Cyber Security Behaviour Tracker 2025

The NCSC runs an annual survey with The Research Agency (TRA) to analyse and track New Zealanders' cyber security knowledge, attitudes, and behaviour.

This research has also been conducted in 2023 and 2024. Comparisons to results of previous years are included where applicable.

May 2025
TRA X NCSC

National Cyber Security Centre

TRA

What we did

A quantitative tracking survey

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

Fieldwork ran from 25th November to 3rd December 2024.

The survey interviewed a nationally representative sample of n=1,006 New Zealanders aged 18 years and over.

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 (MOE) at the 95% level of confidence on overall results (n=1,006) is +/- 3.1%.

Agenda

The broader landscape	1
Cyber security threats	2
Cyber security attitudes and behaviours	3

Story in a nutshell

Cyber security remains highly topical in New Zealand with New Zealanders facing a range of online threats. In the last year especially, this topic has generated widespread media coverage, with online discussions being driven by a variety of organisations.

People are becoming more confident in their cyber security, though awareness and experience of threats remains steady.

Time and stress are the most common impacts, but many also experience financial loss, and this represents a significant cost to New Zealand.

In spite of this, nearly half don't report the cyber attacks they experience, and this behaviour has decreased year-on-year.

Although people personally believe cyber security is important, they don't think others do, which undermines the likelihood of taking action. Last year's increase in preventative actions has held, but there's apathy amongst those not acting.

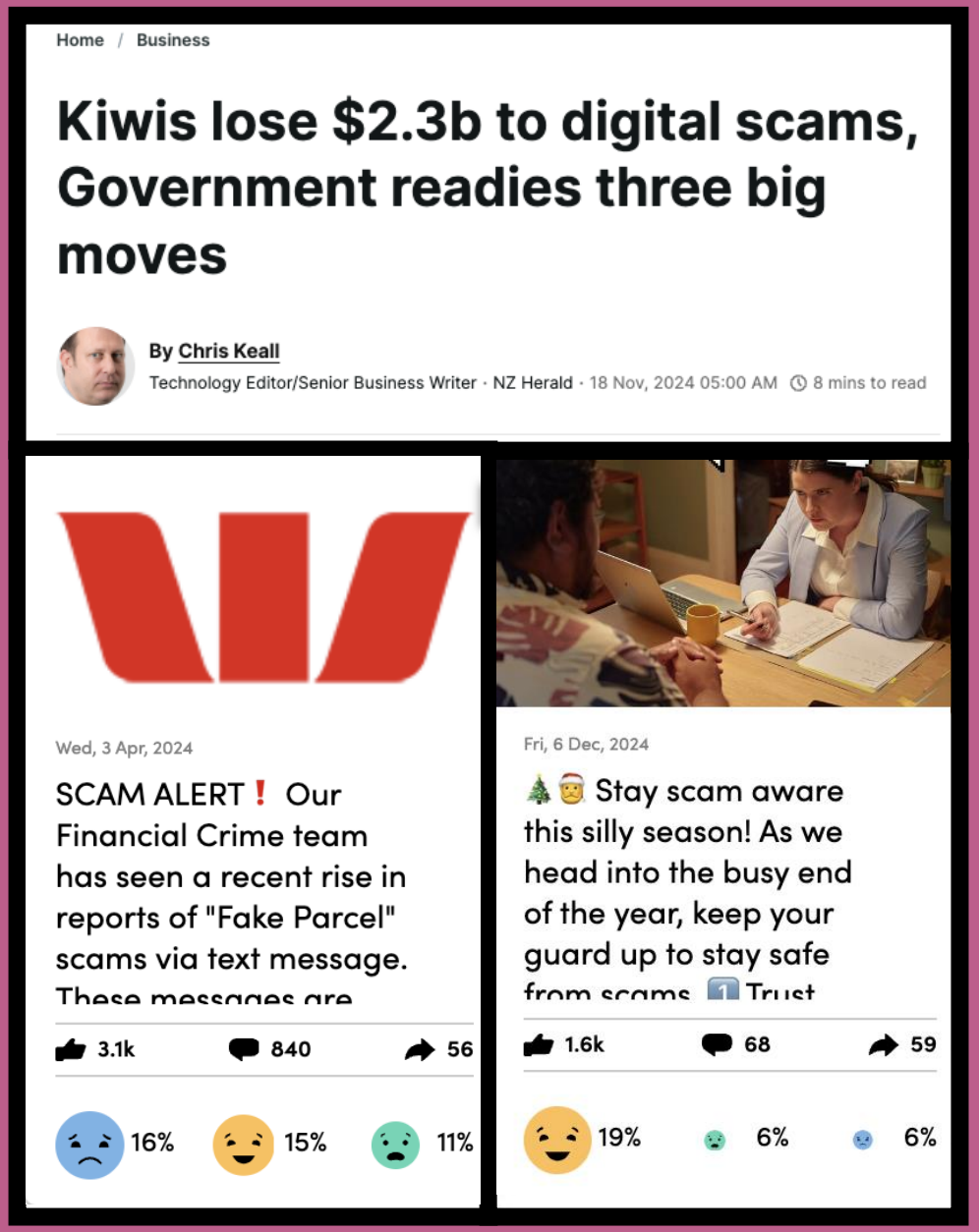
The NCSC is focused on threats that can be prevented by cyber security actions. Responders were asked about a range of online security threats to best understand the threat landscape.

