March 2024
TRA X CERT NZ

Cyber Security Behaviour Tracker 2024

certnz

TRA

This report

In April 2022, CERT NZ conducted research to achieve a comprehensive measure of New Zealanders' cyber security attitudes and behaviours.

Building on this insight, a 2023 survey was conducted to track how New Zealanders' cyber security attitudes and behaviours are changing over time.

Key Objectives

To track uptake of positive cyber security behaviours among New Zealanders.

What we did

A quantitative tracking survey

The online survey interviewed a nationally representative sample of 1,023 New Zealanders, aged 18 years and over.

The survey covered demographics, cyber security awareness, knowledge, barriers to change, behaviours, and information sources.

Fieldwork ran from 28th November – 7th December 2023.

The data was post-weighted to be representative of the New Zealand population in terms of age, gender, region and ethnicity.

The Margin of error at the 95% confidence interval is +/- 2.8%.

This document

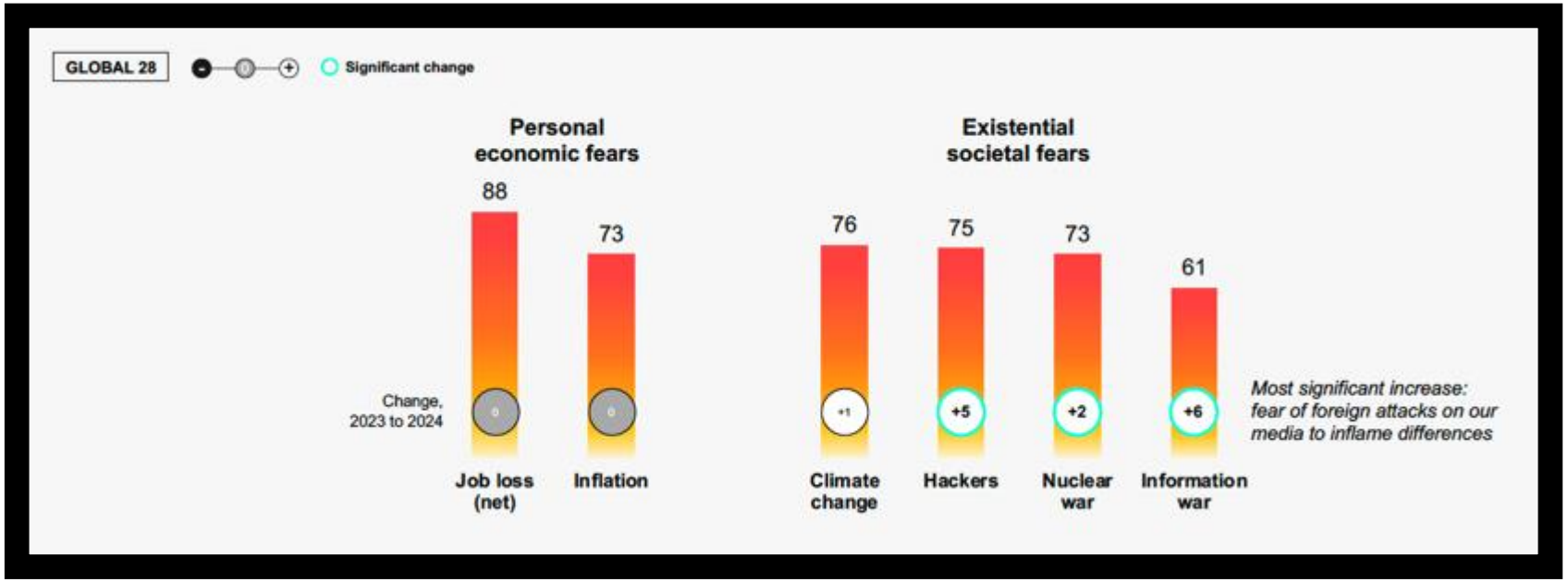
The NZ market context in 2023

1

Cyber vulnerability is a global issue, and societal concerns are on the rise

In fact, concern about hackers is growing at a faster rate than climate change globally.

Cyber vulnerability is a critical societal fear, impacting both people's personal fears and their economic stability.



https://www.edelman.com

Source: Edelman Trust Barometer 2024

Closer to home, in Aotearoa, we are not immune

In 2023 we saw extensive media coverage of cyber crime and vulnerabilities. Emerging technologies such as AI are fuelling public fears.

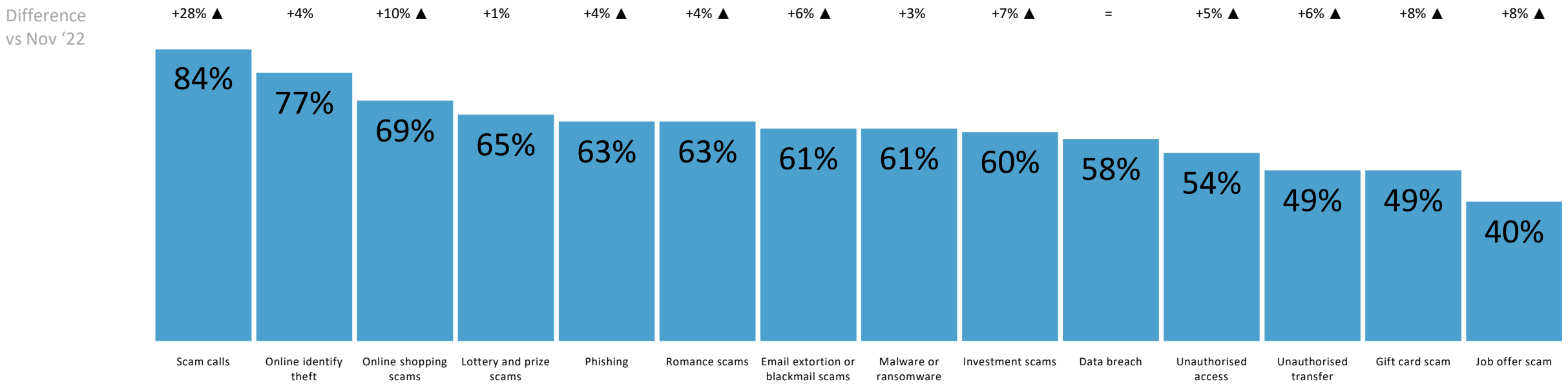
Source: TRA analysis 2023, News and current affairs

CONFIDENTIAL TRA 2023

As a result, New Zealanders are becoming increasingly aware of cyber security threats, especially scam calls

> "People ringing and saying your computer needs fixing and wants you to open your computer."

Awareness of cyber/online security threats, attacks and crime



CYBER_AWARE. From this list of cyber threats, cyber crime and online security, can you please tell us which (if any) you are aware of? Base: November 2022 n=1051, November 2023 n=1023

▼▲ Significantly lower/higher compared to Nov '22

With increased exposure to threats, public perceptions of trusted sources are fluctuating. Banks and government agencies are edging back to early 2022 levels

Top 3 trusted sources for cyber security information/advice

	36% ▲	**24%** ▲	**22%** ▲	**21%** ▲	**18%** ▲
	Banks and other financial institutions	Internet Service providers	Websites/ applications/ forums that I use	Government agencies	Family
Nov 22	21%	19%	16%	12%	13%
Apr 22	36%	28%	18%	33%	12%

INFO_RANKING. And from that same list of information sources, please choose your top three most trusted sources.
Base: April 2022 n= 1,217, November 2022 n=1051, November 2023 n=1023 (Only the five sources with the largest % of trust have been shown)

▼▲ Significantly lower/higher compared to Nov '22

In fact, Government agencies have moved from the 8th to the 4th most trusted source

Trust for Government agencies is edging back up to levels seen back in early 2022.

Top 3 trusted sources for cyber security information/advice – rankings

	April 2022	November 2022	November 2023
Banks and other financial institutions	1	1	1
Internet service providers	3	2	2
Websites / applications / forums that I use	7	3	3
Government agencies	2	8	4
Family	11	6	5
Technology brands that I use	4	7	6
Searching for information online	6	5	7
Friends	9	4	8

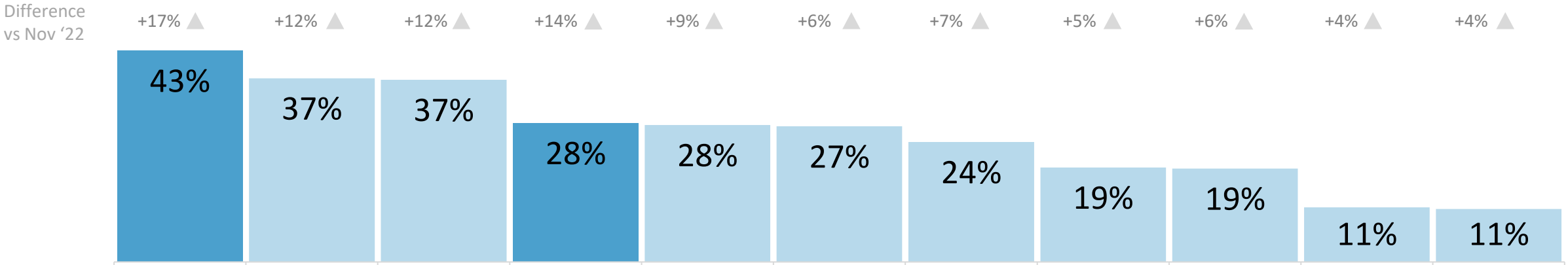
INFO_RANKING. And from that same list of information sources, please choose your top three most trusted sources.
Base: April 2022 n= 1,217, November 2022 n=1051, November 2023 n=1023 (Only the eight sources with the largest % of trust have been shown)

This trust is reflected in the sources people are using for advice and information

People go to banks and other financial institutions first, likely because of the growing financial scam experiences that the public are facing. However, Government agencies (such as CERT NZ and Police) have also seen a noticeable rise in being perceived as sources of information and advice.

> "Check with my bank first as they usually have good, up to date info on what to do and who to contact or report through to."

