GET SET UP FOR SAFETY

Spot a scam

A scam is a made-up story to trick people out of money or steal their information. Learn how to check for red flags.

SPONSORED BY

CHORUS | netsafe

Scams are on the rise and they're getting harder to spot. Improve your scam-spotting skills with Netsafe's advice.

Topics

CHORUS | netsafe

Worried you're being scammed?

- Surprised by this message or that there's a problem?
- Rushed to make a decision, or to move to a different online space?
- Are you being asked to share passwords or personal information?
- Are you being asked to pay online for something you're not sure about?

Check for red flags and take action with SCAMS:

S C A M S

Surprise Control Access Money Stop...

Surprised at the message?
Controlling behaviour?
Access requested?
Money requested?

If yes to any of the above, then:

Stop communicating and seek support.

Contact Netsafe: 0508 638 723 or netsafe.org.nz

CHORUS | netsafe

01

Surprise

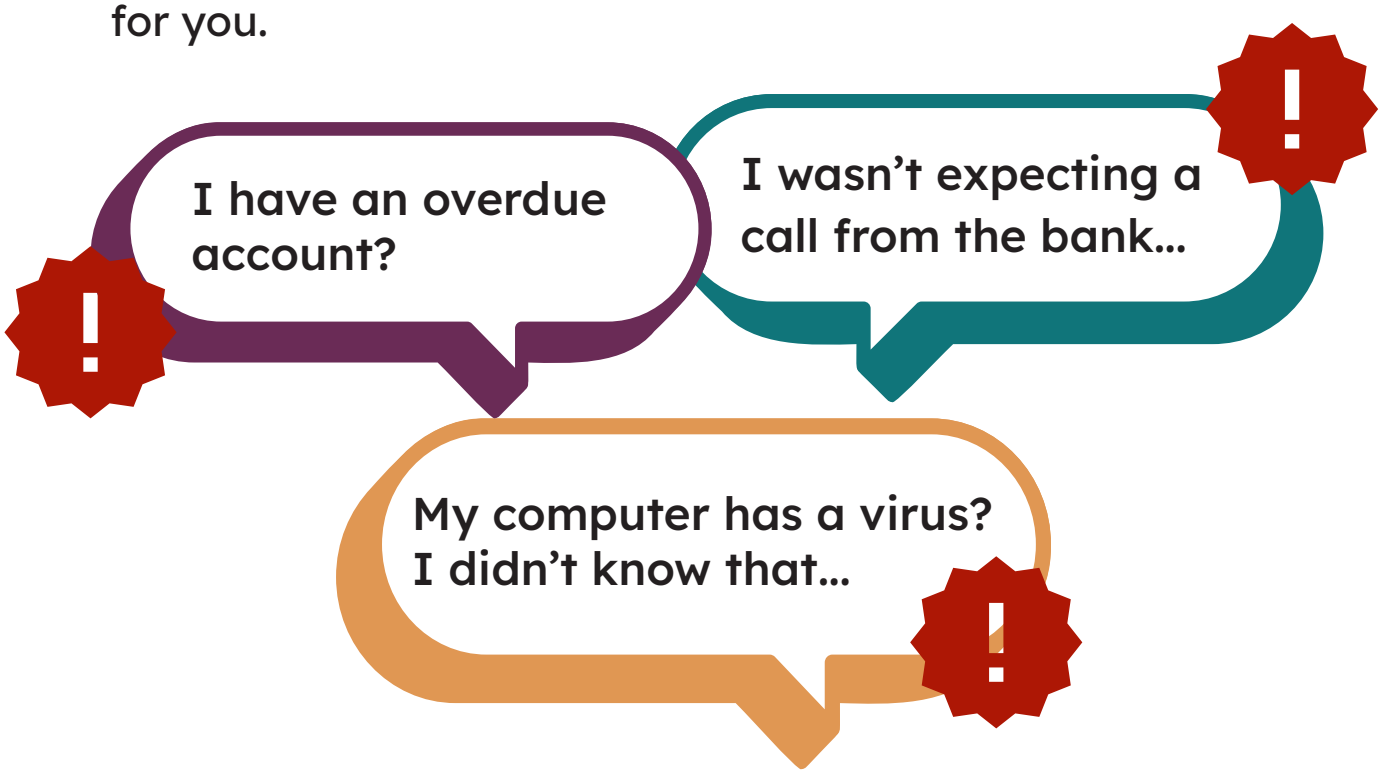
Surprised by a message or that there's a problem?

