certnz

/// Cyber Smart Week
Te Pai Ora o Aotearoa

31 October 2023

/// Computer Emergency Response Team

- We are a government agency.
- We work to improve New Zealanders’ cyber resilience.
- We provide support to New Zealanders affected by cyber incidents.
- We provide educational resources and presentations.
- We publish data and insights on the cyber threat landscape.
- We collaborate with industry and government to prevent cyber threats.

/// Today’s agenda

- Cyber landscape
- Phishing and credential harvesting
- Business account compromises
  - Remote access scams
  - Invoice scams
  - Account takeovers
- Malware and ransomware
- Five simple steps for employees
- Securing your business from cyber threats
- Cyber Smart Week campaign.

Themes and trends in the cyber security environment

2022 annual report highlights

8,160 incident reports

were received.

$20 million

in reported losses.

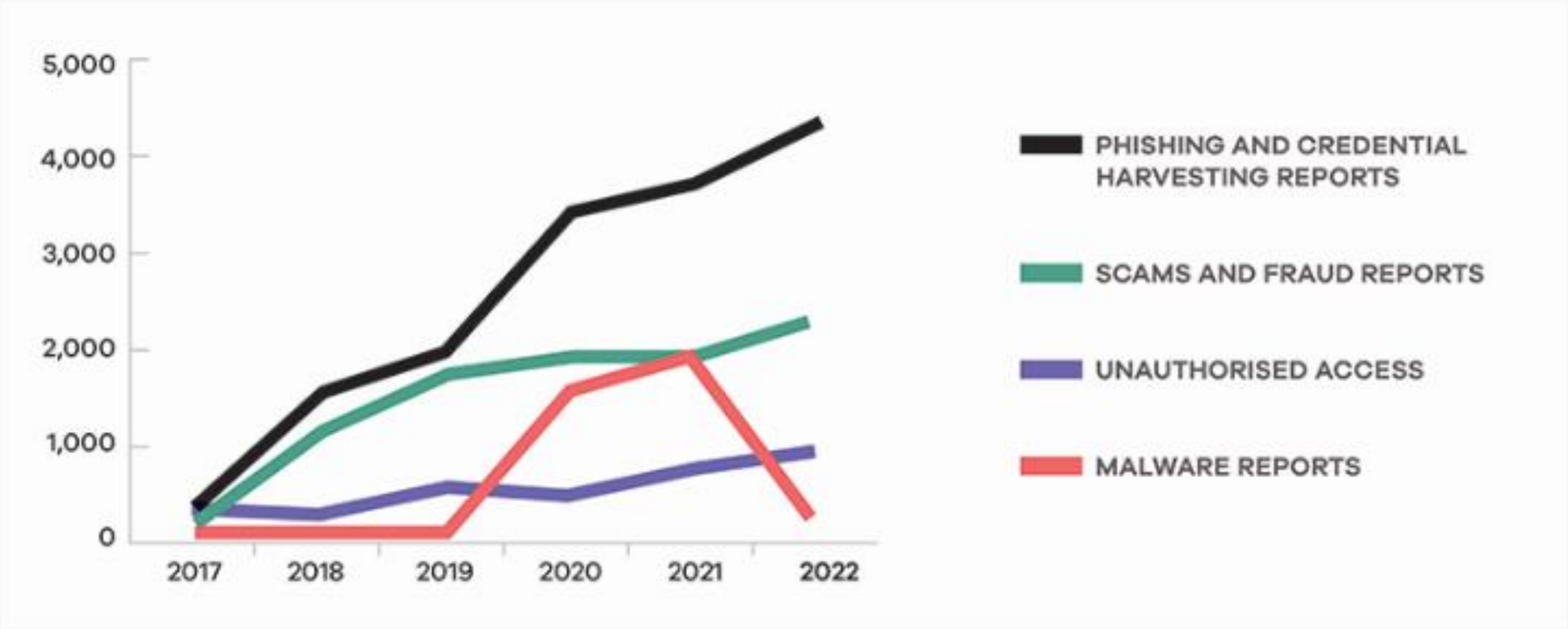
41 vulnerabilities

were reported.

Phishing reports continued to increase

and made up 56% of incident reports.