Sources used for cyber security information/advice



	Banks and other financial institutions	Internet service providers	Websites / applications / forums that I use	Government agencies	Family	Searching for information online	Technology brands that I use	Traditional media	Workplaces	Advertising	Industry advisors / providers
Nov 22	26%	25%	25%	14%	19%	21%	17%	14%	13%	7%	7%
Apr 22	37%	35%	28%	21%	18%	33%	27%	20%	26%	11%	14%

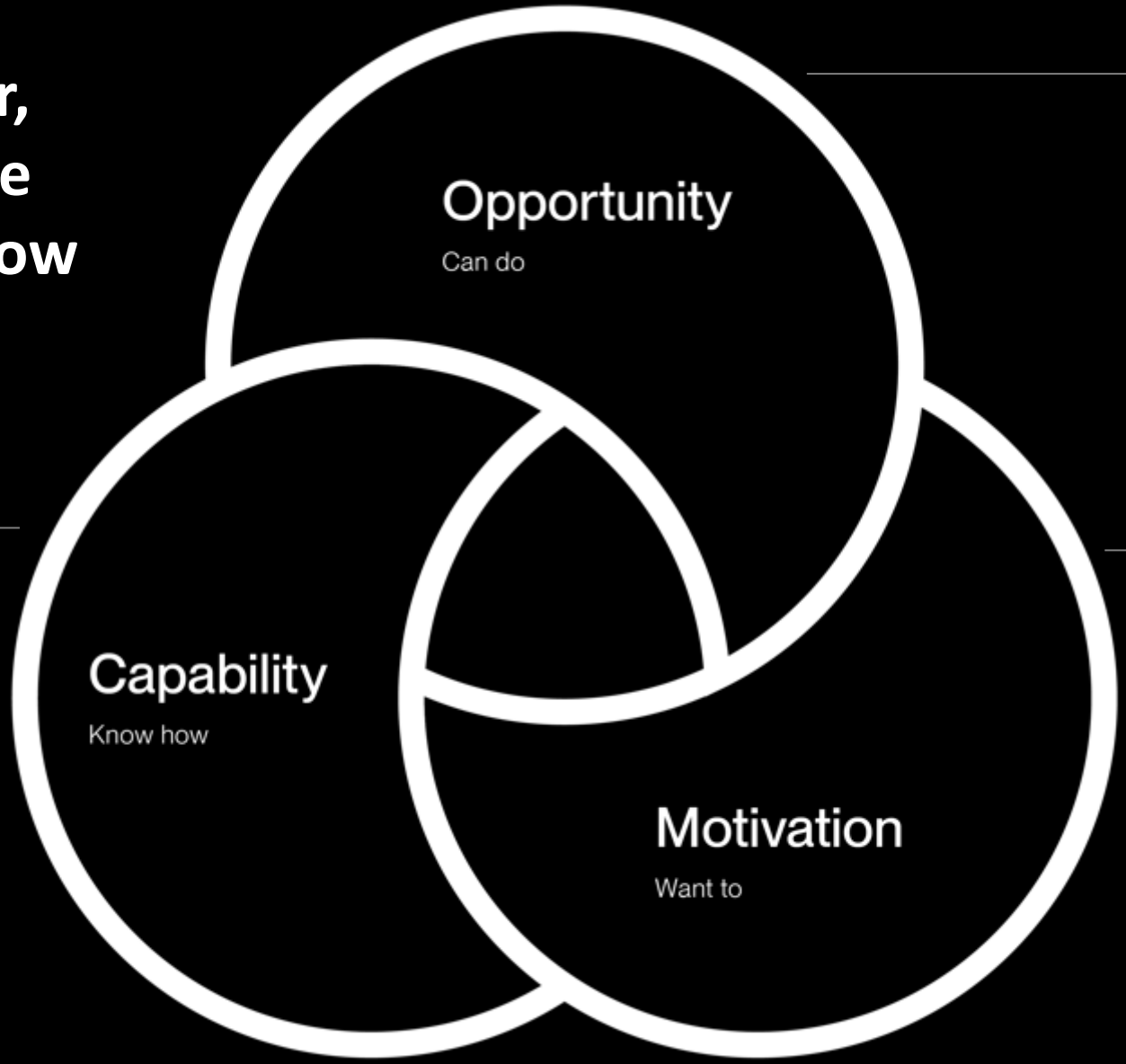
INFO_SOURCE. Where do you currently get cyber security and online security information and / or advice from?
Base: November 2022 n=1051, November 2023 n=1023 (Only significant differences at 95% C.I. have been shown)

▼▲ Significantly lower/higher compared to Nov '22

The first step in driving positive outcomes and behaviour change is ensuring people have the awareness and knowledge of cyber threats.

In the last year, we have seen greater awareness of the risks that exist but also positive behaviour when it comes to searching for more information and advice.

To change behaviour, it's important to take a holistic view on how to bring change



Do people have the 'know how' and the knowledge to be secure online?

- Awareness of the issue
- Do people know how to do the behaviour?
- Do they know what tools and actions can help keep them secure?
- How can we make it easy to be secure?

Does the opportunity present itself for people to take action?

- Despite our best intentions, we forget to act. So how can people's environment remind them to take action?
- Does the context reinforce action?
- What are the moments that matter?
- Who are the messengers that matter?

Are we using the right motivational levers to encourage people to be secure online?

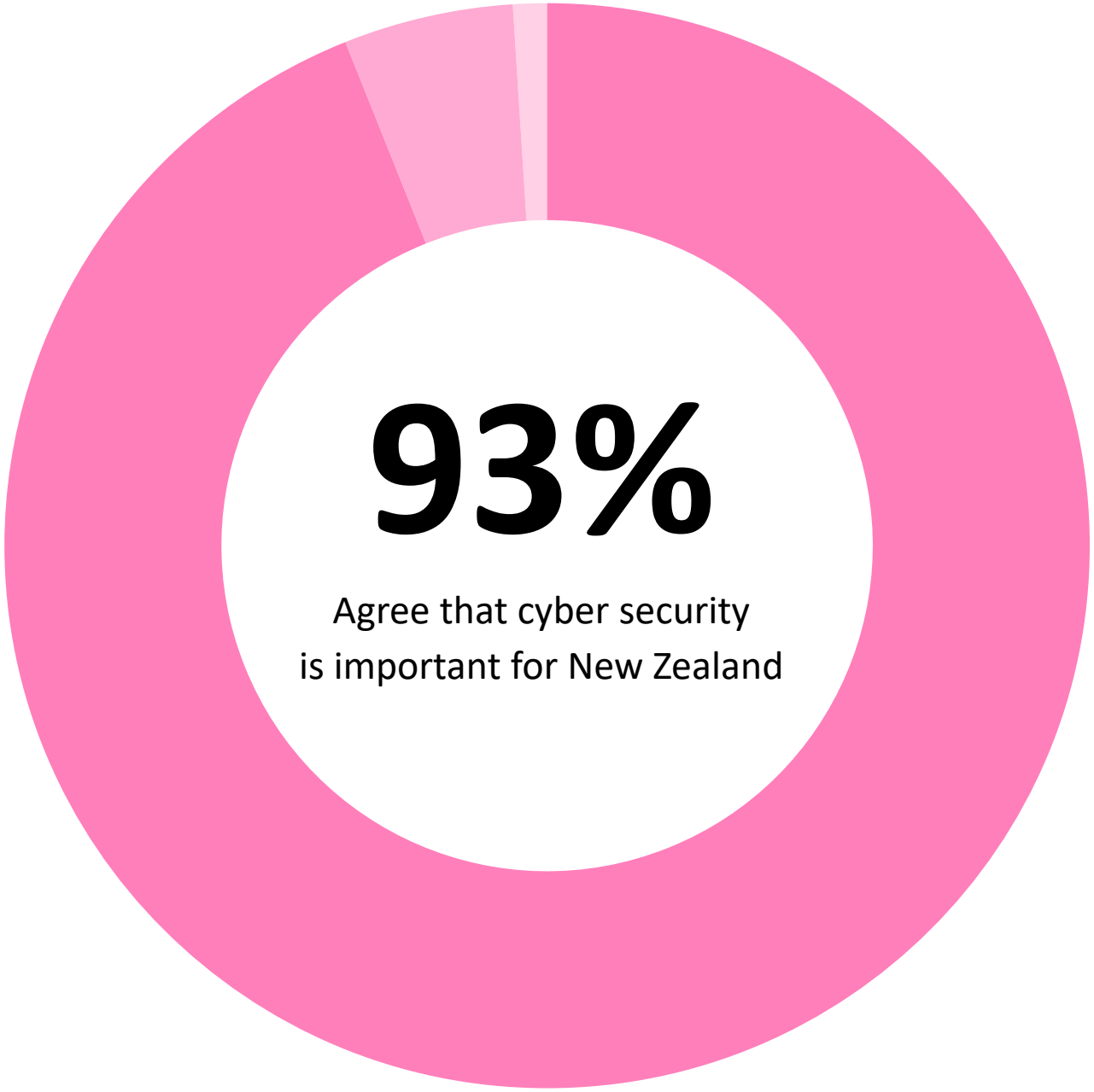
- Do people realise safe behaviour online is important?
- How can we motivate people to be secure when they are busy and acting on auto-pilot?
- How can we reward secure behaviours to encourage further action?

New Zealanders' beliefs towards cyber security

2

New Zealanders are concerned with cyber security

With cyber security incidents increasingly top of mind for New Zealanders, it's no surprise that the vast majority are concerned with cyber security.



Neither agree nor disagree = 5%, Disagree 1%
BELIEFS. Please look at the following statements and indicate how strongly you agree or disagree with each of these (NET: Agree + Agree Strongly).
Base: November 2023 n=1023

People believe the actions taken can prevent threats facing Aotearoa

Two-thirds of New Zealanders think the actions they take can prevent cyber attacks and crimes, and there is concern the public don't know what to do to prevent cyber-crime.

This reinforces the fact that there is belief in Aotearoa – we believe our actions (on balance) have an impact on the outcomes – however, we are uncertain that others know what to do.