The broader landscape

1

Cyber security has continued to remain topical for New Zealanders

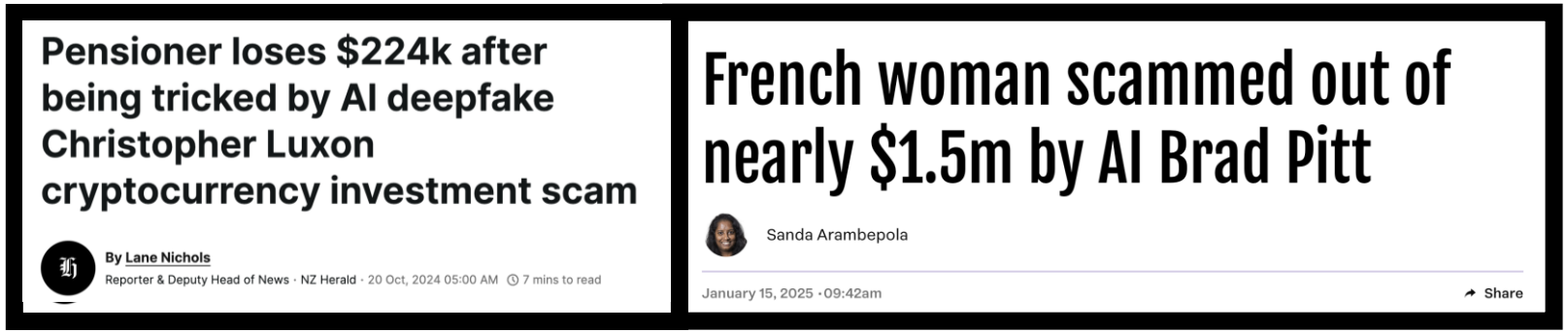
And it remains highly discussed on social media by both individuals and brands. In particular, banks are leading this conversation like never before.



Source: The New Zealand Herald, 2024.
Zavy Radar.

However, now that cyber security is clearly in the public eye, threats are becoming more advanced

Cybercriminals are expanding their toolkits through the use of AI and cryptocurrency to make their attacks disguised and untraceable.



They also capitalise on current events and common personal messages to disguise their threats.

- Crowdstrike
- Postal or courier delivery messages
- Overdue bills / road toll messages

Source: The New Zealand Herald, 2024.
Stuff, 2024.