Unexpected contact

- This can be from someone you know, or someone who says they're from an official organisation like an embassy, your bank or internet provider.

Unexpected problem

- Often someone may say they can fix this surprise problem for you.



CHORUS | netsafe

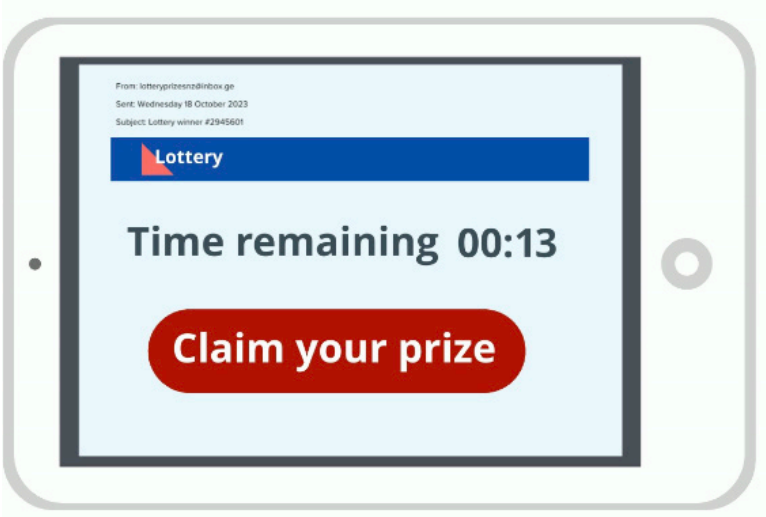
02

Control

Being rushed to make a quick decision, or to move to a different online space?

Being rushed could look like:

- Act now or miss out on something good e.g. prize, bargain.
- Act now or you'll be penalised e.g. fine, account suspension.



Moving to a different online space could look like:

- An online friend is leaving the platform where you met and they ask to keep in touch by a different form of communication like email or using a different social media app.
- An online marketplace seller offers you a discount if you pay direct rather than through the official site payment system.

CHORUS | netsafe

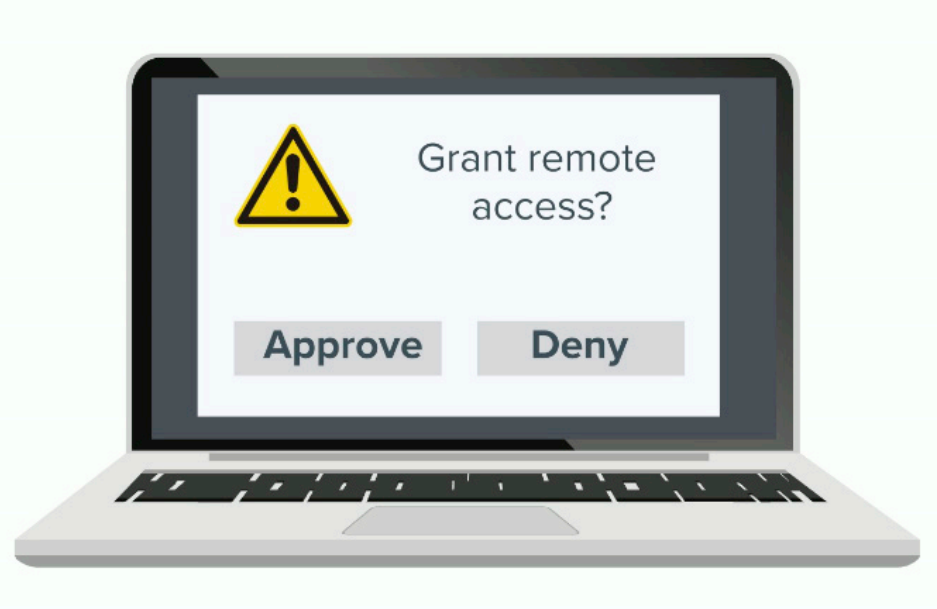
03

Access

Are you being asked to share passwords or personal information?