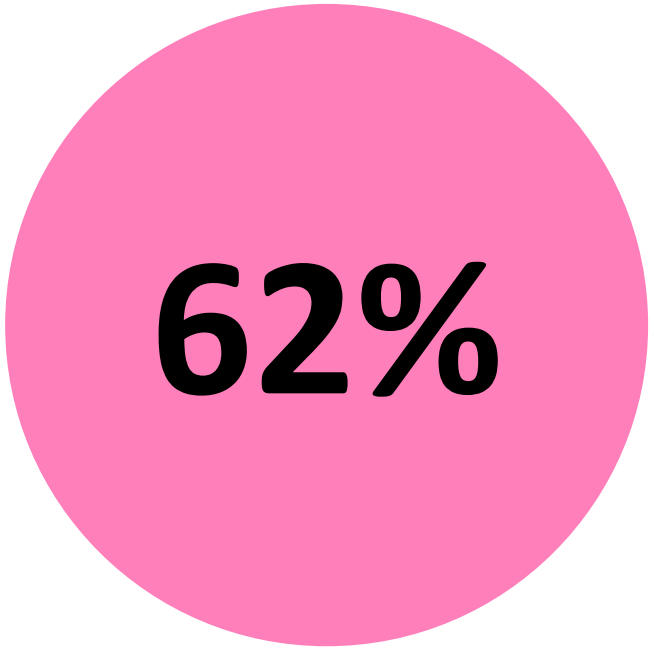
63%

Agree or strongly agree that 'the actions **they** take, can prevent cyber attacks and crimes'

56%

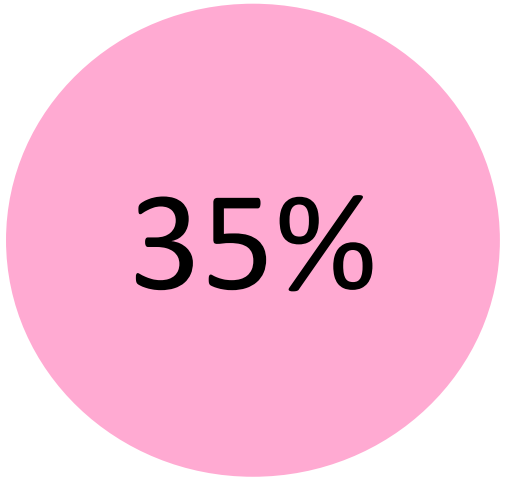
Are unsure or disagree that 'New Zealanders know what to do to stop cyber attacks and crimes'

BELIEFS. Please look at the following statements and indicate how strongly you agree or disagree with each of these (NET: Agree + Agree Strongly).
Base: November 2023 n=1023



Strongly agree it's important to protect **myself** online

Strongly agree it's important to protect **others** online

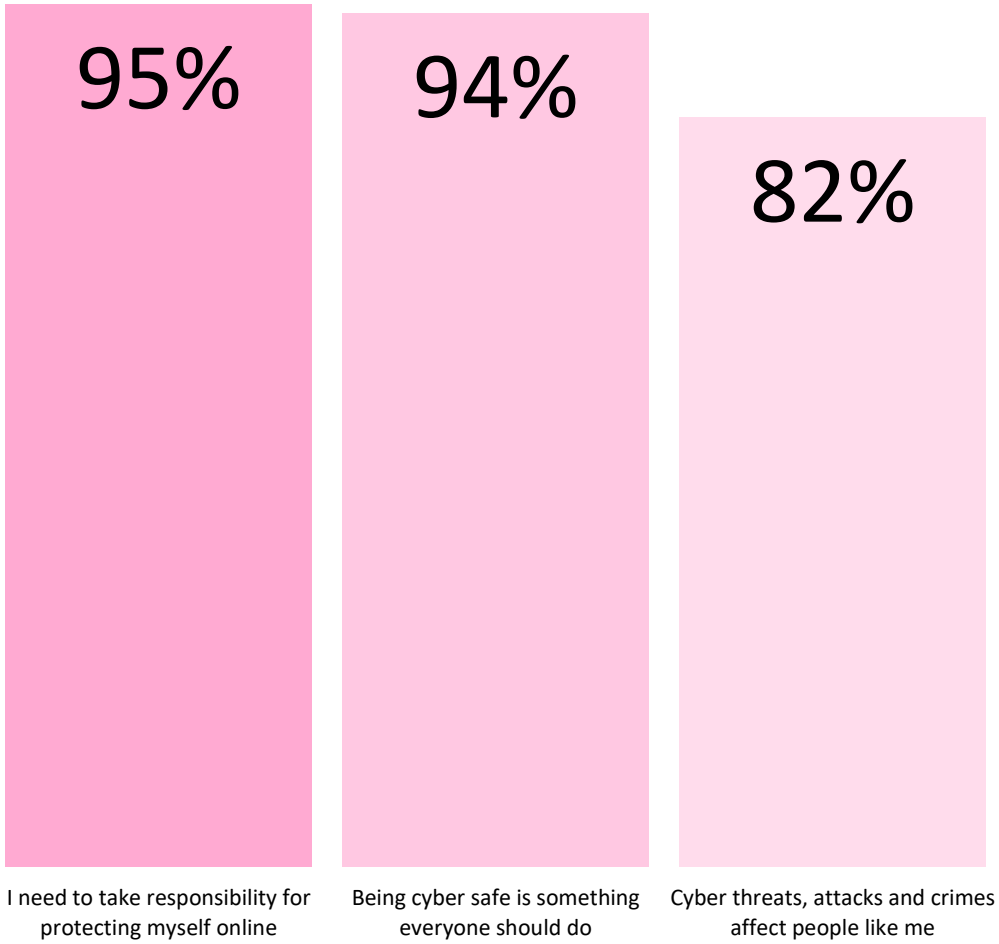


Concern is driven by personal motivation rather than altruistic motivations

With the effects of cybercrime being deeply personal, people are much more concerned with cyber security through a personal lens than a societal or collective lens.

BELIEFS. Please look at the following statements and indicate how strongly you agree or disagree with each of these (Agree Strongly).
Base: November 2023 n=1023

Agree, or agree strongly



Fortunately, most people realise that cyber security is their personal responsibility

The concern with cyber security has carried through into personal responsibility. 95% of New Zealanders know that they need to take personal responsibility for protecting themselves online. Indicating generally positive motivation.

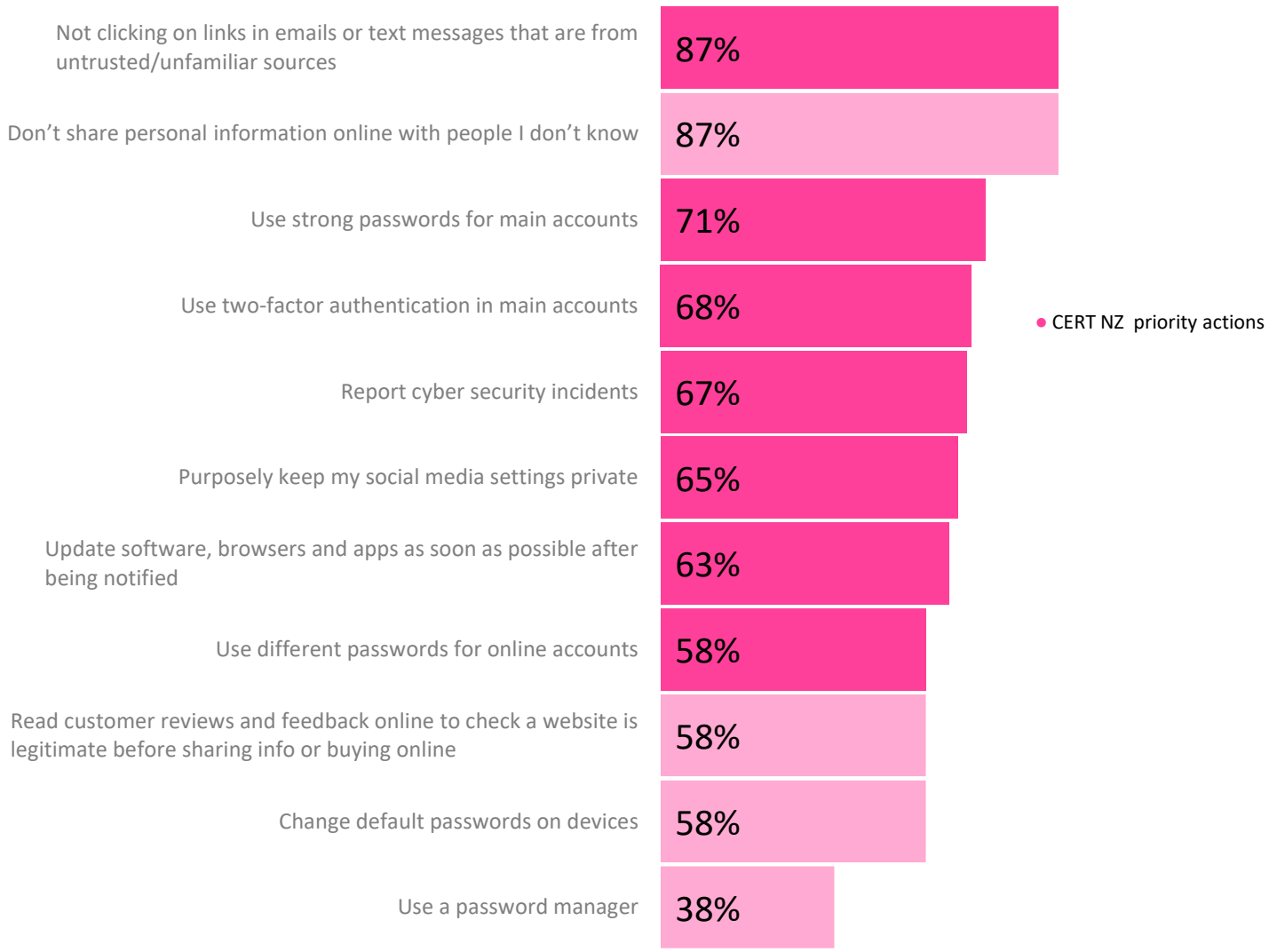
That being said, 18% of New Zealanders continue to think that cyber threats won't affect people like them. This group of people are apathetic to the risk that they face.

BELIEFS. Please look at the following statements and indicate how strongly you agree or disagree with each of these (NET: Agree + Agree Strongly).
Base: November 2023 n=1023

Not all cyber actions are viewed as equally important

While most people believe all cyber actions have a level of importance, using different passwords is considered to be less important than having strong passwords.

Cyber actions importance (Very important)



CYBER_IMPORTANCE: From this list can you please tell us how important you believe these are? (Very important).
Base: November 2023 n=1023

CONFIDENTIAL TRA 2023

Younger New Zealanders place less importance on cyber actions

Average rating for ‘Very important’ per actions by age

60% ▼
18-44 year olds

71% ▲
45-64 year olds

67%
65+ year olds

CYBER_IMPORTANCE: From this list can you please tell us how important you believe these are? (Average across all statements for ’Very important’).
Base: November 2023, 18 -44 years n=509, 45-64 years n=305, 65+ years n= 209.