So, with much public focus on cyber security, and increasingly advanced threats, how is this playing out for Kiwi, in terms of…

1. How they are experiencing cyber threats?
2. The actions they are taking to protect themselves online?

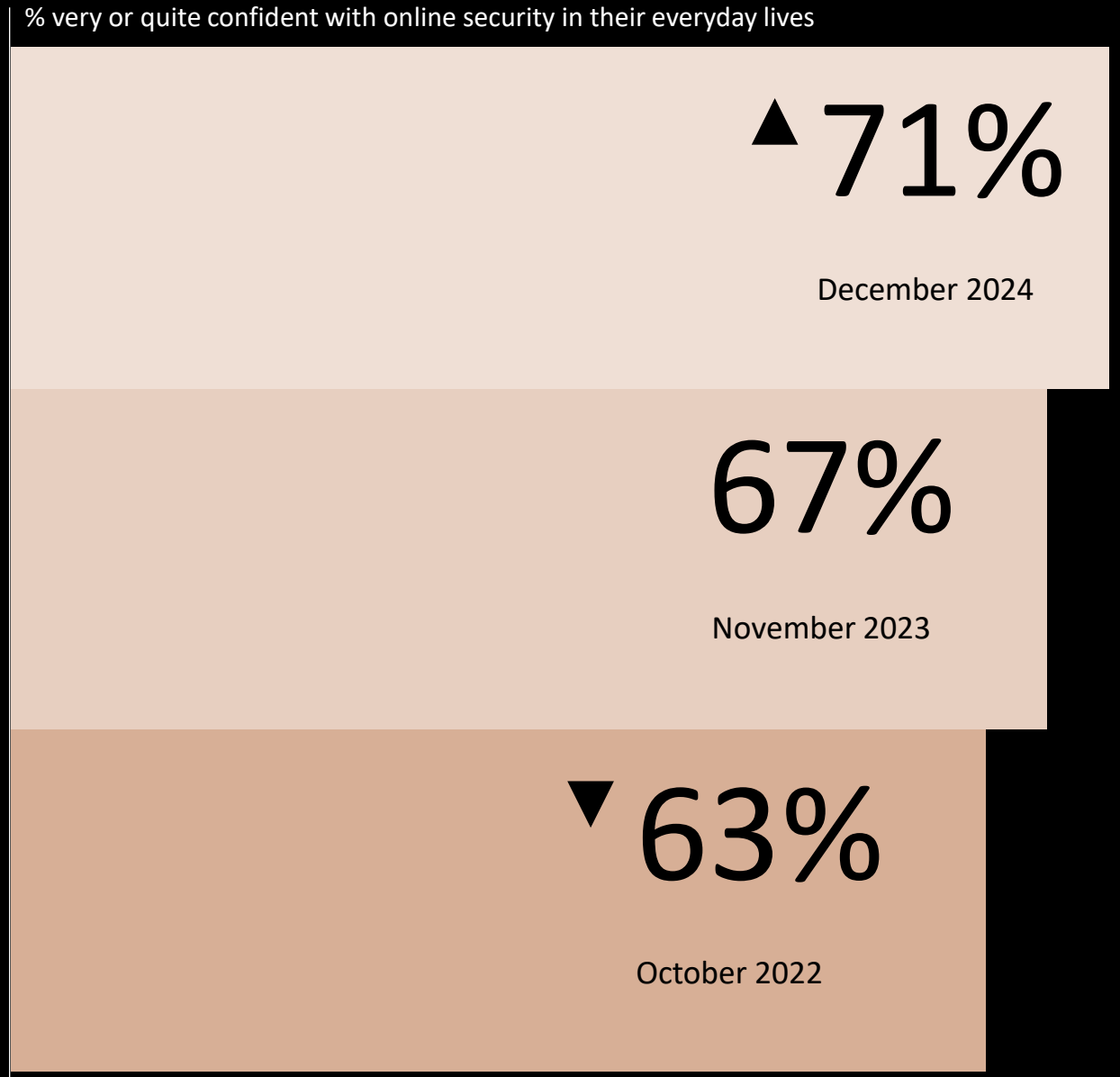
Cyber security threats

While cyber security threats can be prevented through cyber security actions, other types of online threats often rely on deceiving someone into doing something, and rely on a victim to identify the activity as suspicious. Changing cyber security behaviours and implementing cyber security actions can help people protect themselves from a range of online threats.