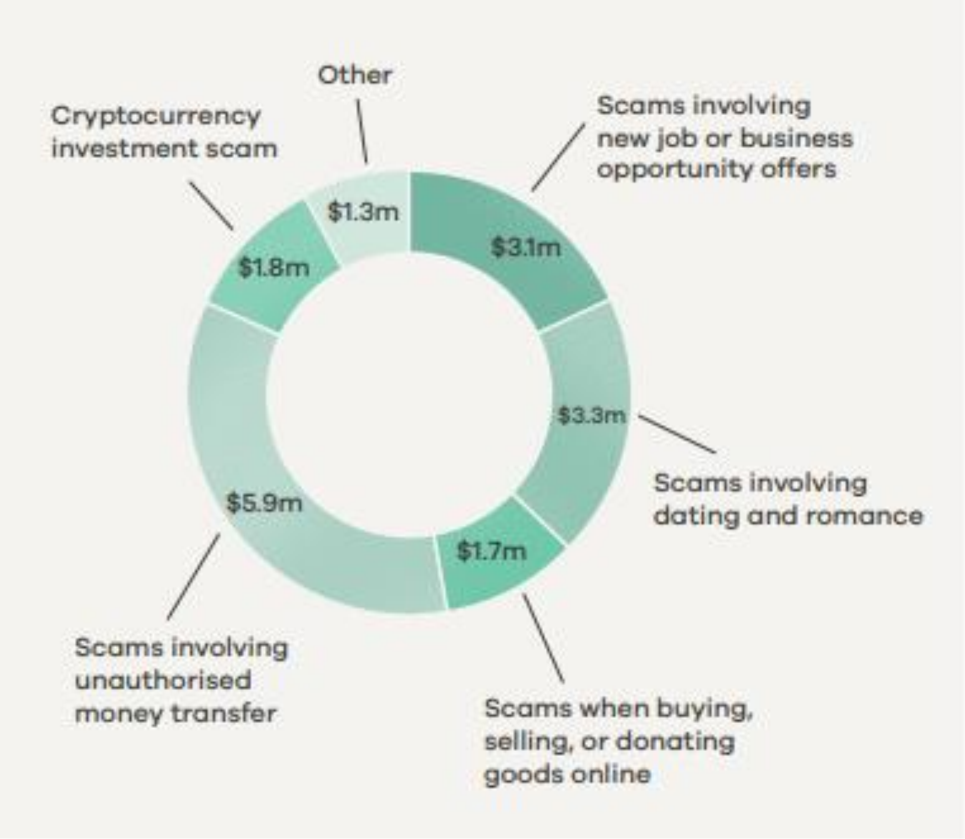
Most reported incident types



/// Breakdown of financial loss in 2022

Of the total of $20 million lost in 2022, scams and fraud accounted for almost $17.1mil – 86 % of overall direct financial loss.

A third involved unauthorised money transfers – with the other two-thirds resulting from people being tricked into transferring money.



Phishing and credential harvesting

/// Phishing scams

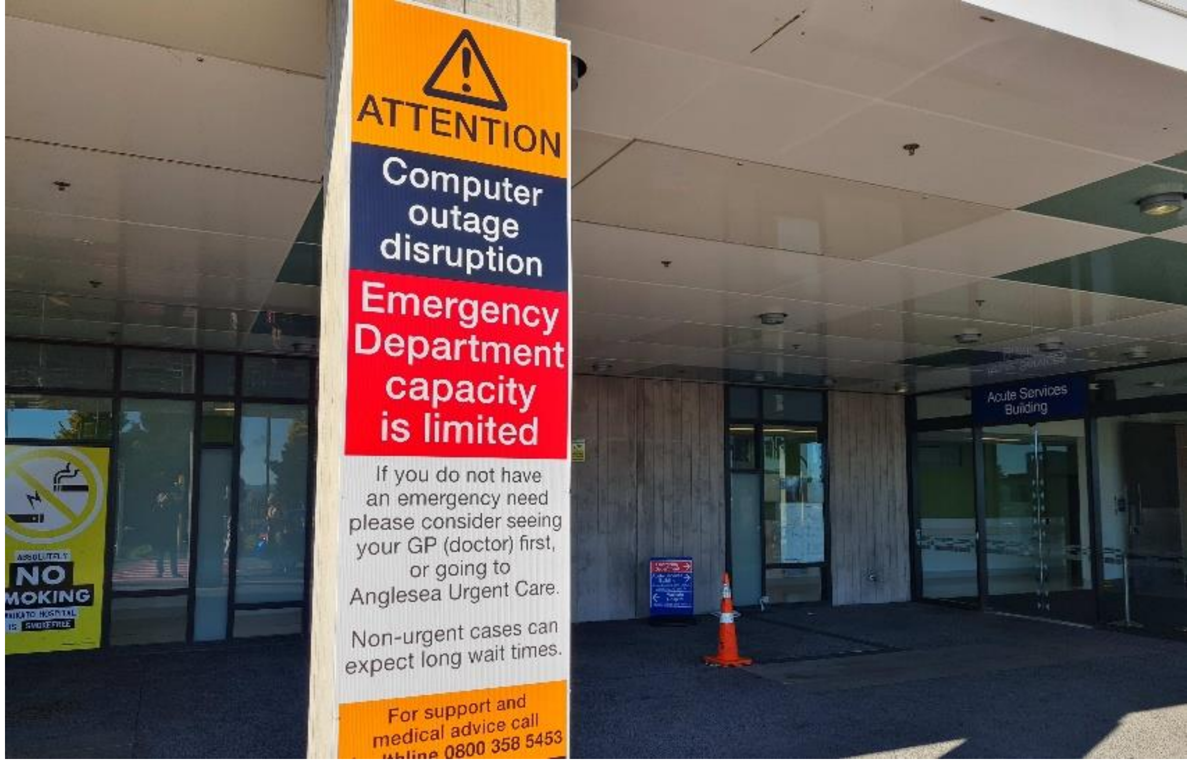
Phishing is the practice of sending fraudulent messages purporting to be from a reputable person or business to induce the recipient to reveal personal or financial information or to take an action which causes them loss or compromises their security.

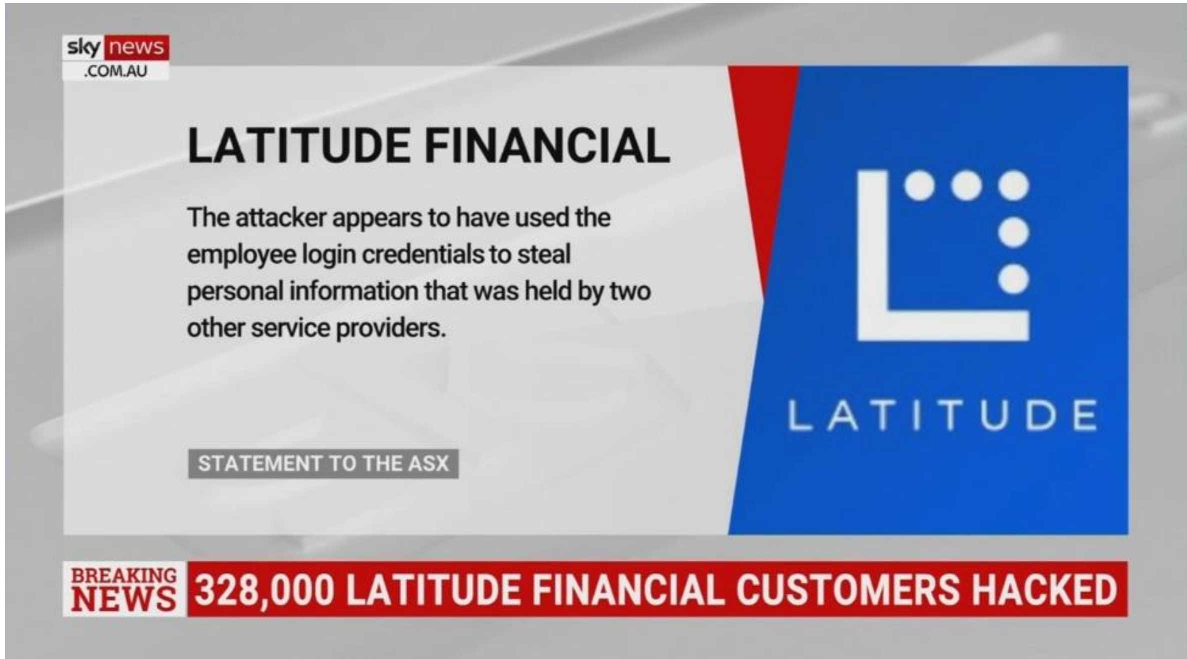
Often phishing is the first line of compromise which leads to more disruptive attacks.