▼▲ Significantly lower/higher compared to the total population

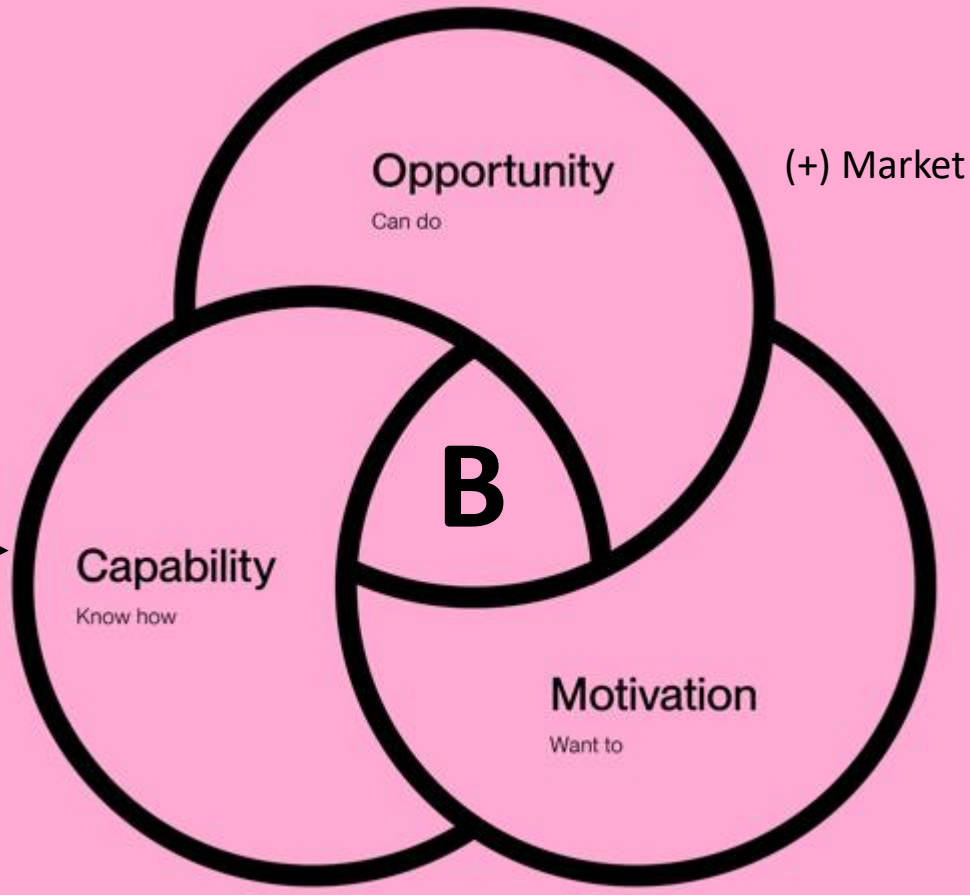
Implication:

Cyber security is important for New Zealanders

New Zealanders have the belief that the actions they take make a difference, and the market context is adding to the '*opportunity*' of thinking about and considering their actions.

They feel a personal responsibility to keep themselves secure online. These elements are key positive forces (+) on behaviour change.

But what is happening when it comes to their actions?



(+) Market context

(+) Cyber awareness

(+) Cyber importance
(+) Personal relevance
(~) Cyber action importance

It is becoming clear there is a different job to do for younger and older generations.

Cyber security behaviour

3

Over half of the New Zealand population have experienced an online security attack or crime in the past six months

This is being driven by a significant increase in events experienced by the 65+ age group. Up 8 points on Nov 2022.

Cyber security events experienced in the last 6 months

	Nov-22	Nov-23	%△
18 - 44 years	51%	54%	+3
45 - 64 years	51%	53%	+2
65+ years	49%	57%	+8▲

Note: Apr 2022 was a slightly different method for this question. PERSONAL_EXPERIENCE. From this same list of cyber threats, online security attacks and crimes, can you please tell us which (if any) you have personally experienced in the past six months? (Percentage that did not select 'None of the above'). Base: November 2023, n=1023. November 2022, n=1051. April 2022 n=1217
Base: November 2023 n=1051 (18 -44 years n=471, 45-64 years n=350, 65+ years n= 230.) November 2023 n=1023 (18 -44 years n=509, 45-64 years n=305, 65+ years n= 209).

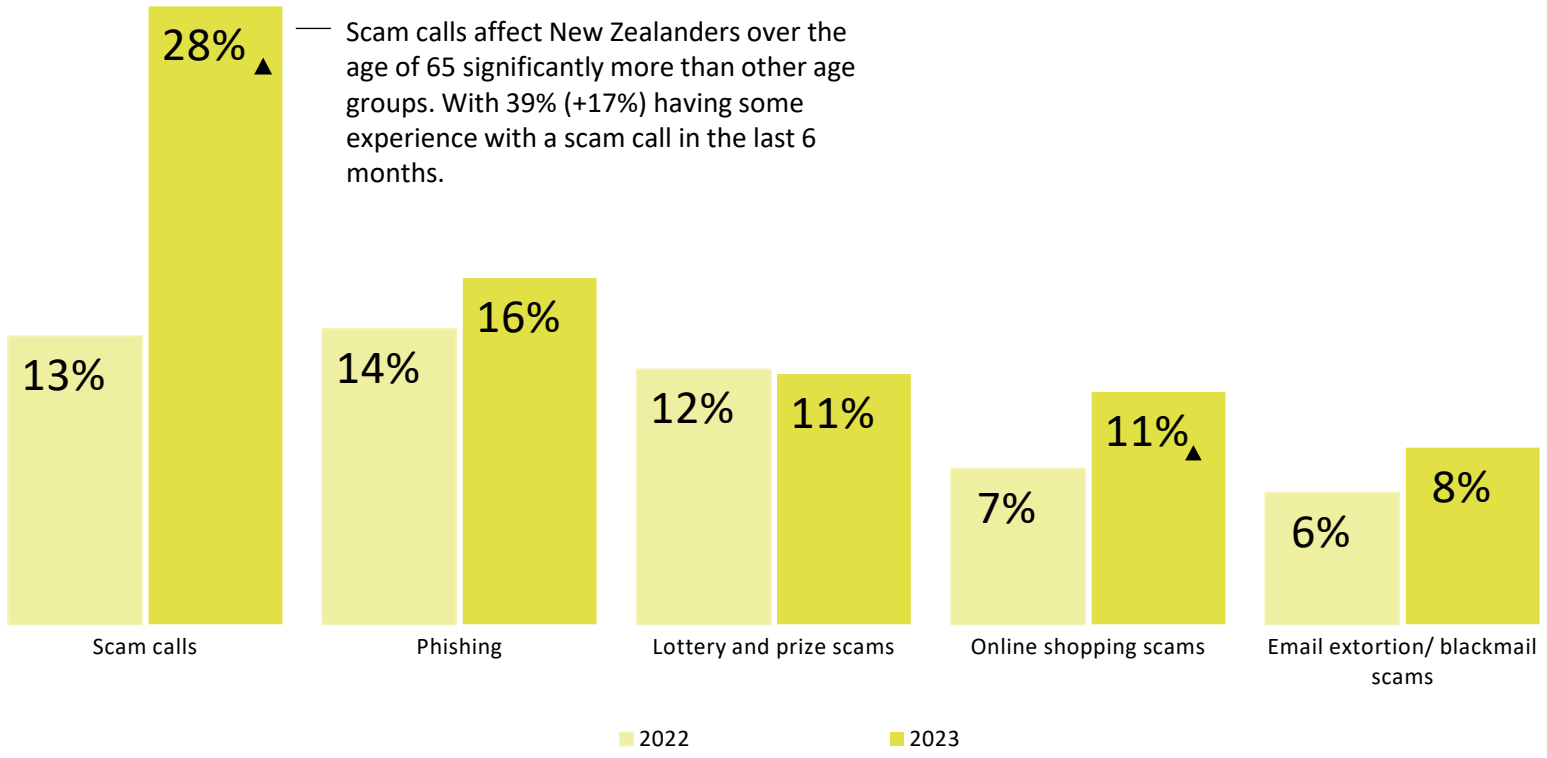
▼▲ Significantly lower/higher compared to Nov '22

In the last year, there has been a significant increase in the number of scam calls and online shopping scams.

Experience is widely prevalent across a range of threats.

Across the 14 specific threats we measure, only 4 threats saw a reduction in personal experience: gift card, investment scams, data breach and unauthorised access. This means that exposure is not just isolated to a few attacks but happening across a range of events.

Cyber security events experienced in the last 6 months (showing the top 5 threats experienced)



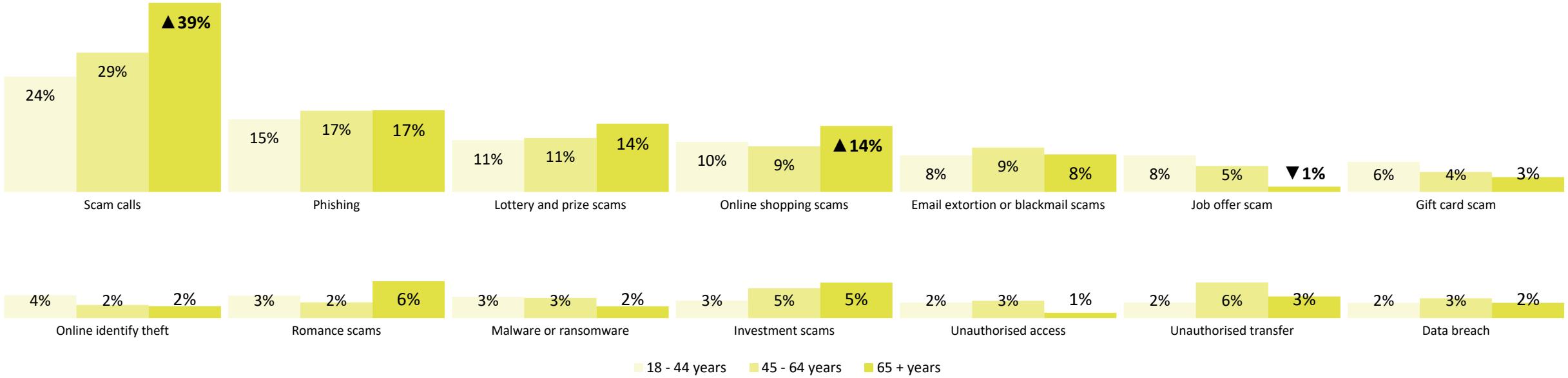
See the appendix for a full list of events
PERSONAL_EXPERIENCE. From this same list of cyber threats, online security attacks and crimes, can you please tell us which (if any) you have personally experienced in the past six months?
Base: November 2022 n=1051, November 2023 n=1023, November 2023 65+ years n= 209

▼▲ Significantly lower/higher compared to Nov '22

CONFIDENTIAL TRA 2023

Older age groups are experiencing scam calls and online shopping scams significantly more

Personal experience of cyber threats, online security attacks and crimes in the last 6 months, by age