Note: While cyber-dependent crime remains the focus for the NCSC, this report includes data about cyber-enabled crime in an effort to best understand how New Zealanders think about and approach a range of cyber security issues.

New Zealanders are becoming increasingly confident in their ability to navigate cyber security

18-34 year olds feel the most confident, but this is growing across all ages and genders.



CYBER_CONF: Which of the following best describes your personal confidence with online security in everyday life?
For example, knowing what preventative steps to take and putting them in place, knowing how to spot something suspicious online…
Base: Total sample 2022 n=1,051; 2023 n=1,023; 2024 n=1,006.

▲▼ Significantly higher/lower than other years

Awareness of specific online threats has held fairly stable overall

Just four threats show a significant shift in awareness	2024	Change vs 2023
Online identify theft	**70%**	**-7**
Phishing	**67%**	**+4**
Unauthorised access	**48%**	**-6**
Job offer scam	**44%**	**+4**

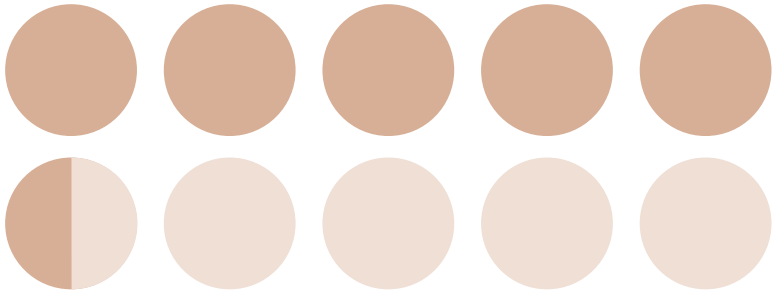
All others remain relatively steady	2024	Change vs 2023
Scam calls	**82%**	**-2**
Online shopping scams	**68%**	**-1**
Lottery and prize scams	**62%**	**-3**
Malware or ransomware	**61%**	**=**
Investment scams	**60%**	**=**
Email extortion or blackmail scams	**60%**	**-1**
Romance scams	**59%**	**-4**
Data breach	**55%**	**-3**
Gift card scam	**47%**	**-2**
Unauthorised transfer	**46%**	**-3**

TRA // National Cyber Security Centre

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?
*See appendix for full wording presented to respondents to describe the threats
Base: Total sample 2023 n=1,023; 2024 n=1,006.

And a similar number of people have experienced online threats

Scam calls reduce in prevalence but remain the threat most experienced.



54%

of New Zealanders experienced a threat in the last 6 months

(no change compared to 2023)

Significant shifts in personal experience	2024	Change vs 2023
Scam calls	23%	-5
Unauthorised access	4%	+2

