect your business and what you'll need to consider when putting an incident response plan in place.

[Read guide](#)



Protect your business



Protect your business against DDoS attacks

Distributed denial-of-service (DDoS) attacks can be complex – find out what's vital to keep your business running in case of an attack, and how to choose the right...

[→](#)

Managing incidents




If you have had an online security incident

Responding quickly to an online security incident can limit the impact to your business. Here's where to start.

[→](#)

Staff security



Types of remote access software

There are different ways to remote into a system or computer. This guide will help you find the right one for your business and circumstances.

[→](#)

Questions and suggestions

Sam Leggett & Hadyn Green

0800 CERT NZ

info@cert.govt.nz

www.cert.govt.nz

www.ownyouronline.govt.nz/business

All the links

Asset lifecycle management

Recording, tracking and maintaining every system asset in your business

About: <https://www.cert.govt.nz/it-specialists/critical-controls/asset-lifecycle-management/>

Creating an asset lifecycle: <https://www.cert.govt.nz/it-specialists/critical-controls/asset-lifecycle-management/creating-an-asset-lifecycle/>

Software updates

Keeping your software and devices updated is one of the most simple and effective steps to take, to ensure your environment stays secure.

<https://www.ownyouronline.govt.nz/personal/get-protected/guides/keep-up-with-your-updates/>

<https://www.cert.govt.nz/it-specialists/critical-controls/patching/>

Passwords

Creating long and strong passwords for your online accounts is one of the most effective ways you can protect your personal information, and keep yourself safe from attackers.

Good passwords: <https://www.ownyouronline.govt.nz/personal/get-protected/guides/how-to-create-good-passwords/>

Password policy for your business: <https://www.ownyouronline.govt.nz/business/get-protected/guides/create-a-password-policy-for-your-business/>

Keep your data safe with a password manager: <https://www.ownyouronline.govt.nz/business/get-protected/guides/using-a-password-manager-in-your-business/>

Have I Been Pwned collects info from multiple data breaches to see if your email address or phone number has been compromised.

www.haveibeenpwned.com

Two-factor authentication (2FA)

As part of your business strategy, you need to think about how to protect both your systems and your customers' accounts. 2FA is one of the tools that can help.

<https://www.ownyouronline.govt.nz/business/get-protected/guides/protect-your-business-with-2fa/>

<https://www.cert.govt.nz/it-specialists/critical-controls/multi-factor-authentication/>

Principle of least privilege

The principle of least privilege means only having the access you need to do your job.

<https://www.cert.govt.nz/it-specialists/critical-controls/principle-of-least-privilege/>

Backups

If you run a business, you know how important it is to keep your data safe. Backups ensure that if any of your data is lost or compromised, you can restore it quickly and easily.

<https://www.ownyouronline.govt.nz/business/get-protected/guides/backups-for-your-business/>

<https://www.cert.govt.nz/it-specialists/critical-controls/implement-and-test-backups/>

Incident response plan

An incident response plan is a step-by-step guide that documents who will do what if a cyber security incident occurs.

<https://www.ownyouronline.govt.nz/business/get-protected/guides/create-an-incident-response-plan/>