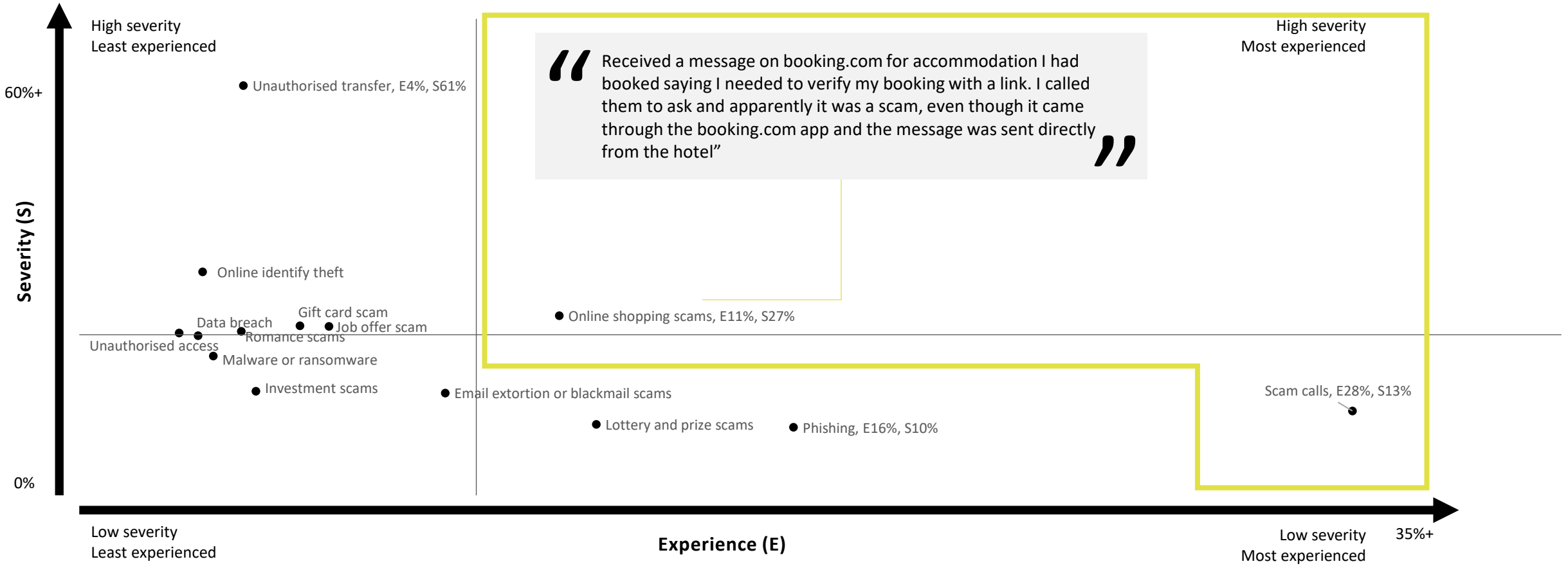


PERSONAL_EXPERIENCE. From this same list of cyber threats, online security attacks and crimes, can you please tell us which (if any) you have personally experienced in the past six months?
Base: November 2023 n=1023 (18 -44 years n=509, 45-64 years n=305, 65+ years n= 209).

Severity does range based on the threat

With online shopping scams having higher than average experience and severity, and scam calls having lower severity but much higher-than-average personal experience in 2024.

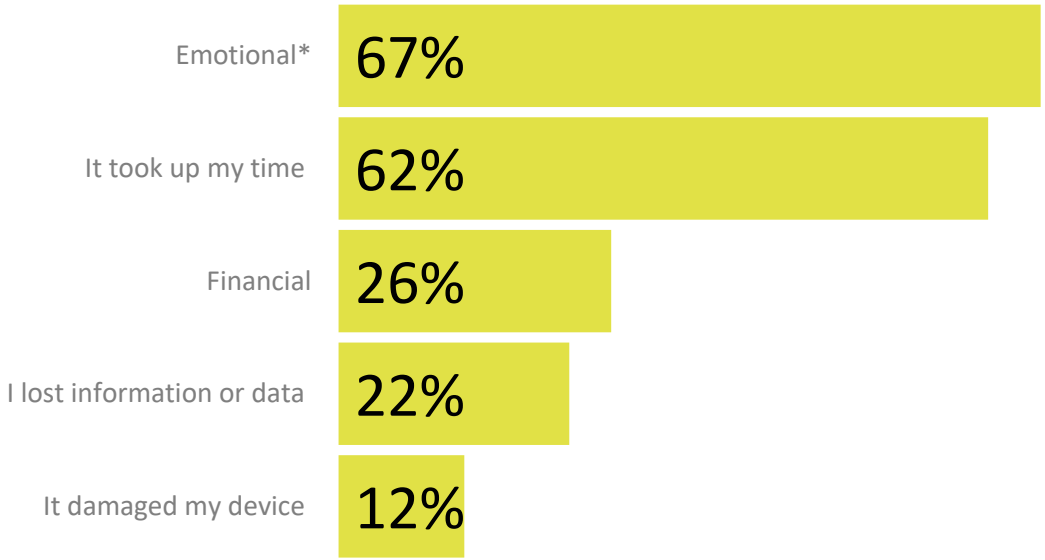
Experience of cyber attacks by severity of attack



CYBER_SEVERITY. Below are the online security issues you have experienced in the past six months. For each, can you please describe the impact it had on you? (NET: Significant + Severe)
PERSONAL_EXPERIENCE. From this same list of cyber threats, online security attacks and crimes, can you please tell us which (if any) you have personally experienced in the past six months?
Base: November 2023 n=1023.

The type of harm experienced is most commonly emotional and time wasting

'Average' type of harm experienced across all actions



CYBER_HARM: Regarding cyber threats, online security attacks and crimes you experienced, in what way were you affected?
* Emotional Harm includes stress, embarrassment, impact on relationships
Base: November 2023 n=1023. 18-44 n=509, 45-64 n=305, 65+ n=209

Interestingly we see that the 65+ age group are less likely to report harm. Under indexing significantly on emotional, financial and damage to devices.

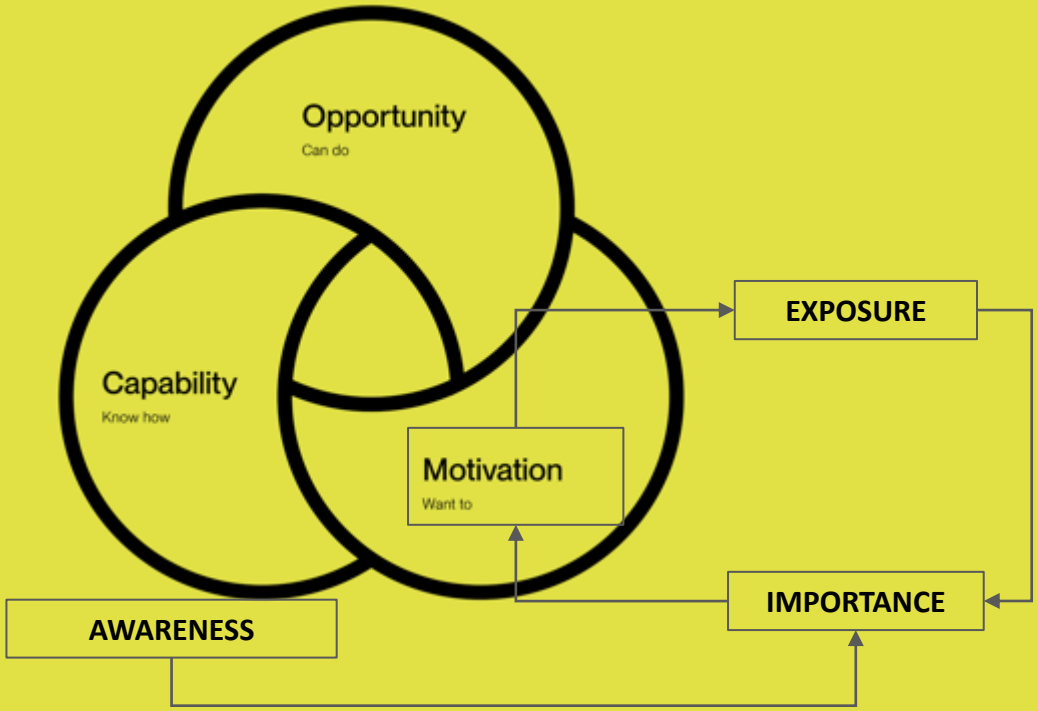
	18–44 years	45-64 years	65+ years
Emotional*	69%	69%	▼ 60%
It took up my time	57%	▲ 71%	57%
I lost money or had to pay money	28%	26%	▼ 20%
I lost personal information or data	▲ 28%	18%	20%
It damaged my device/s	15%	13%	▼ 1%

▼▲ Significantly lower/higher compared to the total population

CONFIDENTIAL TRA 2023

Implication:

Exposure to cybercrime in New Zealand is rising and intensifying



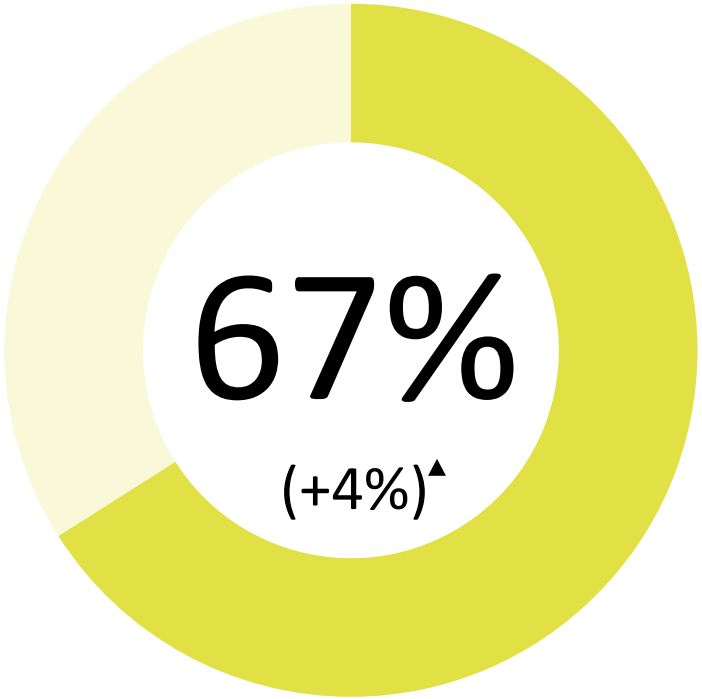
Both awareness of, and exposure to, cyber threats is rising in New Zealand.

Attacks such as scam calls and online shopping scams are not only rising in prevalence but also severity. This is particularly evident with older age groups.

Exposure and severity will have a compounding effect on motivation to do something and to take action.

CYBER_SEVERITY. Below are the online security issues you have experienced in the past six months. For each, can you please describe the impact it had on you? (*Severity: Significant + Severe)
Base: November 2023, those impacted by scam calls n=286.

Positively, people's cyber confidence has increased



feel very/quite confident about cyber security in everyday life

With greater awareness, media coverage and support from industry bodies, cyber confidence is rising in New Zealand. This is driven by younger, under 45 year olds.