This could look like:

- Verify your account by clicking here/logging in.
- Prove who you are to correct an account error.
- We can fix a problem if you give us remote access.
- The web address (URL) doesn't look quite right
  i.e. Trademe.eu or www.Amazonn.com.



CHORUS | netsafe

04

Money

Are you being asked to pay online for something you're not sure about?

This could look like:

- Pay a 'processing fee' to get a prize.
- Send gift cards, bitcoins, or pre-loaded debit cards to help your online friend solve a personal problem.
- Enter your credit card details into an unsecured payment system i.e. no 'https' and the website address doesn't match what you're expecting.

CHORUS | netsafe

05

Stop and seek support

- Surprised by this message or that there's a problem?
- Rushed to make a quick decision, or to move to a different online space?
- Are you being asked to share passwords or personal information?
- Are you being asked to pay online for something you're not sure about?

If yes to any of the above:

Stop communicating:

- For a scam to work, the scammer will need you to do something – click a link, give them information, access or money.
- Don't communicate with them again – if they've called you, hang up the phone.
- Don't click links in any messages.
- Don't pay them any money.

Seek support:

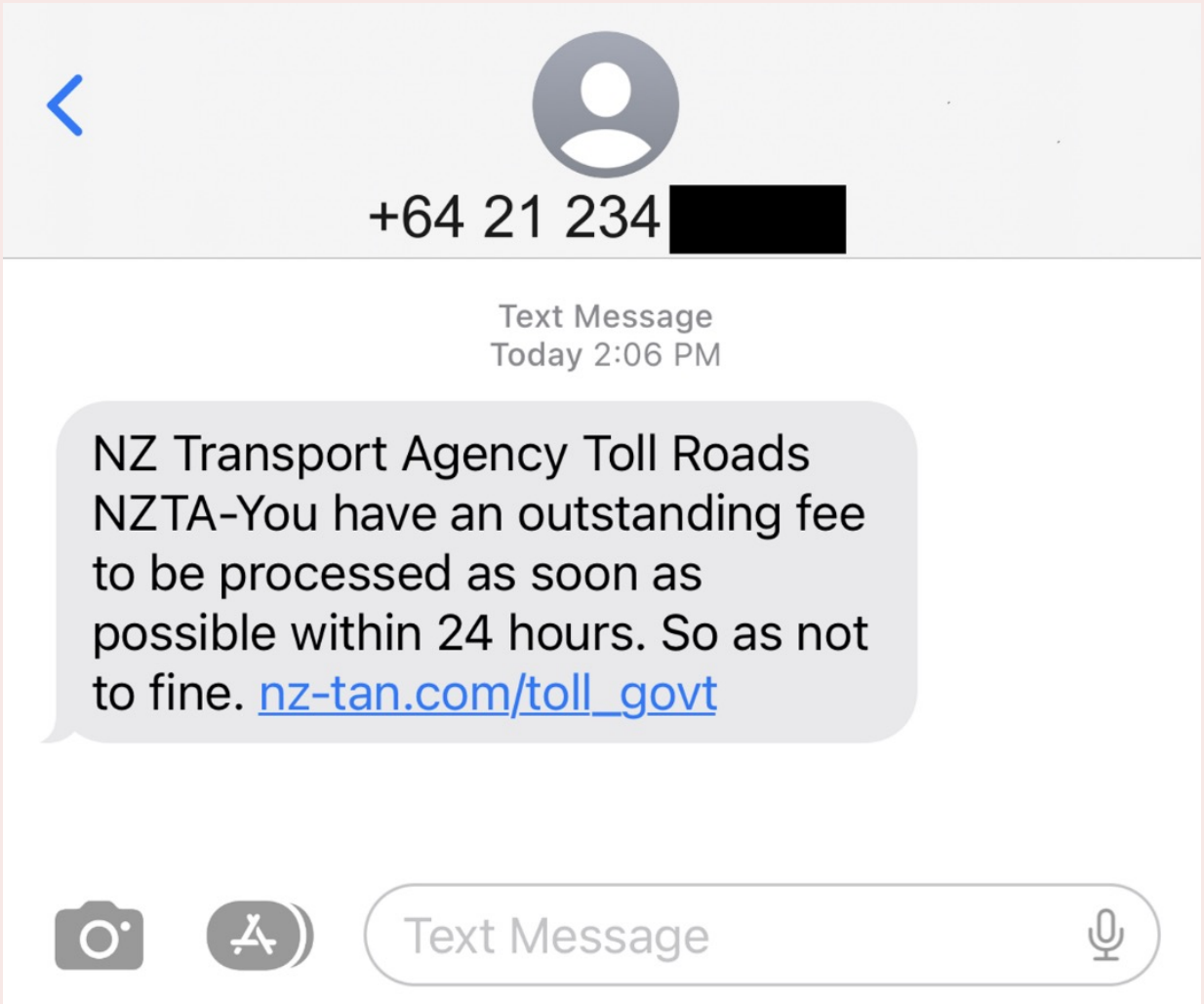
- If you've already paid any money, contact your bank immediately.
- Contact Netsafe for advice about next steps.
- Reach out to your friends/whānau for support.

