

February 2024

Own Your Online

Staying Safe Online for Seniors

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 people (and businesses) affected by cyber incidents.
- Advice and campaigns highlighting online threats and how to deal with them.
- Regular stats about cyber security, which help us see the threats coming up.

Today's agenda

We're going to cover off:

- Common misconceptions
- Different types of threats and scams
- Simple steps to keep secure
- Own Your Online

Common misconceptions



Are you targeted more?

No.

Are you more susceptible?

No.



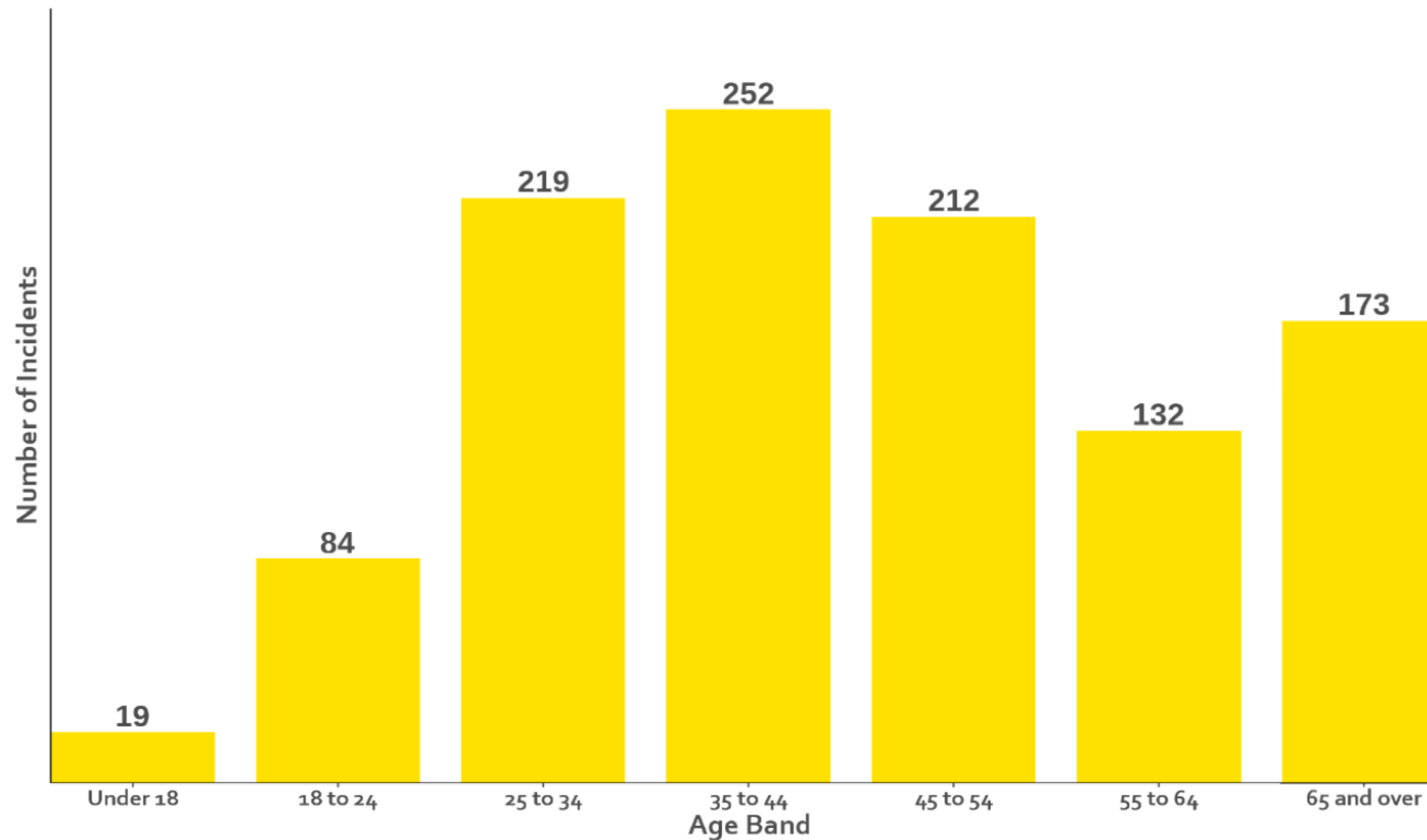
Should you feel embarrassed?