Quite and very confident	November 2022	November 2023	
18 - 44 years	67%	72%	+5 ▲
45 - 64 years	62%	64%	+2
65+ years	56%	59%	+3

▼▲ Significantly lower/higher compared to the total population

CYBER_CONF. Which of the following best describes your personal confidence with online security in everyday life? For example, knowing what preventative steps to have in place, knowing how to spot something suspicious online… (NET: I feel very confident about cyber security in everyday life + I feel quite confident about cyber security in everyday life).
Base: November 2022 n=1051 (18 -44 years n=471, 45-64 years n=350, 65+ years n= 230.) November 2023 n=1023 (18 -44 years n=509, 45-64 years n=305, 65+ years n= 209).

Almost half of New Zealanders have adopted a new cyber security behaviour in the last six months

When asked what actions New Zealanders are now taking that they haven't in the past, five main buckets of actions were identified:

1. **Password Management** (Changing passwords regularly, Using strong and unique passwords)

"Using longer and more complex passwords"

2. **Two-Factor Authentication (2FA):**

"I put two factor authentication on my work email account as I work finance and deal with bank account numbers"

3. **Awareness and Caution** (Being mindful of online threats, Not clicking on suspicious links or emails):

"Going over rules with my children and checking what sites they're using"

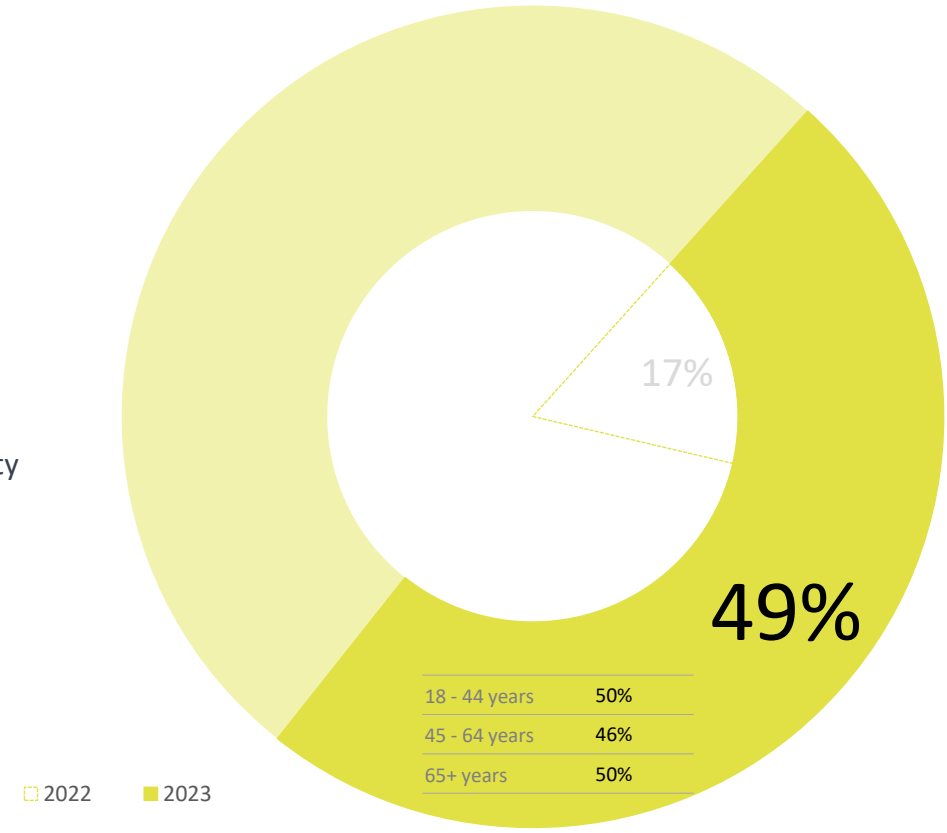
4. **Updating and Software Maintenance:**

"Keeping my devices software and security settings updated"

5. **Privacy and Social Media Management** (Making social media accounts private):

"Deleting old posts and information from social media because I don't feel the need to keep stuff that's more than a couple of years old and the less stuff I have online the better"

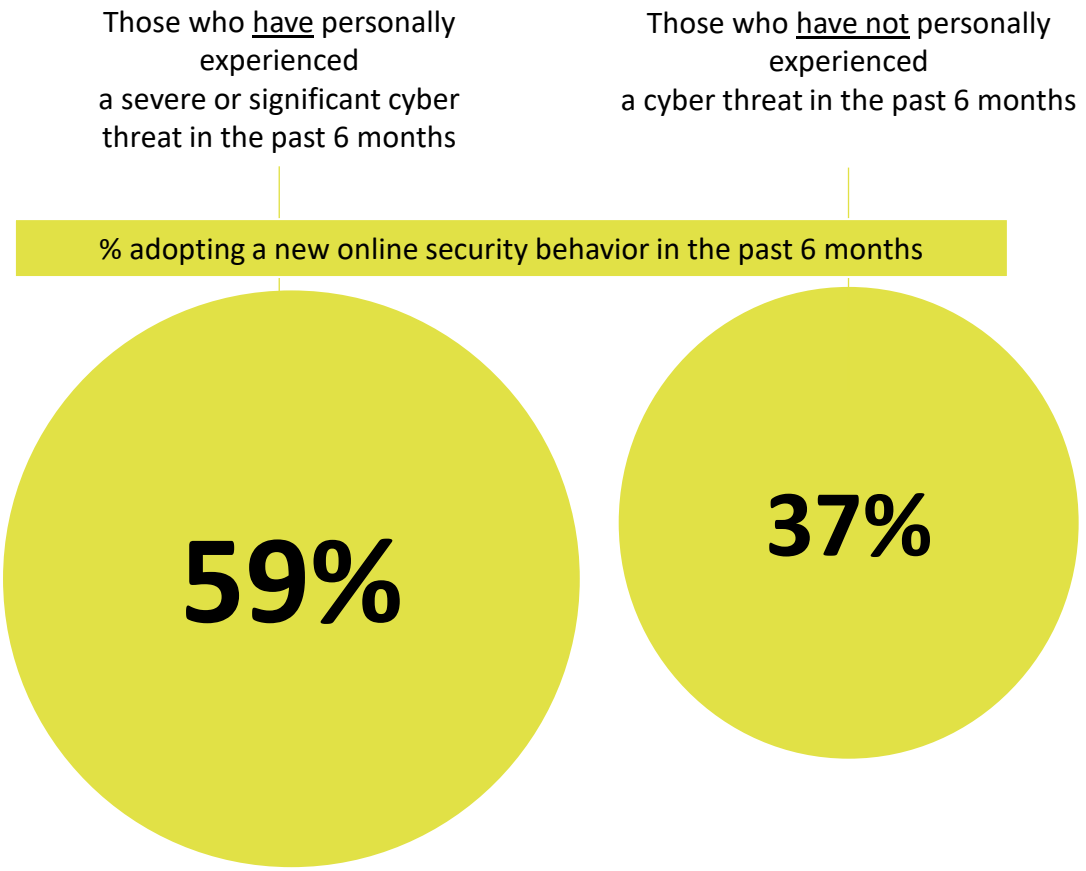
Adoption of new cyber security behaviours in the last six months



*Note, a slight question change in 2023 compared to 2022.
Nov 2022: NEW_BEHAV: In the past six months, have you started to use any new online security behaviours that you were not carrying out previously? Nov 2023 NEW_BEHAV In the past six months, have you taken any actions to keep yourself more secure online? Base: November 2023 n=1023 (November 18 -44 years n=509, 45-64 years n=305, 65+ years n= 209), November 2022 n=1051

NEW_BEHAV_OE You said that you have started to use new online security behaviours in the past six months. Can you briefly tell us what behaviour/s and why you have started using them? *Thematic coding of open-ended responses.*

We continue to see a link between threat exposure and new behaviours being adopted



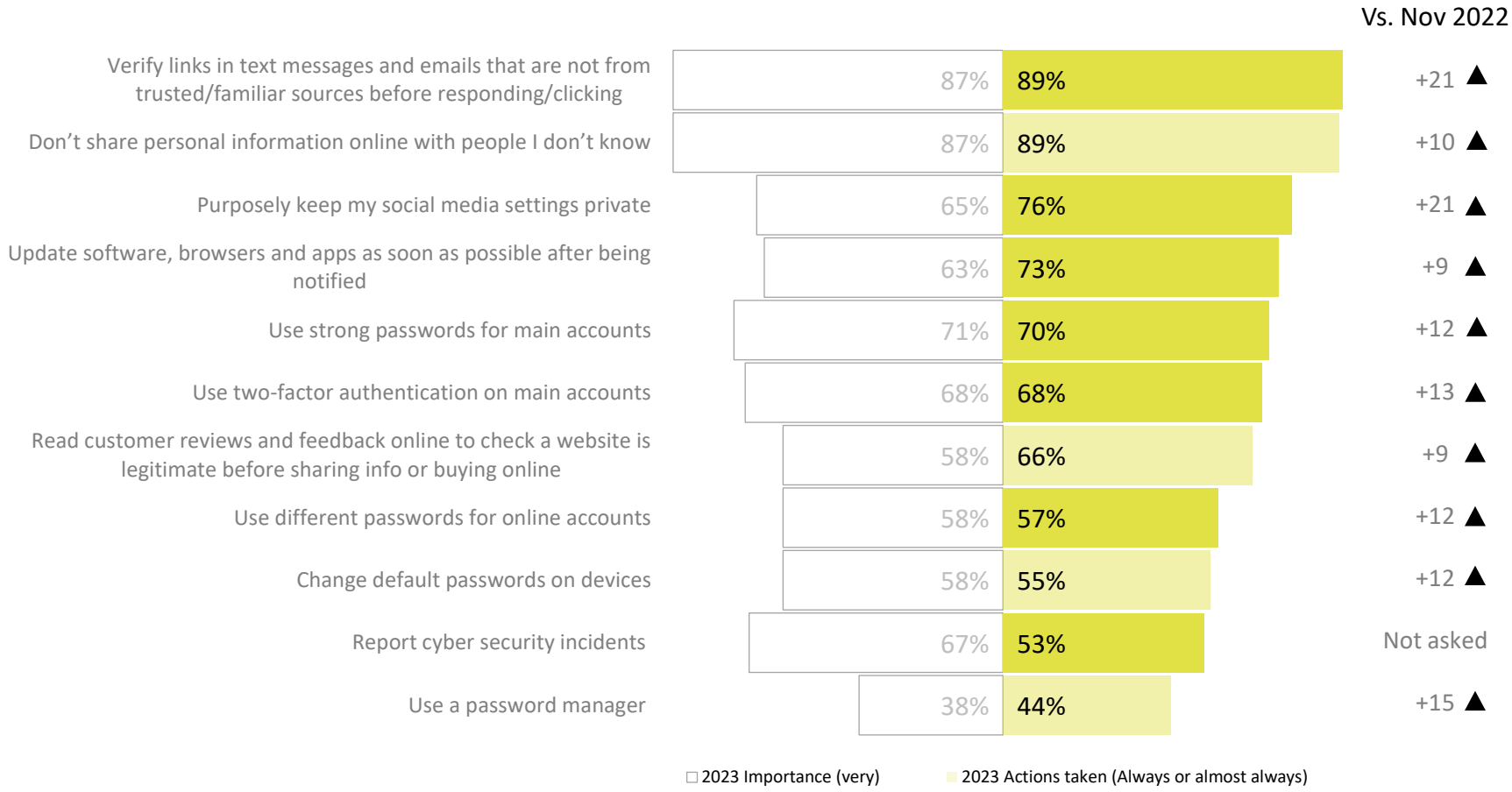
PERSONAL_EXPERIENCE. From this same list of cyber threats, online security attacks and crimes, can you please tell us which (if any) you have personally experienced in the past six months? (severe and significant)
NEW_BEHAV: In the past six months, have you started to use any new online security behaviours that you were not carrying out previously?
Base: November 2023 Those who have personally experienced severe or significant cyber threat in the last 6 months n=447 Those who have not personally experienced a severe or significant cyber threat in the last 6 months n=567

CONFIDENTIAL TRA 2023

In fact, New Zealanders are taking more actions across all key cyber behaviours compared to 2022

The increased awareness and importance of cyber actions is resulting in positive behaviour when it comes to personal actions being taken.