/// Phishing impacts

Impacts of phishing can be significant, and include:

- Financial loss
- Disruption to business operations
- Privacy breaches
- Reputational damage
- Reduction in trust and confidence


ATTENTION
Computer outage disruption
Emergency Department capacity is limited
If you do not have an emergency need please consider seeing your GP (doctor) first, or going to Anglesea Urgent Care.
Non-urgent cases can expect long wait times.
For support and medical advice call
thline 0800 358 5453
NO MOKING
Acute Services Building



sky news .COM.AU

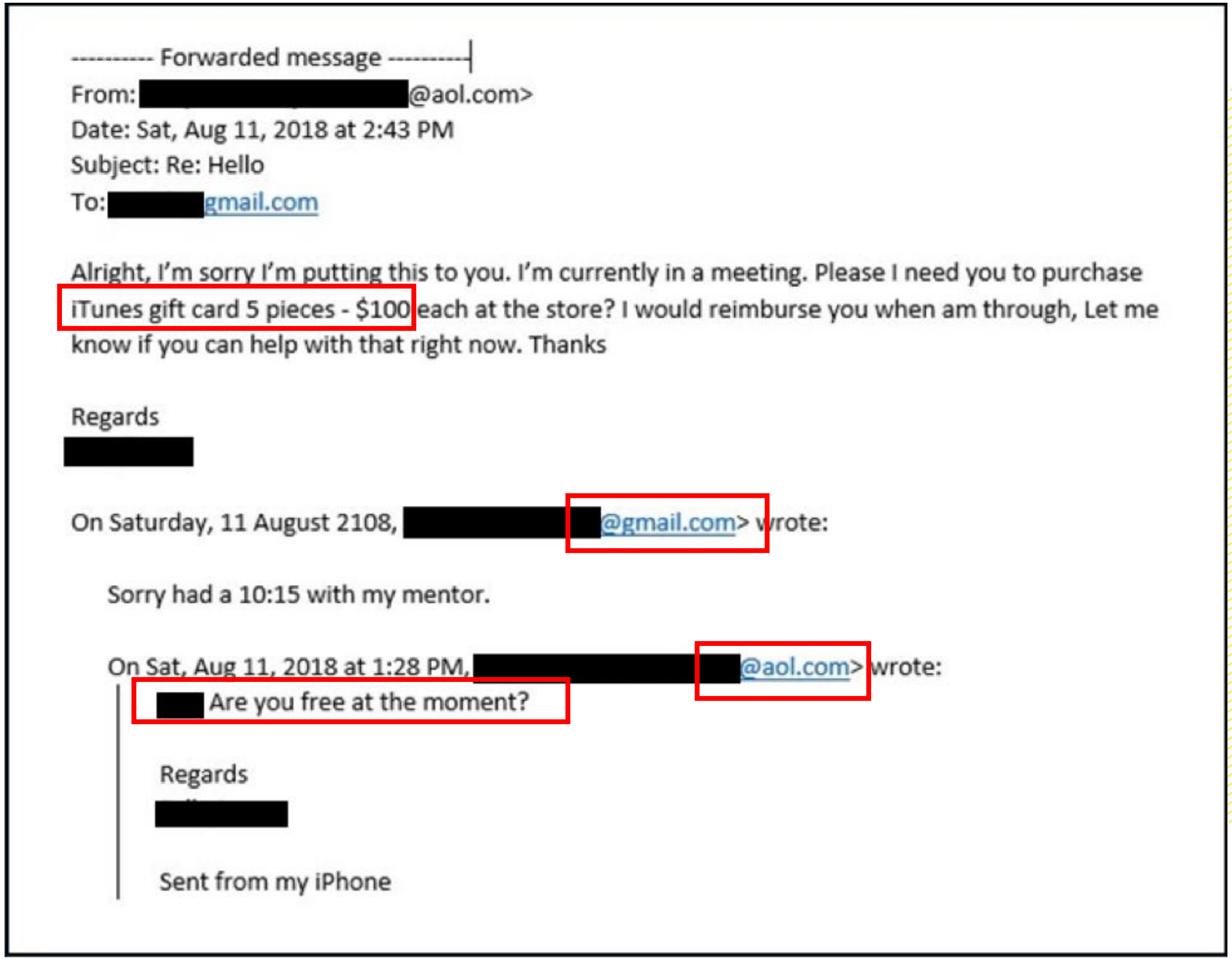
LATITUDE FINANCIAL

The attacker appears to have used the employee login credentials to steal personal information that was held by two other service providers.