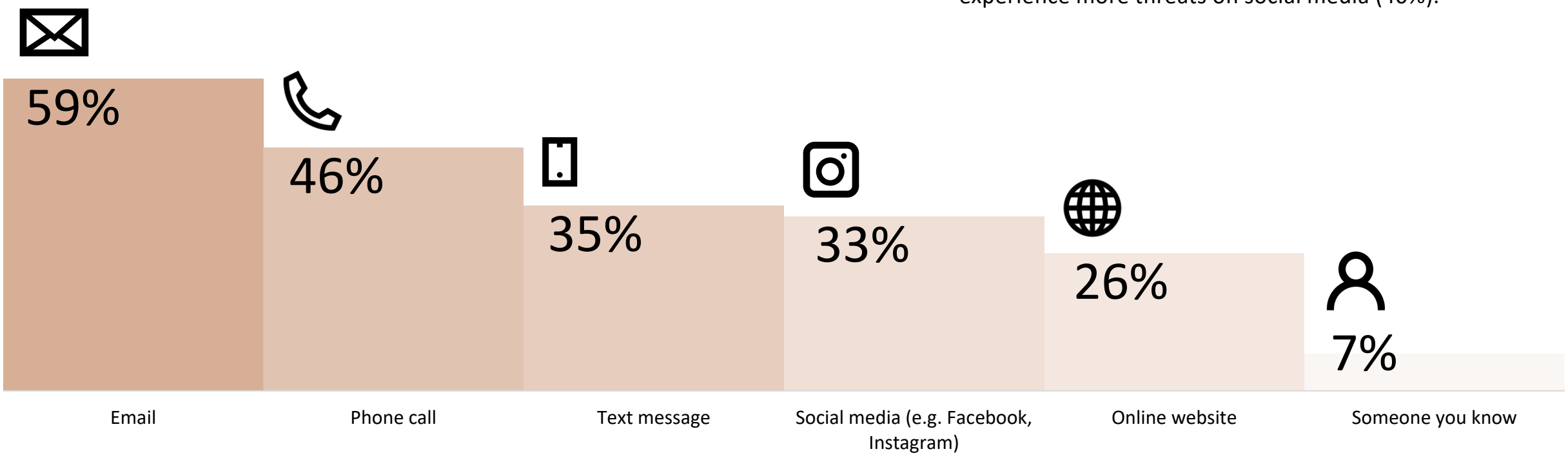
Other personal experience	2024	Change vs 2023
Phishing	14%	-2
Lottery and prize scams	10%	-1
Online shopping scams	9%	-2
Job offer scam	7%	+1
Email extortion or blackmail scams	7%	-1
Gift card scam	6%	+1
Investment scams	5%	+1
Unauthorised transfer	4%	=
Data breach	3%	=
Malware or ransomware	3%	=
Romance scams	3%	-1
Online identify theft	3%	=

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: Total sample 2023 n=1,023; 2024 n=1,006.

Most threats are encountered online, but traditional channels like phone calls and texts are also targeted