All CERT NZ priority actions have increased.



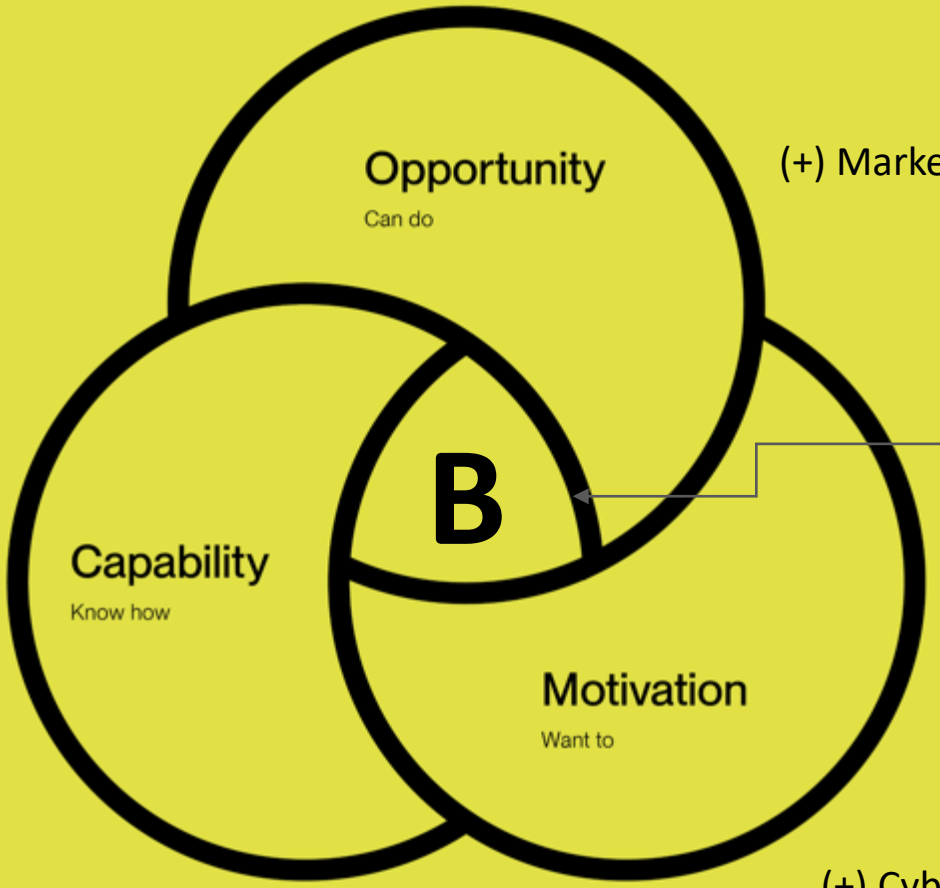
CYBER_ACTIONS2. There are a number of online security steps people can put in place to keep themselves more secure when online. From this list of online security steps, can you please tell us how often you currently do them? (NET: Always + Almost always).
CYBER_IMPORTANCE: From this list can you please tell us how important you believe these are?
Base: November 2023 n=1023. November 2022 n=1051

Implication:

We are seeing a change in behaviour

Forces such as market context, greater awareness of threats and greater importance placed on cyber security means New Zealanders are starting to adopt new behaviours.

With the significant jumps in actions taken, and almost half of the population adopting new behaviours in the last 6 months, it is clear behaviour is changing.



(+) Market context

(+) Cyber behaviour

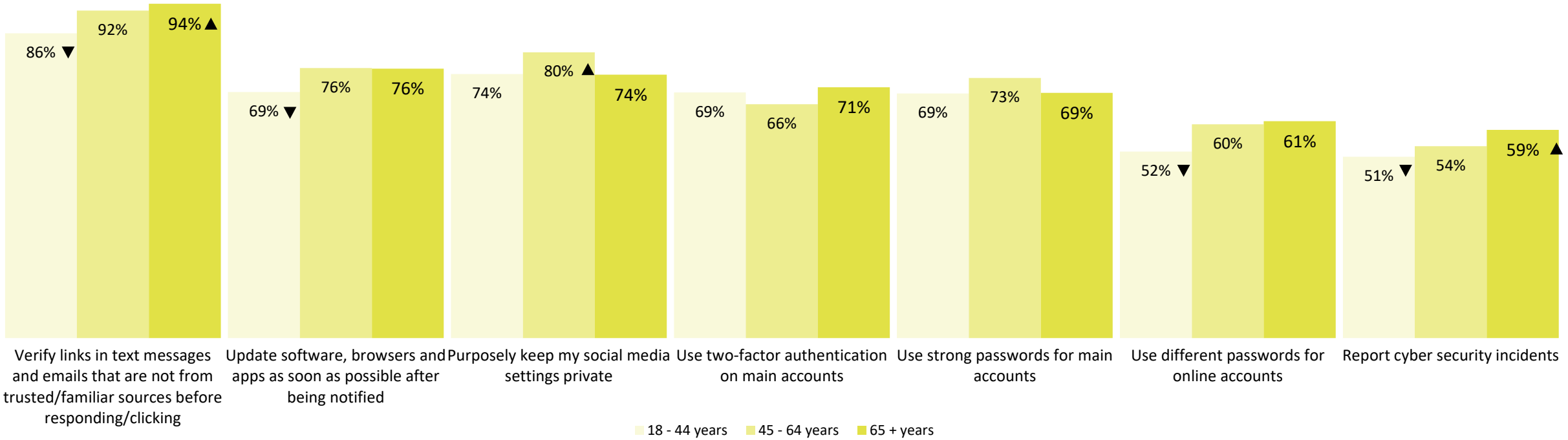
(+) Cyber awareness
(+) Confidence

(+) Cyber importance
(+) Personal relevance

Complacency among younger New Zealanders means they are taking less action than older New Zealanders

This is particularly evident across CERT NZ's priority actions, with significant differences between the older and younger age generations across a number of these actions. This is showing that additional consideration is required both when it comes to *messaging* and *the messenger* for younger and older generations.

Actions taken (Always or almost always)



CYBER_ACTIONS2. There are a number of online security steps people can put in place to keep themselves more secure when online. From this list of online security steps, can you please tell us how often you currently do them? (Always or almost always)(CERT NZ priority actions)
Base: November 2023 n=1023 (18 -44 years n=509, 45-64 years n=305, 65+ years n= 209).

▼▲ Significantly lower/higher compared to the total population

Barriers to action are consistent across the preventative measures

		2FA on main accounts	Strong passwords for main accounts	Different passwords for online accounts
% of population that are sometimes, rarely or never take the action(s)		29%	29%	43%
Motivation	**I don't want to / I can't be bothered**	19%	26%	26%
Motivation	**I feel I am already doing enough**	19%	21%	20%
Opportunity	**I keep forgetting to**	17%	22%	27%
Opportunity	**I don't have time**	11%	14%	10%
Capability	**I don't know how to do it / it's too complicated**	16%	14%	12%

WHY_BARRIERS For behaviours above where you answered sometimes, rarely, or never, please tell us what is stopping you from doing that action.
Base: November 2023 n = 1023

However, there is an opportunity to address barriers in a more targeted way

With younger (18-44 year old) audiences, focusing on:

- Time (*Opportunity*)
- Apathy (*Motivation*)

For older (over 65 years) audiences:

- Too complicated (*Capability*)
- Feeling like they are doing enough (*Motivation*)

		2FA on main accounts			Strong passwords for main accounts			Different passwords for online accounts		
		18 – 44 years	45 - 64 years	65 + years	18 – 44 years	45 - 64 years	65 + years	18 – 44 years	45 - 64 years	65 + years
Motivation	I don't want to / I can't be bothered	25%	21%	10%	32%	23%	18%	32%	24%	16%
Motivation	I feel I am already doing enough	16%	19%	29%	15%	23%	35%	18%	18%	30%
Opportunity	I keep forgetting to	18%	18%	5%	31%	26%	15%	29%	27%	21%
Opportunity	I don't have time	16%	9%	5%	17%	9%	5%	15%	8%	7%
Capability	I don't know how to do it / it's too complicated	16%	26%	35%	16%	16%	19%	11%	16%	21%

WHY_BARRIERS: For behaviours above where you answered sometimes, rarely, or never, please tell us what is stopping you from doing that action
Base: November 2023 n=1023 (18 -44 years n=509, 45-64 years n=305, 65+ years n= 209).

Implication:

We need to leverage barriers to accelerate progress with specific audience groups

We are seeing action being taken in Aotearoa, across the main actions CERT NZ are focused on.

However, barriers still exist.

A targeted approach can be taken in specific areas, with specific audiences.