06

Practice using SCAMS

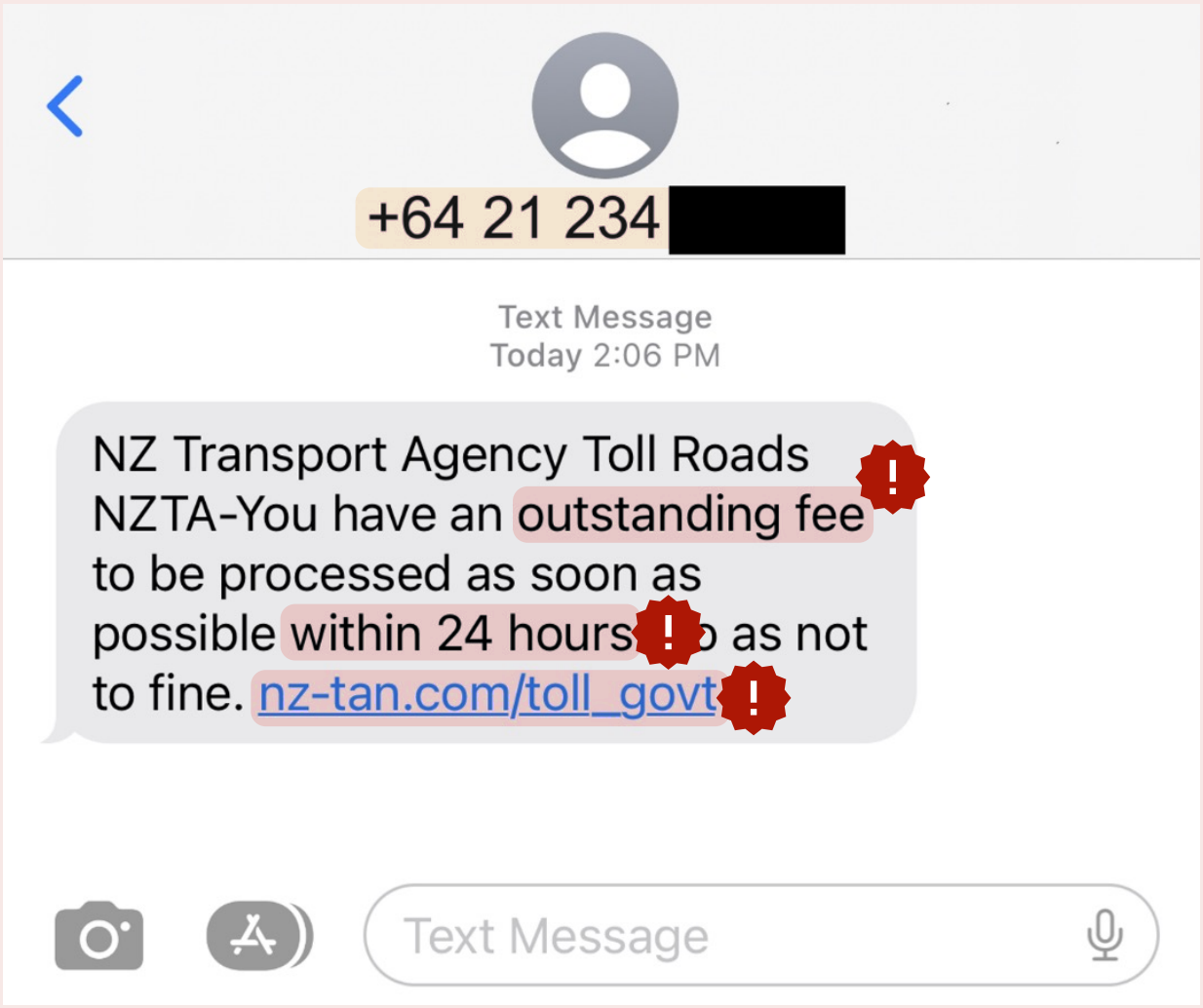
Look at the examples of common scams below and see if you can spot all the signs of a scam.