No.


REPORTING BY AGE

Of the 2,136 incidents responded to by CERT NZ during Q3, 41% provided their date of birth. These numbers now include incidents where there was no money loss.

Figure 13: Incidents affecting individuals – breakdown by age



Statistics from quarter three of 2023 (July to September)



Common threats and scams

'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)

Not from an Inland Revenue email address



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.

We do not put bill or refund amounts in emails

You must request it within 10 business days confirm

This is not an Inland Revenue email address

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.

Thu 23/01/2020 10:18 AM

NT NZ Transport Agency
It's time to renew your vehicle's licence (rego)

<no.reply@nzta.co.nz>

Not from @nzta.govt.nz

Hi there,

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

Your **VEHICLE's** licence (re

<http://transact-nzta.dnsdojo.com?https://transact.nzta.govt.nz/transactions/renewvehiclelicence/>

Click or tap to follow link.

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 \(unsubscribe\)](#).

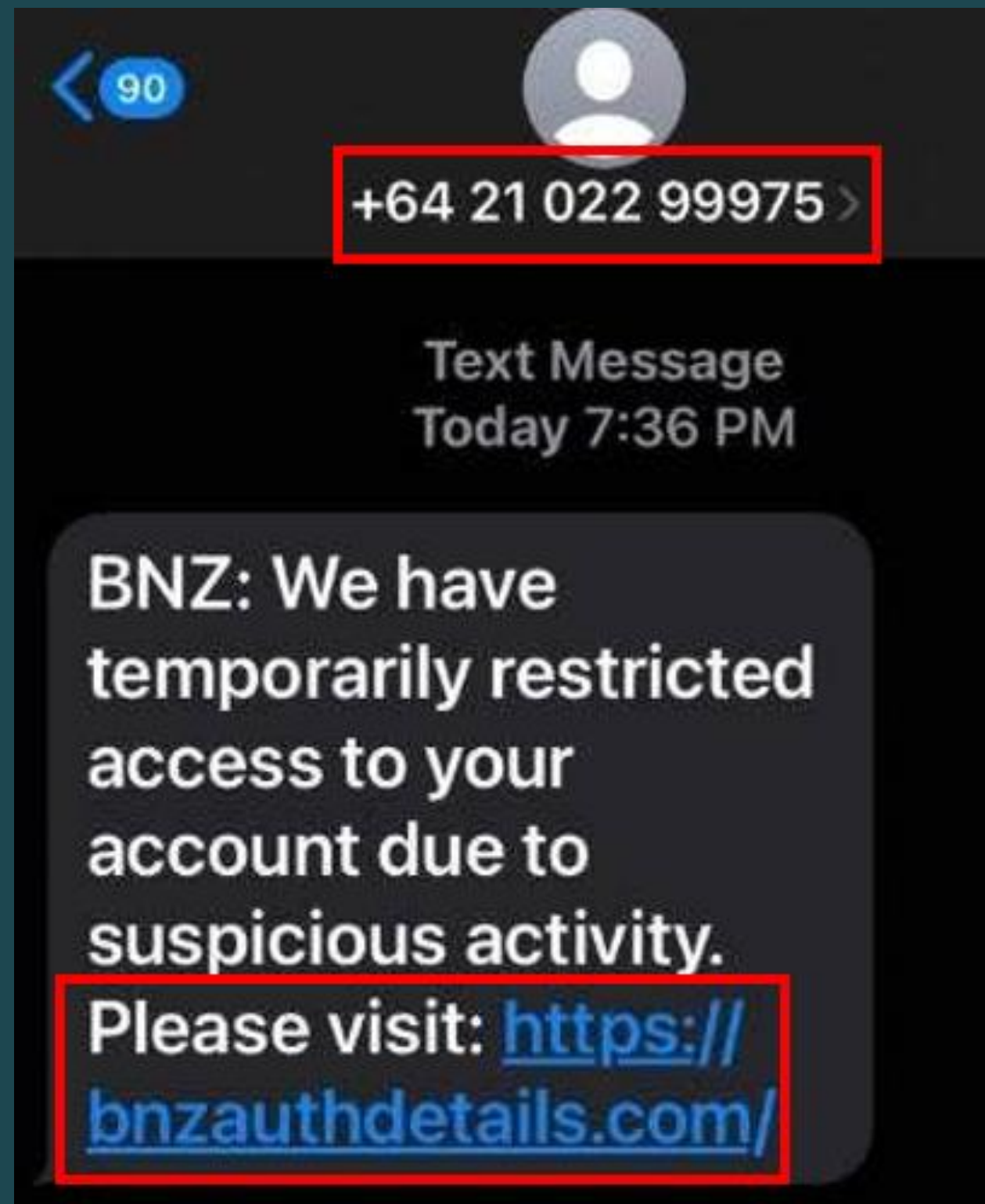
Please don't reply to this email (we don't monitor responses). Here are the ways you can [contact us](#) if you have any questions.