STATEMENT TO THE ASX

LATITUDE

BREAKING NEWS 328,000 LATITUDE FINANCIAL CUSTOMERS HACKED



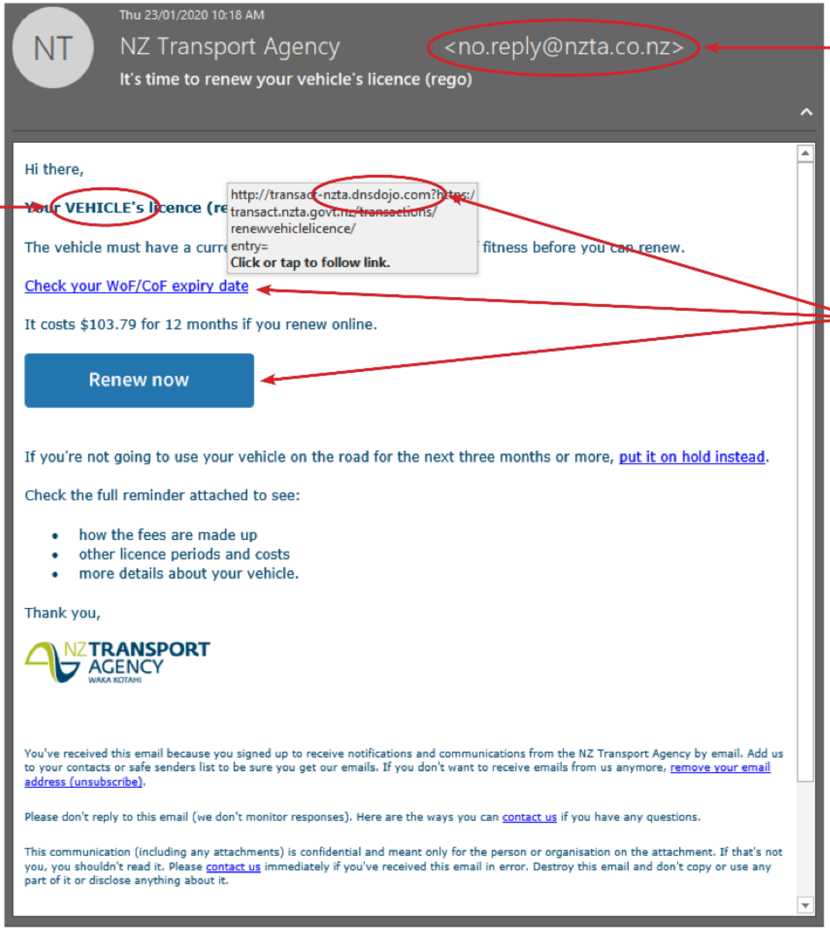
---------- Forwarded message ---------
From: [redacted]@aol.com>
Date: Sat, Aug 11, 2018 at 2:43 PM
Subject: Re: Hello
To: [redacted]gmail.com

Alright, I'm sorry I'm putting this to you. I'm currently in a meeting. Please I need you to purchase iTunes gift card 5 pieces - $100 each at the store? I would reimburse you when am through, Let me know if you can help with that right now. Thanks

Regards
[redacted]

On Saturday, 11 August 2108, [redacted]@gmail.com> wrote:

> Sorry had a 10:15 with my mentor.
>
> On Sat, Aug 11, 2018 at 1:28 PM, [redacted]@aol.com> wrote:
>
> > [redacted] Are you free at the moment?
> >
> > Regards
> > [redacted]
> >
> > Sent from my iPhone



Thu 23/01/2020 10:18 AM

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

http://transact-nzta.dnsdojo.com?https://transact.nzta.govt.nz/transactions/renewvehiclelicence/entry=
Click or tap to follow link.

The vehicle must have a curre … fitness before you can renew.

Check your WoF/CoF expiry date

It costs $103.79 for 12 months if you renew online.

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,

NZ TRANSPORT AGENCY
WAKA KOTAHI

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).

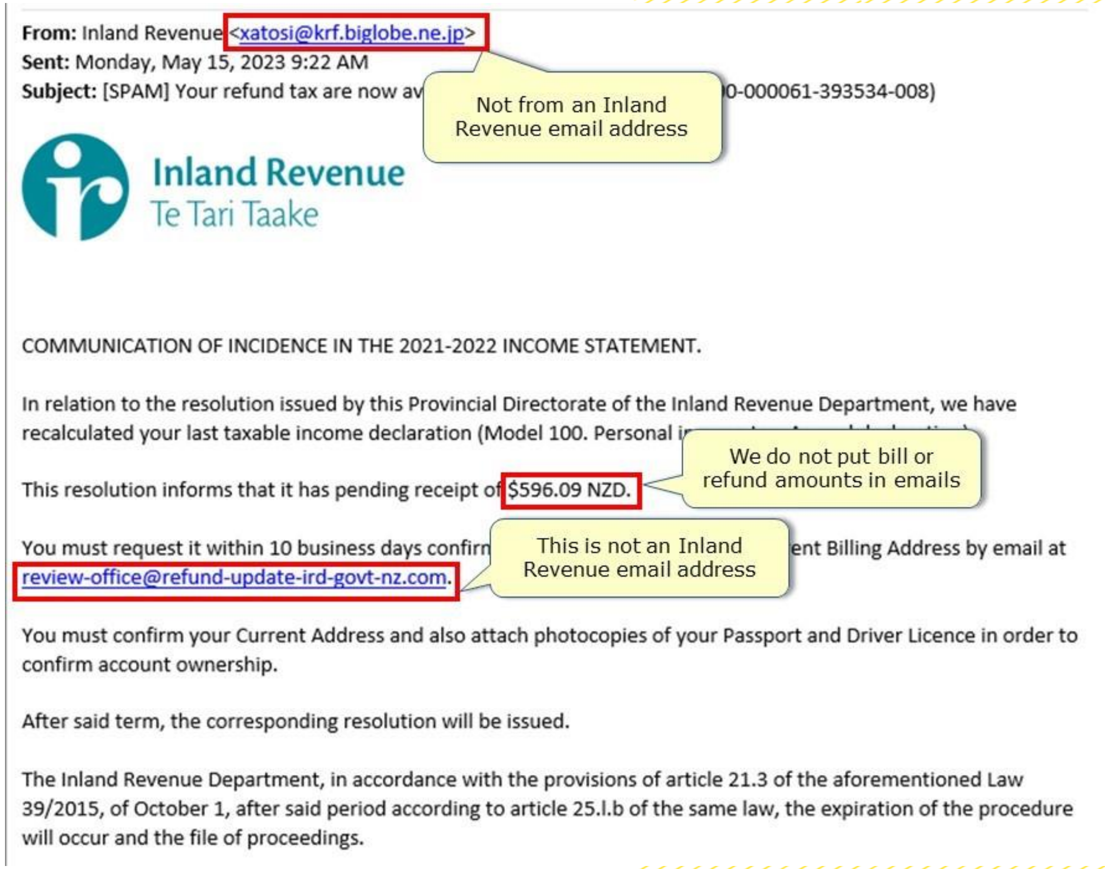
Please don't reply to this email (we don't monitor responses). Here are the ways you can contact us if you have any questions.