EXAMPLE 1:



CHORUS | netsafe

The message fails three red flags: Surprise, Control, and Money. If you had clicked on this link and paid money, you'd need to contact your bank immediately, reach out to whānau for support, and contact Netsafe for next steps.



CHORUS | netsafe

EXAMPLE 1 ANSWERS continued

Surprise – an outstanding fee is usually a surprise.

Control – You're being rushed to pay within a time limit. The link is for a new online space – one that doesn't match the service it claims to have come from.

Access – In this case, the potential scam is targeting money rather than personal information.

Money – you're being asked to pay money through an unsecured website. There's no 'https' in the address and URL is not the official NZTA web address.

For bonus points, there are extra scam signs to spot:

- The message is from a personal or an international phone number. A message from a government agency won't show like this.
- It has spelling and grammar errors. This is often a sign of a scam, although AI tools have made it easier for scammers to get it right.

EXAMPLE 2

From: donotreply_inlandrevenue@inbox.ru
Sent: Tuesday August 8, 2023 9:44 AM
Subject: New letter from Inland Revenue

Inland Revenue
Te Tari Taake

Kia Ora

You have an incoming tax refund payment on hold, awaiting account and verification:

Original URL: http://13.239.[redacted]
Click or tap to follow link

Log into myIR to rectify this issue.