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.

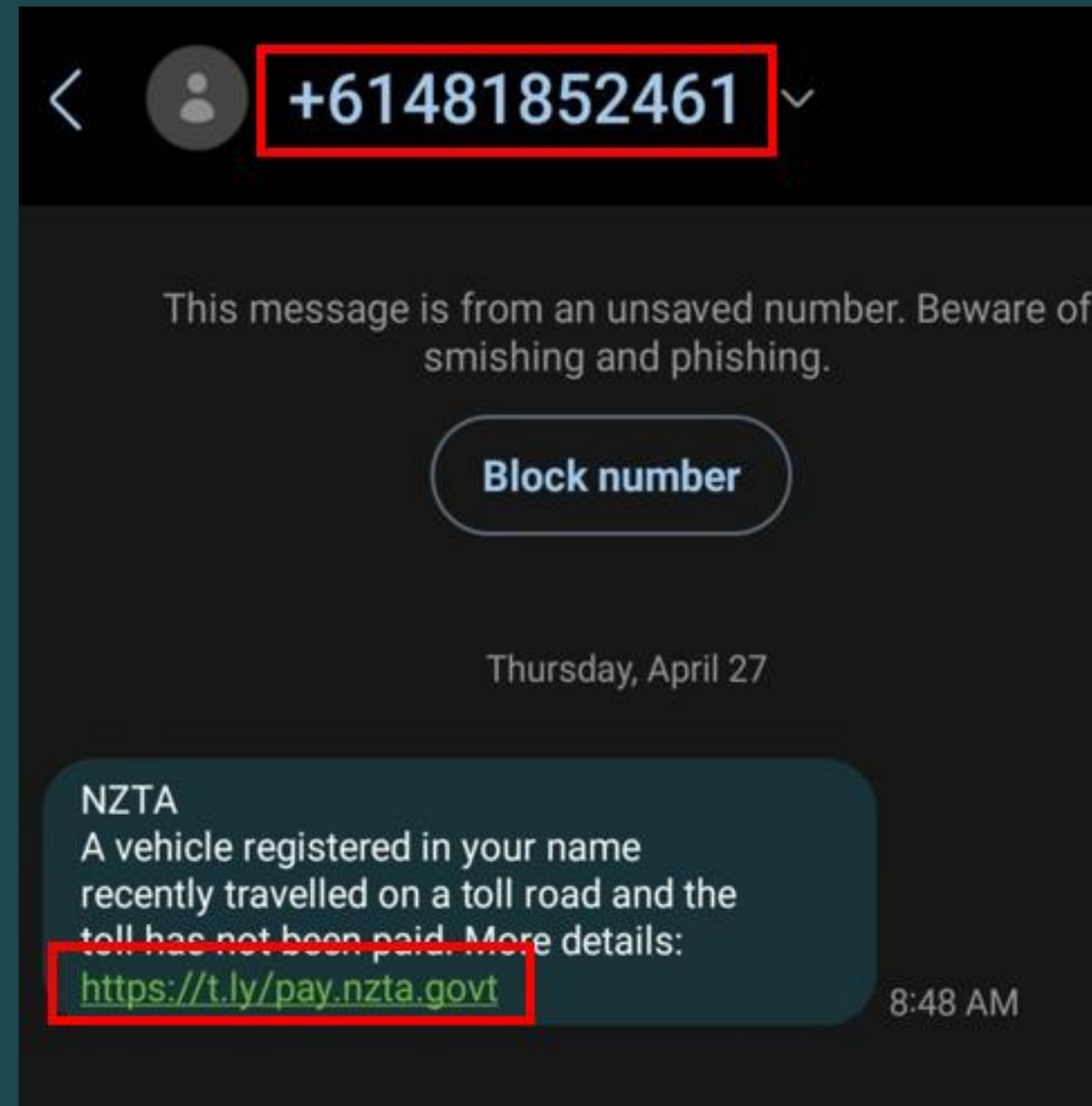
Hovering over links show you they don't go to nzta.govt.nz