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.

Not from
@nzta.govt.nz

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

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



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)

Inland Revenue
Te Tari Taake

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.

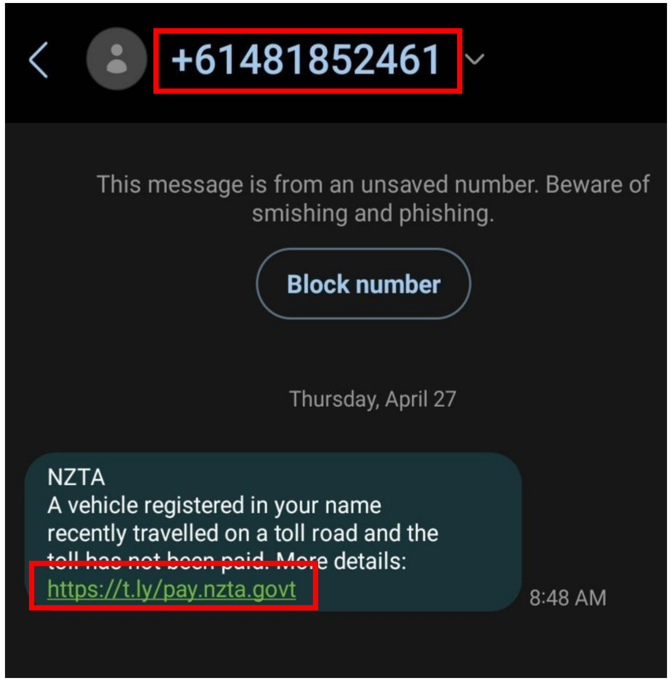
After said term, the corresponding resolution will be issued.

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.l.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



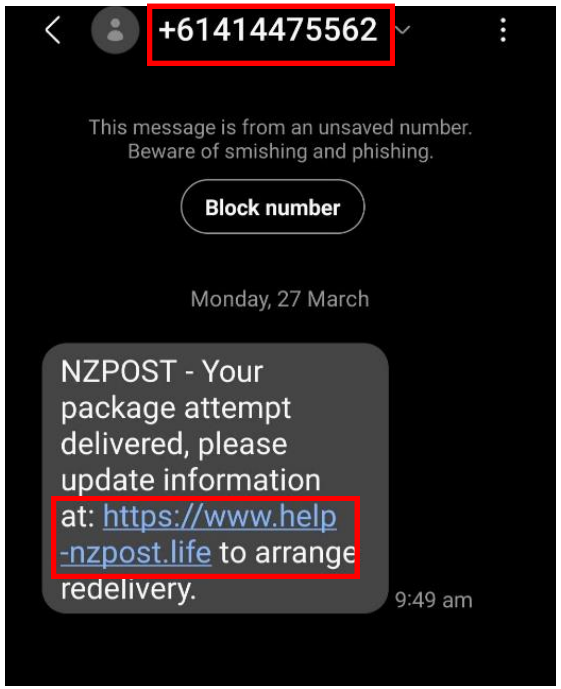
+61481852461

This message is from an unsaved number. Beware of smishing and phishing.

Thursday, April 27

NZTA
A vehicle registered in your name recently travelled on a toll road and the toll has not been paid. More details: https://t.ly/pay.nzta.govt

8:48 AM



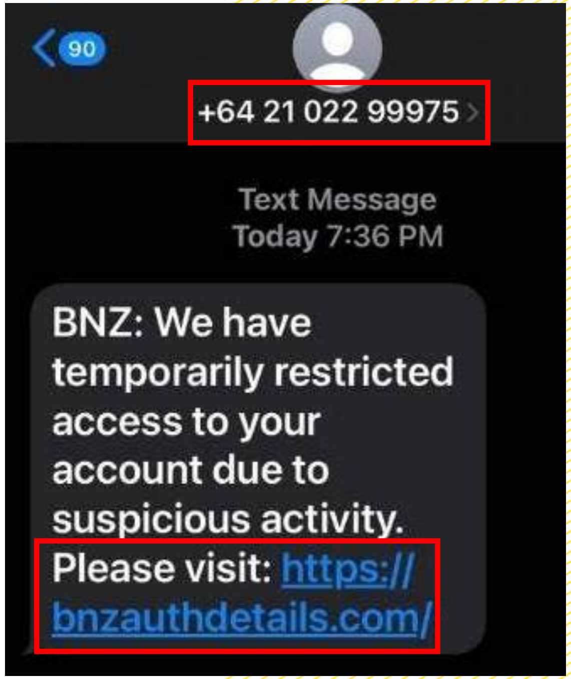
+61414475562

This message is from an unsaved number. Beware of smishing and phishing.

Monday, 27 March

NZPOST - Your package attempt delivered, please update information at: https://www.help-nzpost.life to arrange redelivery.

9:49 am



+64 21 022 99975

Text Message
Today 7:36 PM

BNZ: We have temporarily restricted access to your account due to suspicious activity. Please visit: https://bnzauthdetails.com/

/// Phishing scam prevention

How to spot them

- Check email addresses
- Check phone numbers
- Check URLs of links & websites
- Stop and think if the message:
  - Is out of the blue
  - Doesn't match usual activities
  - Creates a sense of urgency
  - Requests payment or credentials.