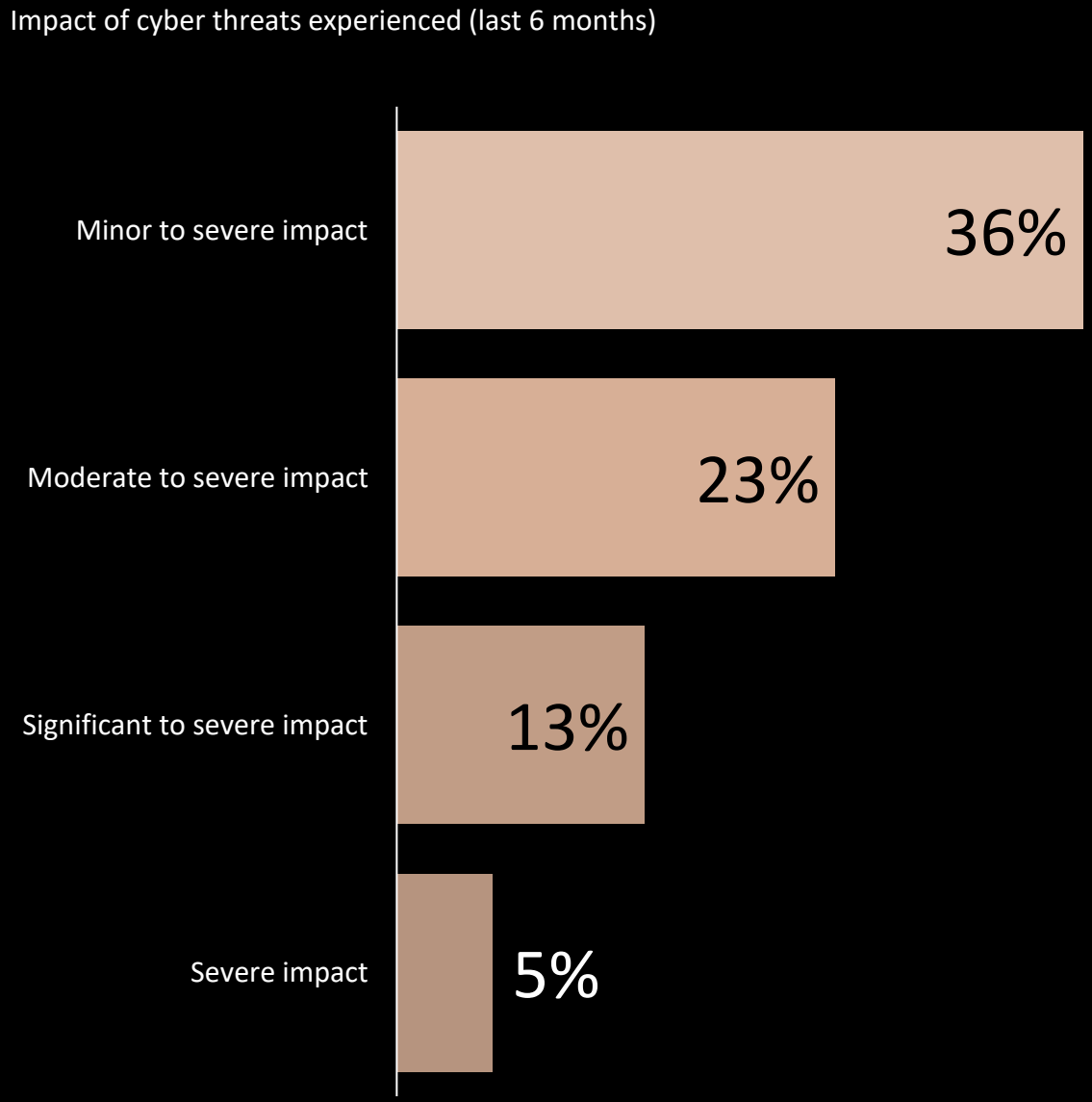
Platform where threats were experienced

55+ year olds are more likely to experience online security threats through phone calls (53%), and 18-34 year olds experience more threats on social media (40%).



CYBER_PLATFORM: Below are the online security issues you have experienced in the past six months.
For each, where did you experience the issue?
Base: People who experienced a cyber threat 2024 n=523.

36% of New Zealanders have been impacted by an online threat in the last six months