Apathy (can't be bothered)

Too complicated

Time
Feeling like they are doing enough

Implication:

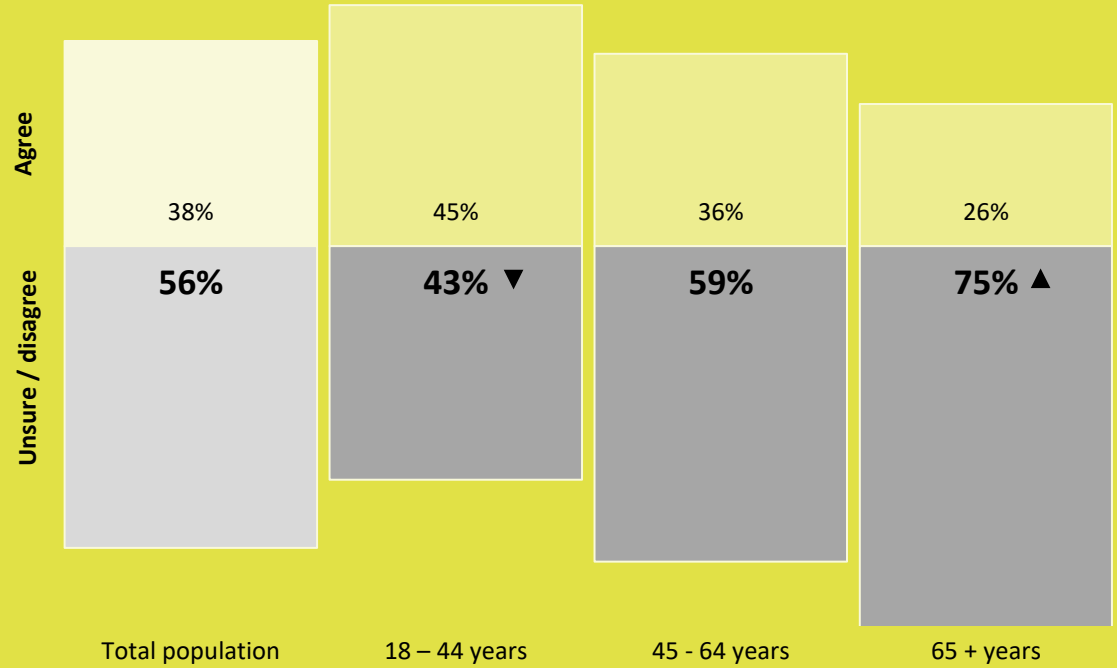
CERT NZ and Own Your Online play a critical role

Information, education and support will be critical in Aotearoa to ensure the public feel empowered and informed to act, especially helping overcoming the complexity and complacency different groups are feeling.

Currently, older people are feeling significantly more unsure if New Zealanders are equipped with the know-how regarding the mitigation of cybercrime.

56% are unsure or disagree New Zealanders know what to do to stop cyber attacks and crimes

Question statement:
New Zealanders know what to do to stop cyber attacks and crimes



▼▲ Significantly lower/higher compared to the total population

BELIEFS. Please look at the following statements and indicate how strongly you agree or disagree with each of these Base: November 2023 n=1023 (18 -44 years n=509, 45-64 years n=305, 65+ years n= 209).

Implication:

A nuanced approach can be taken across age groups

18-44 year olds

This group has significantly lower awareness of cyber threats (11 points lower on average). This awareness is offset by significantly greater cyber confidence.

This group is generally more complacent, putting significantly less importance on cyber actions overall.

They have unique motivational issues being time poor and more apathetic to the risk they face; opportunity and motivation being their largest barriers to action.

45-64 year olds

This group sits in the middle ground between the other two age brackets. Their awareness of cyber threats is consistent with the 65+ group at 66% on average. But they have the lowest reported rate of personal experience of cybercrime.

This groups sits in the middle when it comes to motivation. They don't display the apathy of the younger age bracket and aren't hampered by the lack of technical ability of the older age group.

Time is the biggest impact from threats experienced, likely due their demanding and busy lives.

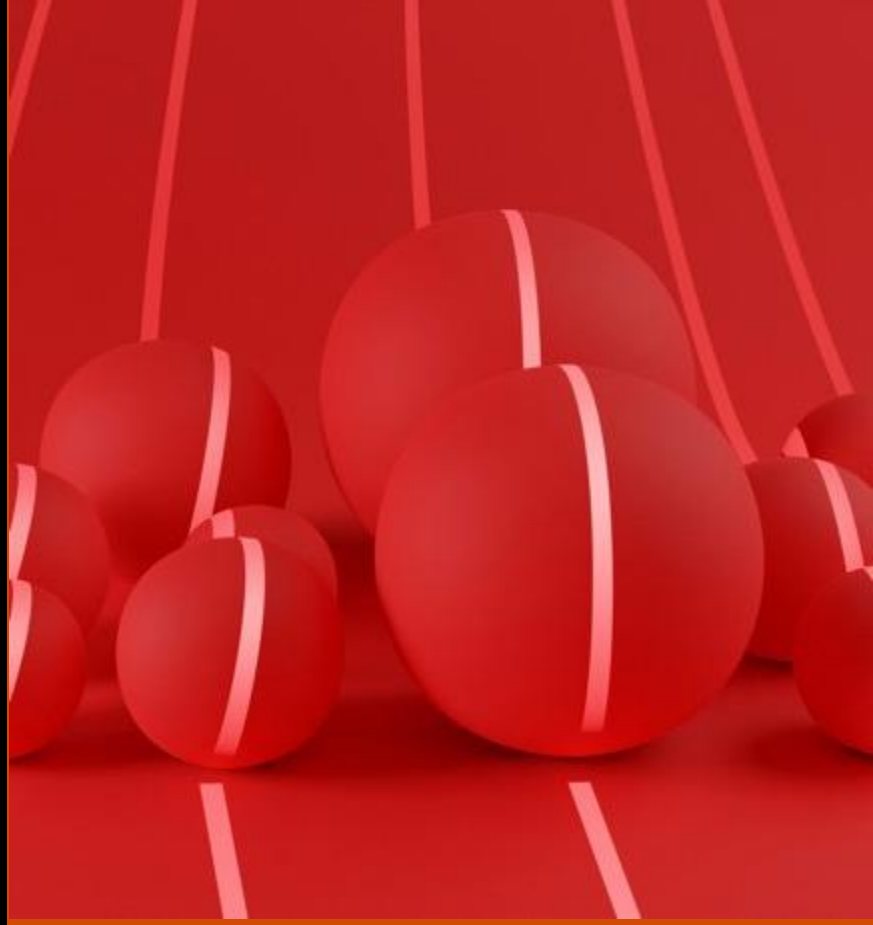
65+ year olds

This group has high awareness of threats, in line with the 45-64 year olds at 66% on average.

They have significantly less cyber confidence than the other two groups. They are experiencing cyber events at the highest rate of the groups that we measure, having also incurred the largest significant increase in cyber security events experienced from November 2022.

This group presents a unique challenge when it comes to motivation. On one hand they don't feel that they know what to do (capability) and on the other hand they feel as if they are already doing enough (motivation).

Bringing it all together



4

Aotearoa is maturing in cyber security awareness, motivation and capability

The context of cyber and its importance has been so elevated in the last 12 months that it is causing people to re-evaluate their own cyber capability and actions.

This is having a positive impact on cyber behaviour generally.

Cyber criminals don't stand still. Individuals must maintain active involvement in their personal cyber security. This might mean reinforcing good behaviour and progress being made (motivation) or leveraging different messengers to connect with audiences that existing brands or assets wouldn't otherwise reach.

Who are the messengers that matter?

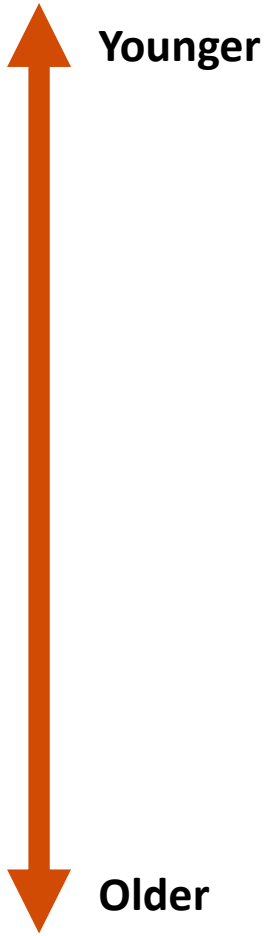
How can we reward behaviours to encourage further action?

CONFIDENTIAL TRA 2023

There is opportunity to address the generational differences and needs in the future

It is clear there are differences in the audience behaviour and needs of various demographics.

Messaging will be critical to cut through and continue to drive behaviour change and safe cyber behaviours. This might mean a variation in channels, messages and ‘the reward’.



CONFIDENTIAL TRA 2023

Appendix

Additional detailed data

PERSONAL_EXPERIENCE. From this same list of cyber threats, online security attacks and crimes, can you please tell us which (if any) you have personally experienced in the past six months?

	Nov-22	Nov-23	Change
Scam calls	13%	28%	● 15%
Phishing	14%	16%	2%
Lottery and prize scams	12%	11%	-1%
Online shopping scams	7%	11%	● 4%
Email extortion or blackmail scams	6%	8%	2%
Job offer scam	5%	6%	1%
Gift card scam	6%	5%	-1%
Investment scams	6%	4%	-2%
Unauthorised transfer	3%	4%	1%
Romance scams	4%	4%	0%
Malware or ransomware	2%	3%	1%
Online identify theft	2%	3%	1%
Data breach	4%	3%	-1%
Unauthorised access	4%	2%	-2%
● ● Significantly higher/lower than other groups			

CONFIDENTIAL TRA 2023

CYBER_HARM: Regarding cyber threats, online security attacks and crimes you experienced, in what way were you affected?

	Scam Calls	Phishing	Lottery and prize scams	Online shopping scams	Email extortion or blackmail scams
% of people experienced this	28%	16%	11%	11%	8%
It was stressful	44%	29%	43%	52%	49%
I lost money or had to pay money	7%	12%	21%	51%	7%
It took up my time	74%	58%	63%	46%	66%
It was embarrassing	21%	18%	24%	28%	33%
It impacted my mental wellbeing	19%	12%	15%	20%	23%
I lost personal information or data	6%	12%	17%	13%	20%
It damaged my device/s	4%	6%	14%	10%	5%
It impacted relationships with friends or family	5%	6%	4%	8%	7%
None of the above / prefer not to answer	9%	26%	11%	6%	11%

*Please note only the five cyber harm incidents with the highest incidence rate have been shown

CYBER_HARM: Regarding cyber threats, online security attacks and crimes you experienced, in what way were you affected?Base: November 2023 n=1023

CYBER_SEVERITY.
Below are the online security issues you have experienced in the past six months. For each, can you please describe the impact it had on you?

(Significant and severe)

	Nov-22	Nov-23	Change
Online shopping scams	25%	27%	+2%
Lottery and prize scams	13%	11%	-2%
Investment scams	10%	16%	+6%
Job offer scam	14%	25%	+11%
Gift card scam	26%	25%	-1%
Unauthorised transfer	34%	61%	+27%
Unauthorised access	32%	24%	-8%
Scam calls	9%	13%	+4%
Romance scams	23%	25%	+2%
Online identify theft	47%	33%	-14%
Data breach	30%	24%	-6%
Malware or ransomware	36%	21%	-15%
Phishing	9%	10%	+1%
Email extortion or blackmail scams	18%	15%	-3%

CONFIDENTIAL TRA 2023