How to report them

- Mark as junk or phishing through your email provider.
- Forward text messages to 7726 (Department of Internal Affairs)
- Forward emails to phishpond@ops.cert.govt.nz (CERT NZ)

Scams targeting businesses

/// Social media account takeovers

Malicious actor gains unauthorised access to a social media account with malicious intent.

The accounts are commonly compromised via phishing, and then used to defraud others.

How to prevent account takeovers

- Long, strong unique passwords
- Change passwords periodically
- Enable 2FA
- Being phishing-conscious

Social media account takeovers continued

What to do if your account is compromised

- Report it to the platform and ask others to report the account.
- Inform your customers so they aren’t defrauded.
- If your email account is still secure, use the account recovery process.
- If you are unable to recover the account, create a new account.
- Report the compromise to CERT NZ for personalised incident recovery advice.

/// Invoice scams

Scammers compromise a business' email account and send invoices requesting payment to a new bank account.

or

Scammers send fake invoices requesting payment for goods or services that you didn't ask for or receive.

How to prevent invoice scams

- Keep your business accounts secure.
- Check the email address before paying invoices.
- Double check any new or changed bank account numbers.
- Consider electronic invoicing options.

/// Remote access scams

In a remote access scam, a scammer attempts to persuade you into giving them remote control over your computer.

Once they have access, they can steal information and/or money.

Impersonation tactics

- International software companies
- Telecommunications or tech firms
- Bank fraud teams
- Law enforcement
- Local or overseas regulators.

/// Remote access scams continued

How to prevent them

- Never give remote access to someone unless you've requested it first.
- Never access banking or sensitive information during a remote access session.
- Don't save your passwords in your browser.

How to report them

- Report the phone number to your telecommunications provider.
- Report unauthorised transactions to your bank.
- Report the scam to CERT NZ.

Malware and ransomware

/// Malware

Malware is software specifically designed to disrupt, damage or gain unauthorised access to a computer system.

Once malware is on a device, cyber criminals can steal sensitive information, encrypt data or increase system vulnerabilities.

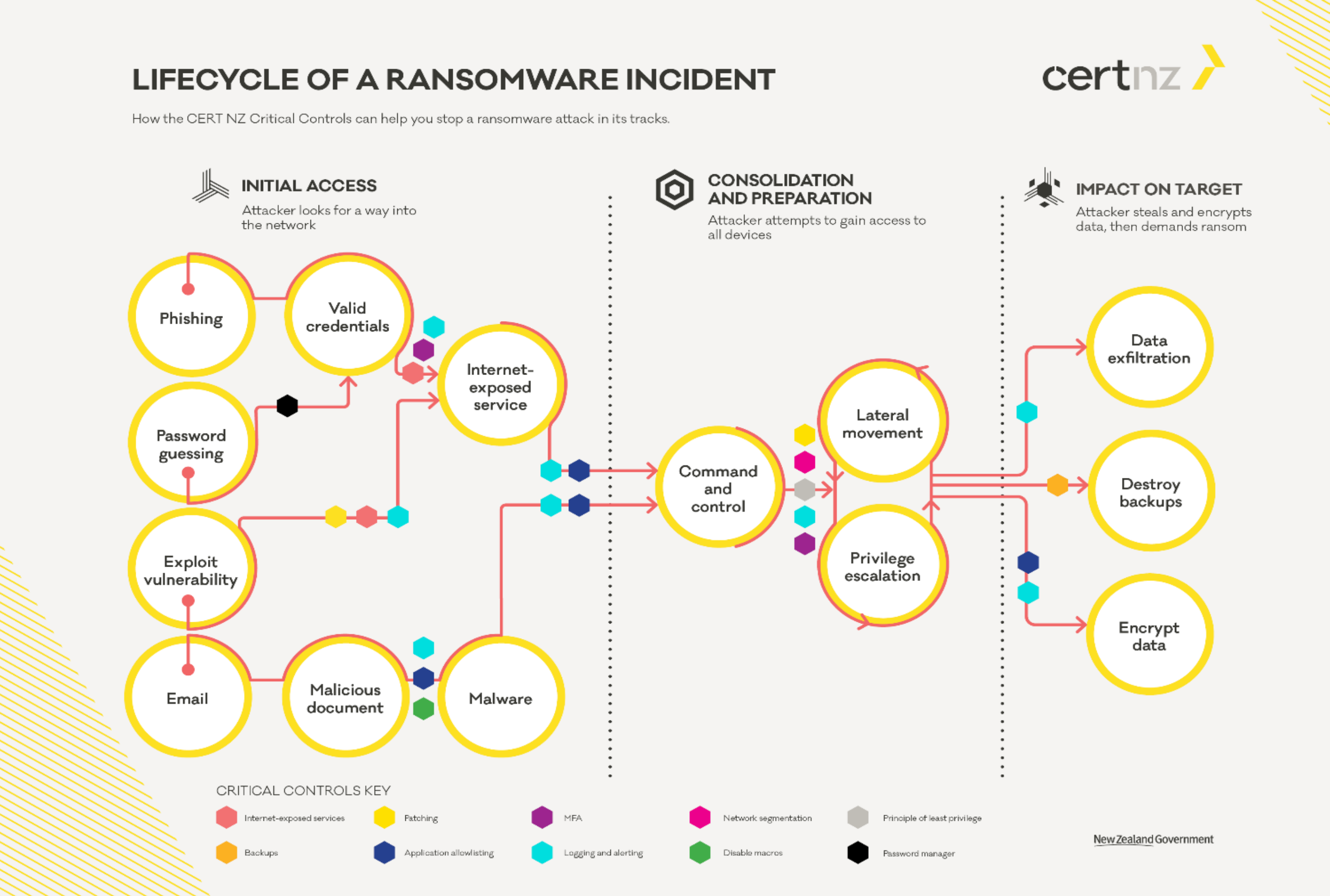
Common types of malware

- Usually attached to files from:
  - Emails
  - Downloads
  - Portable devices (like USBs)
- Different types include:
  - Worms
  - Trojans
  - Spyware and adware

/// Ransomware

Ransomware is a financially-motivated cybercrime. It is a type of malware designed to block access to a computer system until a sum of money is paid.