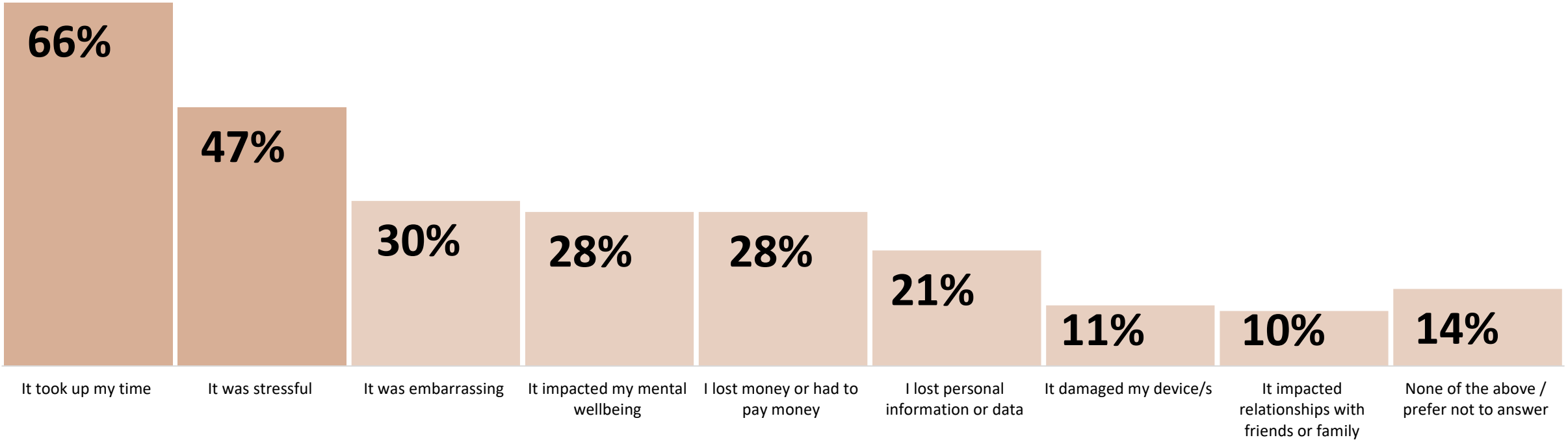


CYBER_SEVERITY: Below are the online security issues you have experienced in the past six months. For each, can you please describe the impact it had on you?
Base: Total sample 2024 n=1,006.

Time-loss and stress are the most common impacts of online threats

Many who experience scams have their mental wellbeing impacted too.

Type of harm inflicted by cyber threats (amongst those who experienced harm)



CYBER_HARM: Regarding the cyber threats, online security attacks and crimes you experienced, in what way were you affected?
Base: People who experienced minor-severe cyber harm 2024 n=361.

When people lose money, the impact experienced is especially meaningful

88%

of those who lost money described the impact as moderate, significant or severe

CYBER_HARM: Regarding the cyber threats, online security attacks and crimes you experienced, in what way were you affected?
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?
Base: People who lost money in a cyber attack 2024 n=98.

A conservative sizing of the financial loss suffered by New Zealanders due to online threats is $1.6 billion

Financial loss from cyber attacks in 2024

830,000

Number of people experiencing financial loss

1,300,000

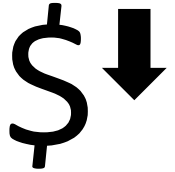
Total number of online attacks where financial loss was experienced