- Notice of direct credit

Thanks,
Customer Service Team

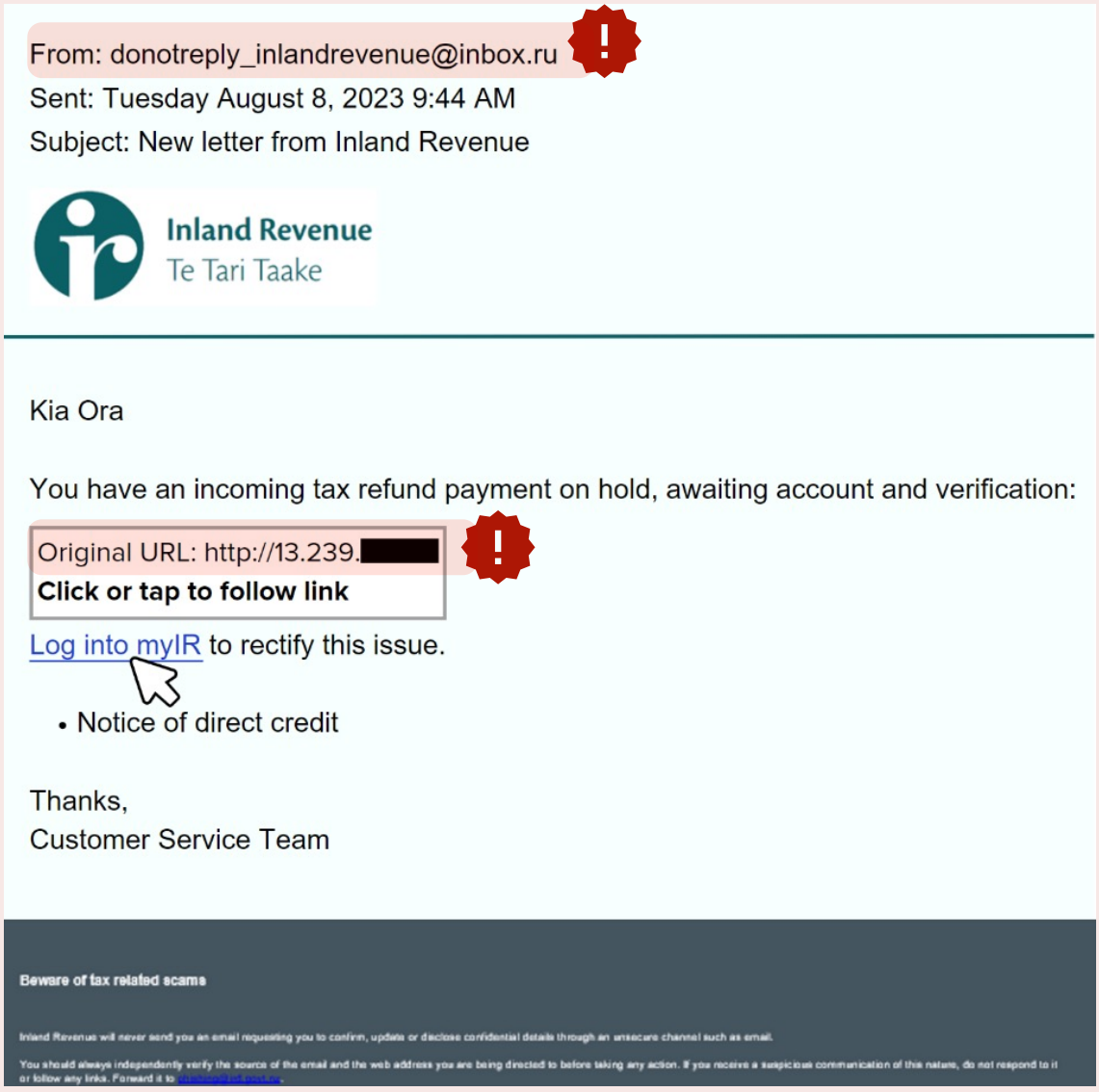
Beware of tax related scams

Inland Revenue will never send you an email requesting you to confirm, update or disclose confidential details through an unsecure channel such as email.

You should always independently verify the source of the email and the web address you are being directed to before taking any action. If you receive a suspicious communication of this nature, do not respond to it or follow any links. Forward it to [redacted].

EXAMPLE 2

The message fails two red flags – Control and Access. Even failing one red flag means it could be a scam and you should be ready to stop communicating and contact Netsafe for next steps.



From: donotreply_inlandrevenue@inbox.ru

Sent: Tuesday August 8, 2023 9:44 AM

Subject: New letter from Inland Revenue

Inland Revenue
Te Tari Taake

Kia Ora

You have an incoming tax refund payment on hold, awaiting account and verification:

Original URL: http://13.239.[redacted]
Click or tap to follow link

Log into myIR to rectify this issue.

- Notice of direct credit

Thanks,
Customer Service Team

Beware of tax related scams

Inland Revenue will never send you an email requesting you to confirm, update or disclose confidential details through an unsecure channel such as email.

You should always independently verify the source of the email and the web address you are being directed to before taking any action. If you receive a suspicious communication of this nature, do not respond to it or follow any links. Forward it to [redacted]

EXAMPLE 2 ANSWERS CONTINUED

Surprise – Often a scam may work because of timing. In this case, scammers often send IRD scams during tax season so this message may not trigger the surprise red flag.

Control – The link is for a new online space – not the IRD website.

Access – The message is asking for personal information to be entered through the link. It's likely the link will be a fake IRD sign-in page and attempt to capture your username and password.

Money – The message doesn't directly ask for payment, so may not trigger this red flag.

Explore all of our scams advice and interactive activities including videos, learning modules, fact sheets and more by visiting **netsafe.org.nz/older-people**.

On the above web page you can also check out our Little Black Book of Scams to find out almost everything you need to know about the most common scams targeting New Zealanders today.

You can download a copy to read on your device or print out the 32-page booklet to keep by the computer at home.

Additional resources

Explore our full range of Get Set Up for Safety in-depth guides, quick fact sheets and interactive learning activities for older adults and those that support them. There are over 20 to choose from, covering online safety and security topics including:

- Device & account security
- Scam awareness & response
- Social media & dating safety
- Emerging tech, accessibility and terminology

Visit netsafe.org.nz/olderpeople

If you're unsure about a situation or need further advice, you can find more information on the Netsafe website netsafe.org.nz.

We're here for you. If you require assistance or experience online harm, contact Netsafe.

Call 0508 638 723

Visit netsafe.org.nz

report.netsafe.org.nz

SPONSORED BY
CHORUS | netsafe