Ransomware actors are increasingly well-resourced and sophisticated.



LIFECYCLE OF A RANSOMWARE INCIDENT

certnz

How the CERT NZ Critical Controls can help you stop a ransomware attack in its tracks.

INITIAL ACCESS

Attacker looks for a way into the network

Phishing

Valid credentials

Internet-exposed service

Password guessing

Exploit vulnerability

Email

Malicious document

Malware

CONSOLIDATION AND PREPARATION

Attacker attempts to gain access to all devices

Command and control

Lateral movement

Privilege escalation

IMPACT ON TARGET

Attacker steals and encrypts data, then demands ransom

Data exfiltration

Destroy backups

Encrypt data

CRITICAL CONTROLS KEY

Internet-exposed services

Patching

MFA

Network segmentation

Principle of least privilege

Backups

Application allowlisting

Logging and alerting

Disable macros

Password manager

New Zealand Government

Five steps for employees to keep secure

/// Long, strong, unique passwords

- Longest is strongest: use at least 15 characters.
- Use a passphrase that's four or more words.
- Always use unique passwords for critical accounts.
- Avoid common patterns and personal information.
- Check if your password has been compromised at haveibeenpwned.com.

/// Turn on two-factor authentication (2FA)

- 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 login details and can let you know your account details have been compromised.
- Read 2FA codes carefully and only enter them if the message description matches the action you are taking.

/// Update devices and apps

- Updating devices improves performance and fixes weakness that could let attackers in.
- The easiest way to do this is by going to settings and turning on automatic updates.

/// Protect your privacy online

- Be mindful about what you do online – your digital imprint is highly valuable.
- Check your privacy settings on social media.
- Use 'private' or 'friends only' to control who sees your information.
- Check websites are private before submitting personal information.

/// Think before you click

- Be wary of opening links and attachments.
- If you think the message is legitimate, check with the organisation or person.
- If it sounds too good to be true, it probably is.

Securing your business from cyber threats

/// Knowing and responding to cyber risks

Building cyber security awareness

- 82% of cyber breaches involve a human element.
- People can be the strongest cyber defence.
- Invest in awareness and training.

Creating an incident response plan

- Have a written plan which is accessible, and staff are familiar with.
- Understand your risks.
- Identify and report incidents.
- Determine incident sale and response.

Elevate your cyber security posture

Top 11 cyber security tips

- Install software updates
- Implement 2FA
- Back up data
- Set up logs
- Create an incident response plans
- Change default passwords
- Choose the right cloud services
- Only collect the data you need
- Secure your devices
- Secure your network
- Check financial details manually.

CERT NZ's Critical Controls

- Patch your software and systems
- Implement MFA and verification
- Provide and use a password manager
- Configure logging and alerting
- Security awareness building
- Asset lifestyle management
- Implement and test back ups
- Implement network segmentation
- Implement application control
- Enforce the principle of least privilege.

A NEW CYBER SMART WEEK

30 October – 5 November 2023

Cyber attacks have been growing in prevalence and sophistication,
and the need for strong cyber security practices has never been more important.

Unfortunately, many people aren’t well equipped to face these growing threats.

We want to use Cyber Smart Week 2023 to change that…

/// Cyber security is on the radar

80%

of New Zealand individuals and SMEs both saying they regularly hear about them

98%

of New Zealand can name at least one cyber threat

60%

of people are concerned about the safely of their personal information online

/// But, it's not a priority

17%

of people have adopted a new cyber safe behaviour in the past six months

79%

Of individuals and 59% of SMEs have not reported a cyber incident in the past because they didn't think it was worth it

58%

say they don't know how to do it or it's too complicated

57%

say they keep forgetting to

48%

say they don't want to, or can't be bothered

Cyber Smart Week 2023

30 October to 5 November

own
your
online

certnz

Cyber Smart Week 2023

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.

Theme: Exposed

Objective: Raising the importance of cyber security by showing New Zealanders what's at stake when we don't get cyber security right.

Featuring ten New Zealanders who have been targeted by attackers going about their online lives.

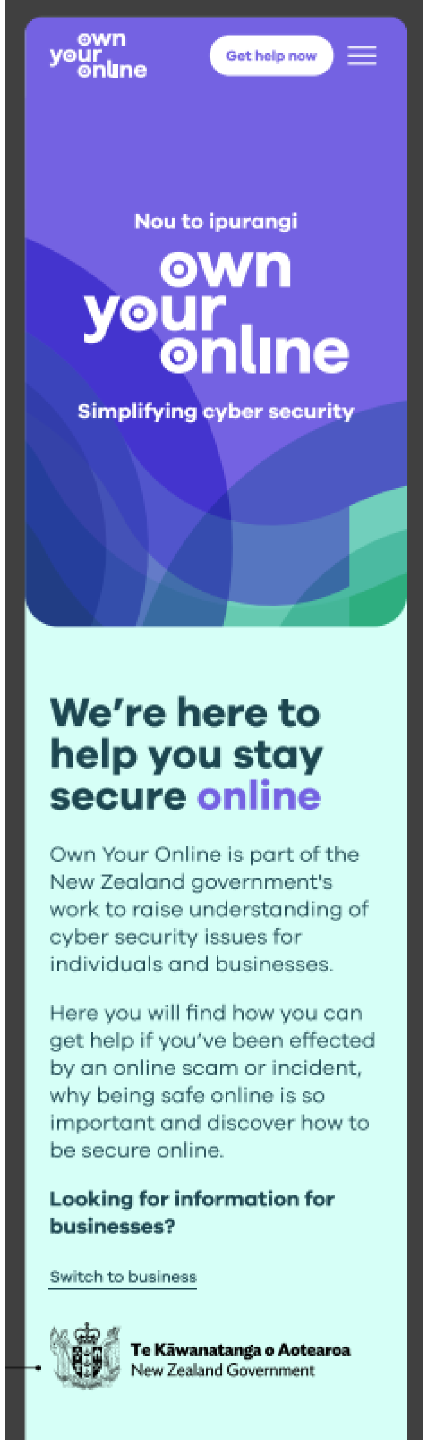
certnz

Don't expose your life online. Own it.
Learn how to protect yourself online.
ownyouronline.govt.nz
certnz
own your online
cyber smart week