Phishing text messages

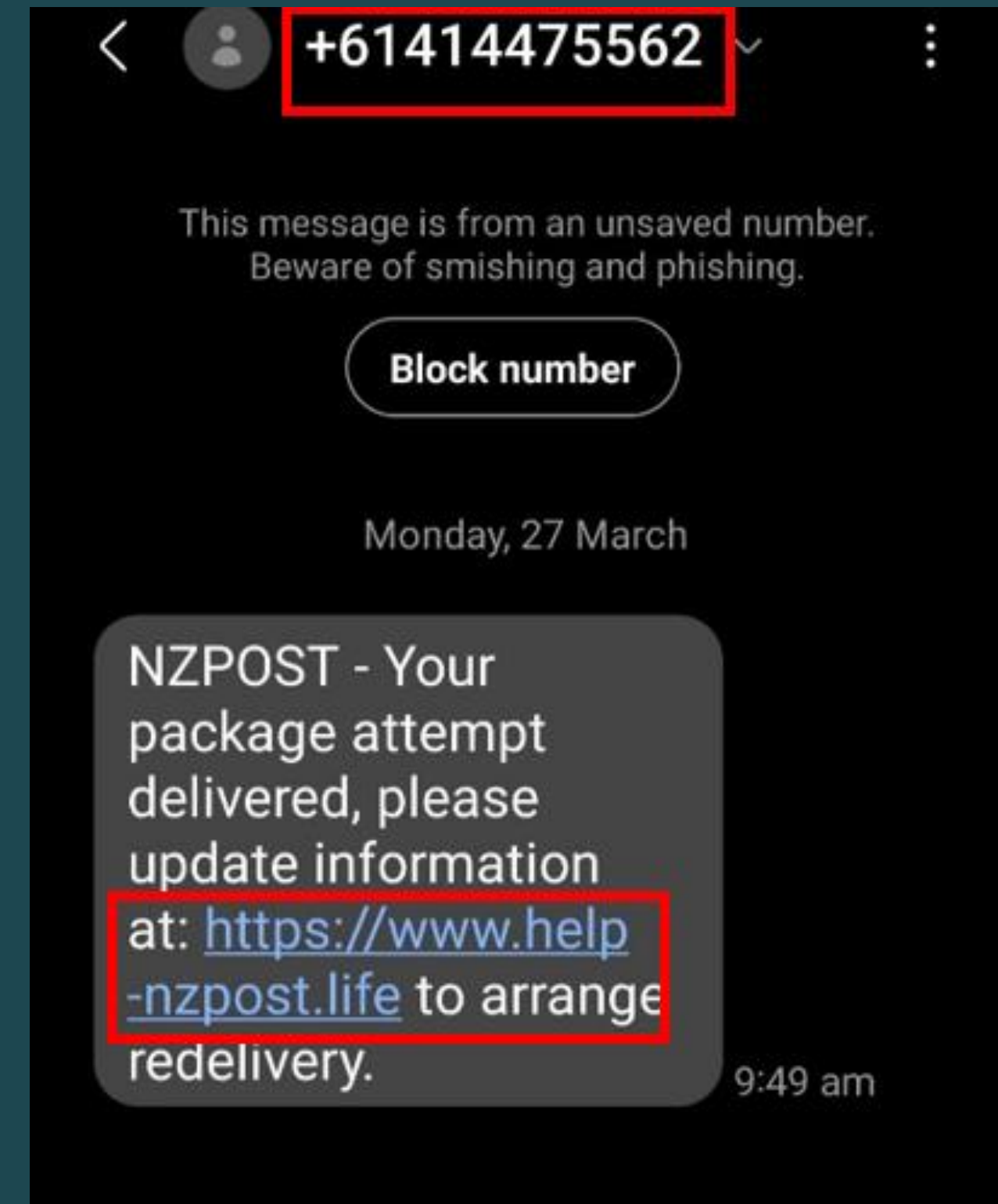
What to look for



- 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



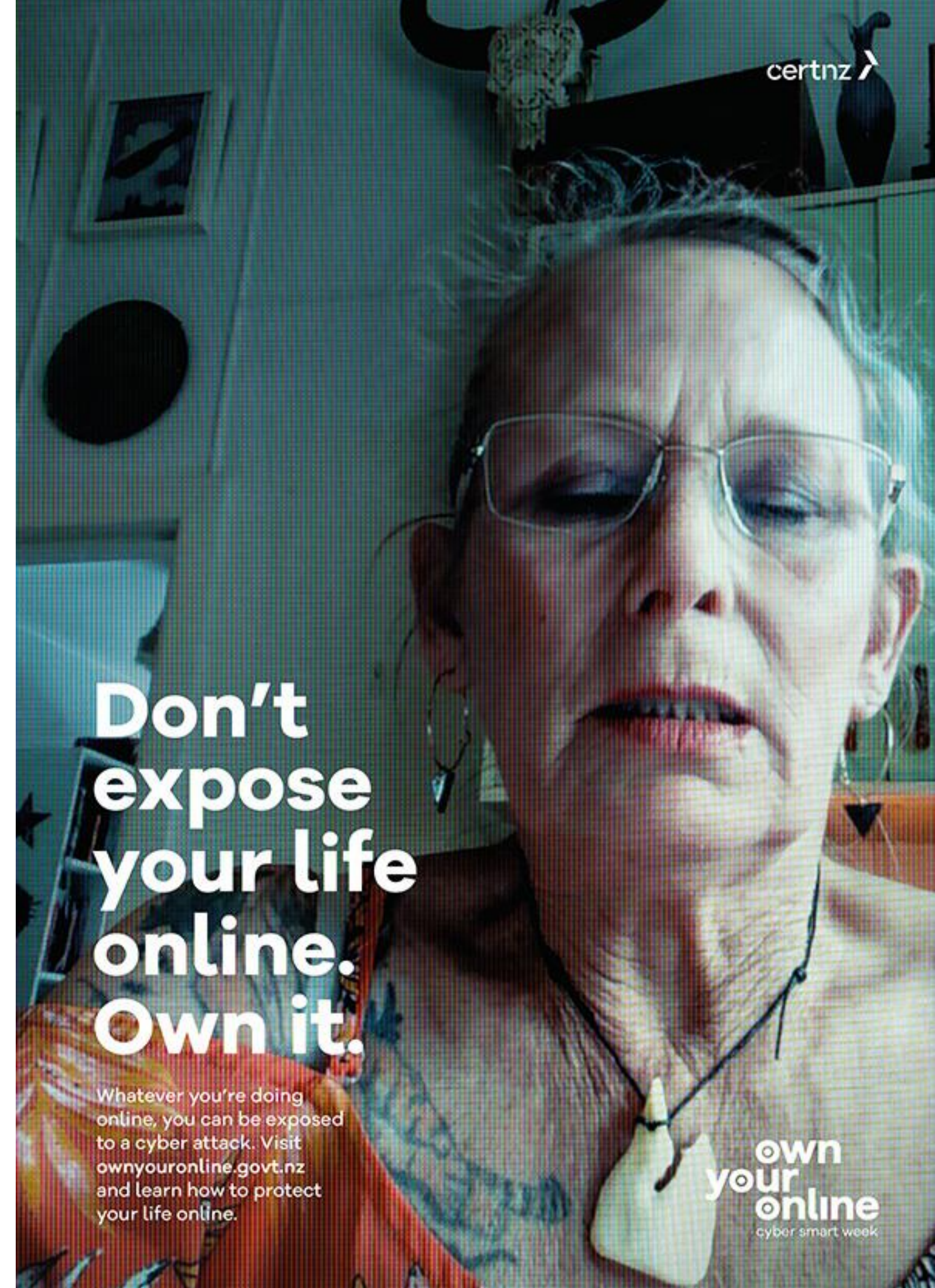
- Sent from a phone number not a four-digit 'short code'
- Phone number uses Australian area code (+61)
- Not a real NZ Post website

Remote access scams

In a remote access scam, a scammer persuades you to give them access to your computer or mobile device.