CERT NZ activity

- Free Auckland exhibition
  - Tuesday Club, 42 Airedale Street, Auckland CBD: 31 October–2 November
- ownyouronline.govt.nz/exposed
- Outdoor billboards
- Social advertising
- Online advertising
- Webinars

own
your
online



Nou to ipurangi

own your online

Simplifying cyber security

We’re here to help you stay secure online

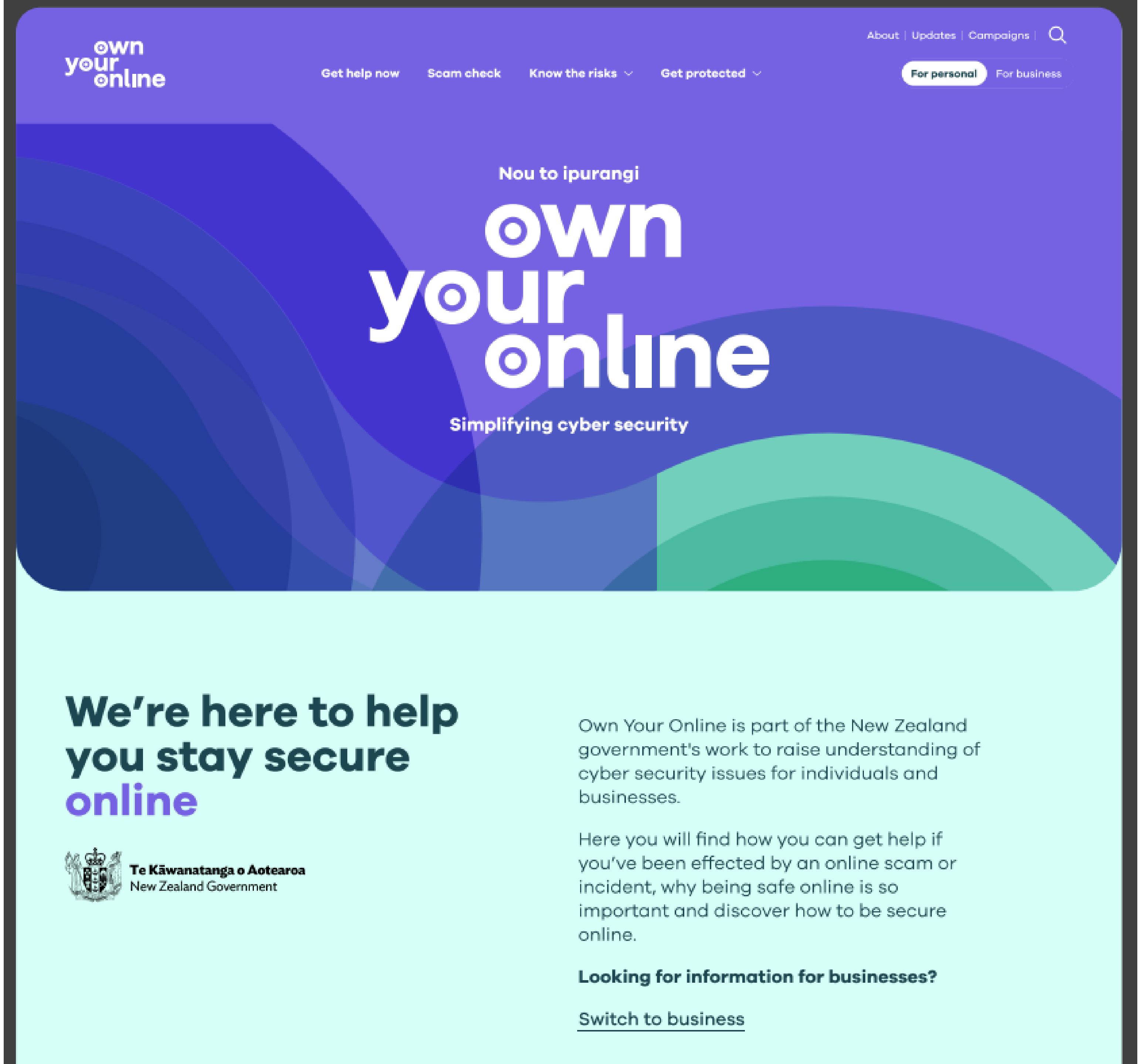
Own Your Online is part of the New Zealand government's work to raise understanding of cyber security issues for individuals and businesses.

Here you will find how you can get help if you’ve been effected by an online scam or incident, why being safe online is so important and discover how to be secure online.

Looking for information for businesses?

Switch to business

Te Kāwanatanga o Aotearoa
New Zealand Government



Nou to ipurangi

own your online

Simplifying cyber security

We’re here to help you stay secure online

Te Kāwanatanga o Aotearoa
New Zealand Government

Own Your Online is part of the New Zealand government's work to raise understanding of cyber security issues for individuals and businesses.

Here you will find how you can get help if you’ve been effected by an online scam or incident, why being safe online is so important and discover how to be secure online.

Looking for information for businesses?

Switch to business

certnz

Any questions?

Contact

Erica Boscato

☎ 0800 CERT NZ

✉ Erica.boscato@cert.govt.nz

🌐 www.cert.govt.nz

@CERTNZ