Once they have access, they can steal your personal information or money.

own
your
online



**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.

own
your
online
cyber smart week

Remote access scams

Red flags for remote access scams:

- Cold calls from someone claiming to be a technical expert.
- Claims there is an issue with your internet or bank account.
- Request to download software to your phone or computer.
- Requests to log into your online banking account or other financial platforms.

Key takeaway:

If a cold call, claims there is a technical issue with your computer or account, and asks you to download software, it is most likely a scam

Romance scams

Romance scams are where social engineering techniques are used to create emotional relationships to steal money or services.

Thea was involved in an online romance scam. She doesn't want you to be.

Visit ownyouronline.govt.nz and learn how to protect your life online.

Romance scams

Red flags for romance scams

- You've met someone online and they are based overseas.
- They make excuses for not meeting up, doing video calls or returning to New Zealand.
- They use intimate language very quickly to build the relationship and trust.
- They experience a personal or business emergency, and then they request money or a loan.

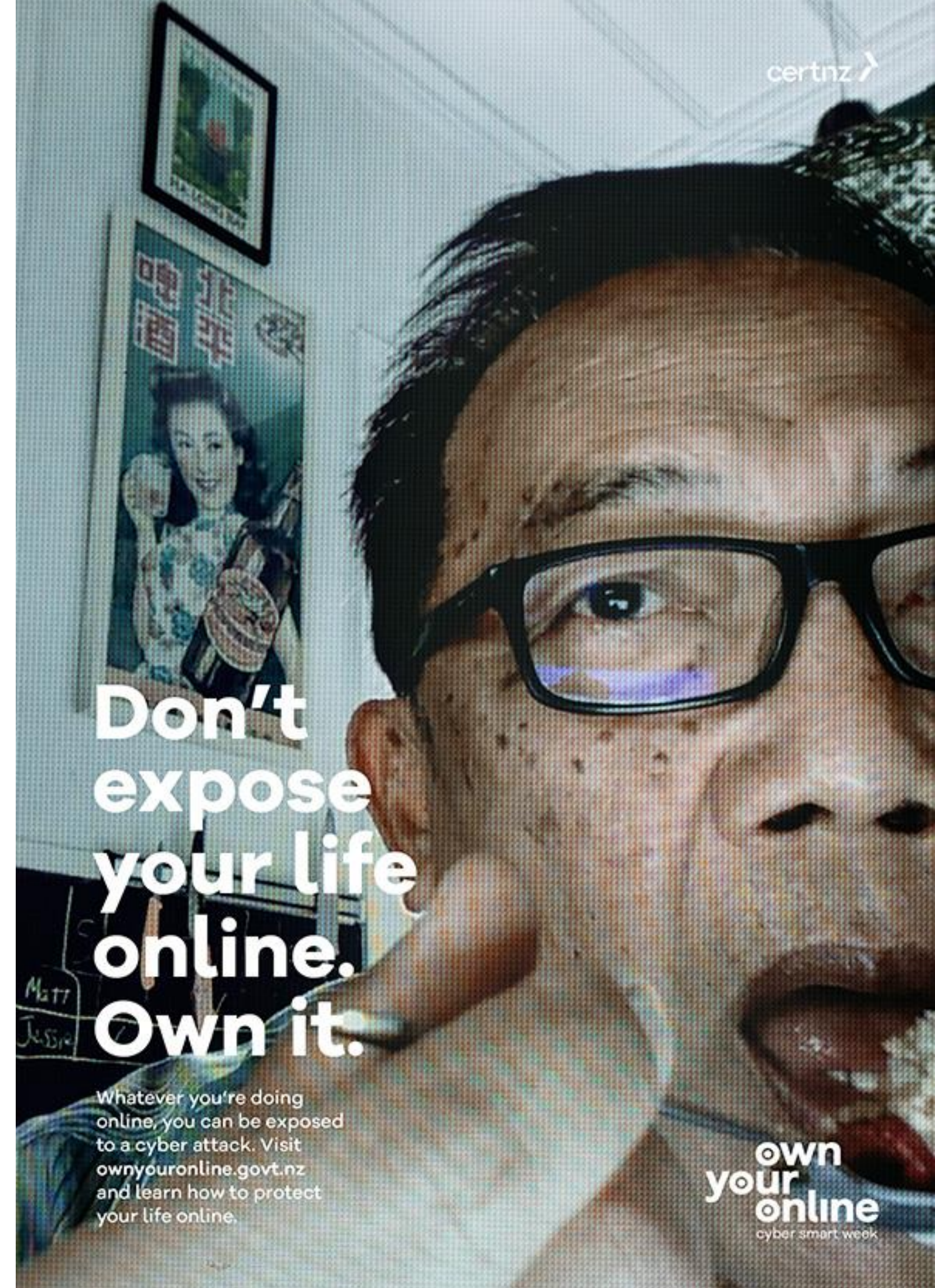
Key takeaway

If an online relationship moves quickly and results in requests for money or financial aid, it is most likely a scam.

Investment scams

Investment scams are where scammers convince you to transfer money to a non-existent investment.

own
your
online



certnz

**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.

own
your
online
cyber smart week

Investment scams

Red flags for investment include:

- The investment company approached you out of the blue.
- There is time pressure or a sense of urgency, for example the offer will expire soon.
- The offer is too good to be true: they are offering high returns with low risk.
- The investment company or their advisor is based outside New Zealand.

Key takeaway

If a company approaches you out of the blue with financial advice or guidance. Legitimate New Zealand financial companies are bit allowed to do that. Check if the company is registered on the Financial Service Providers Register.

<https://fsp-register.companiesoffice.govt.nz/>

Main things to be wary of.

- Any unsolicited contact – email, social media messages, phone calls or text messages.
- Messages that creates a strong sense of urgency

Main takeaways:

- Stop for a moment and think before doing anything.
- This can happen to anyone; it is not your fault.
- Know where to report and where to get help.
- Don't let embarrassment stop you from reporting it.



Simple steps to stay secure

Passwords

Use long, strong, unique passwords

- Longest is strongest: use at least 15 characters.
- Do not use the same password for your important accounts.
- Use a passphrase by joining four or more random words together and adding numbers of symbols as needed.
- Avoid common patterns and personal information.
- Check if your password or email account has been compromised at www.haveibeenpwned.com



Two-factor authentication

An extra layer of protection

- Two-factor authentication (2FA) is a unique code sent to your phone or taken from an app that only you have access to.
- 2FA is an incredibly powerful tool that 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 use them if the message description matches the action you are taking.
- Do not share them with anyone.



Updates

Turn on auto-updates on apps and devices

- Updating devices – phones and computers – 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.



Privacy

Protect your privacy online

- Be mindful about what you do and share online.
- Check your privacy settings on social media and consider using the 'private', 'friends only' or 'lock' functions to control who sees your information.
- Check websites are secure before submitting personal information.



Stop and think

Think before you click

- Be wary of opening links and attachments, especially from people you don't know.
- If you have any doubt, check with the person or organisation by using their official number.
- If it sounds too good to be true, it probably is.





Know where to report

Responding to online scams

Reporting scams helps keep others 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.

Official bank details

ANZ

0800 269 296

<https://www.anz.co.nz/banking-with-anz/banking-safely/reporting-fraud/report-scam-fraud/>

ASB

0800 272 372

<https://www.asb.co.nz/banking-with-asb/online-security/security-help-me.html>

BNZ

0800 735 901

<https://www.bnz.co.nz/about-us/online-security/recognising-scams#report-scams>

Kiwibank

0800 113 355

<https://www.kiwibank.co.nz/contact-us/security/types-of-scams/phishing/>

Westpac

0800 937 8722

<https://www.westpac.co.nz/personal/ways-to-bank/safety-and-security/report-a-scam-or-phishing-email/>

Learn more

Ask your local Age Concern what programmes they have or know of in your area, www.ageconcern.org.nz or freephone 0800 65 2 105.

Each Age Concern run programmes to suit their communities – e.g. one on one sessions, eight-week modules, in partnership with banks etc.

Thanks for your time

Sam Leggett & Hadyn Green

0800 CERT NZ

info@cert.govt.nz

www.cert.govt.nz

www.ownyouronline.govt.nz