1.6

Average number of attacks experienced per target

$1.6B

Total amount lost in 2024



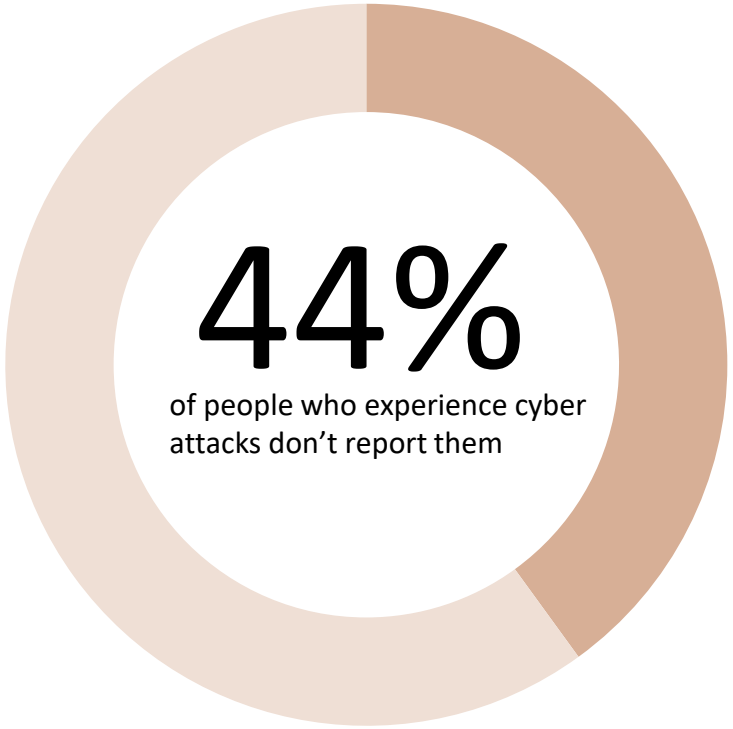
$1,260

Average amount lost per online attack

Figures are approximate. The margin of error at the 95% level of confidence on estimates is +/- 3.1%. The estimated total amount lost falls within a 95% confidence interval of 95% confidence interval of $1.58B and $1.68B.
The average amount lost by each target who experienced financial loss was $1950.
CYBER_HARM: Regarding the cyber threats, online security attacks and crimes you experienced, in what way were you affected?
CYBER_LOSS: For each issue, approximately how much money did you lose or have to pay?
Base: Total sample 2024 n=1,006.

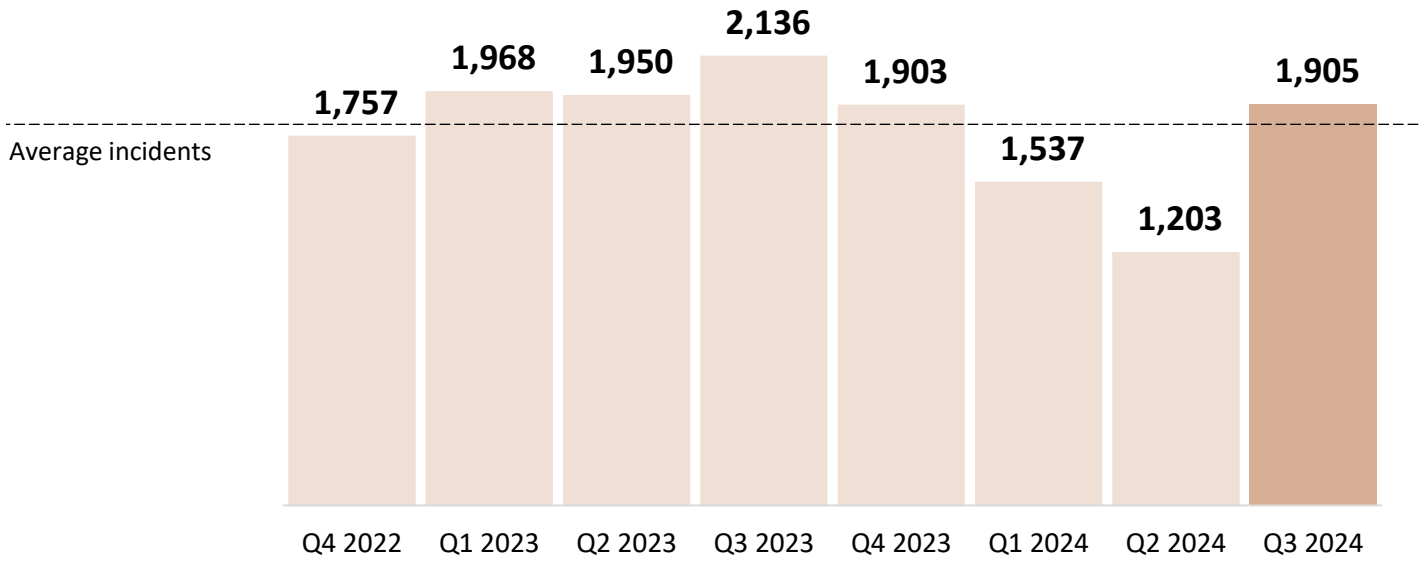
Despite the harm experienced through online threats, nearly half don’t report the attacks they experience

Males are less likley to report cyber threats (51% who experience cyber attacks don’t report them).



Number of incidents

A total of 1,905 incidents were reported via the NCSC’s online reporting tool in Q3 2024

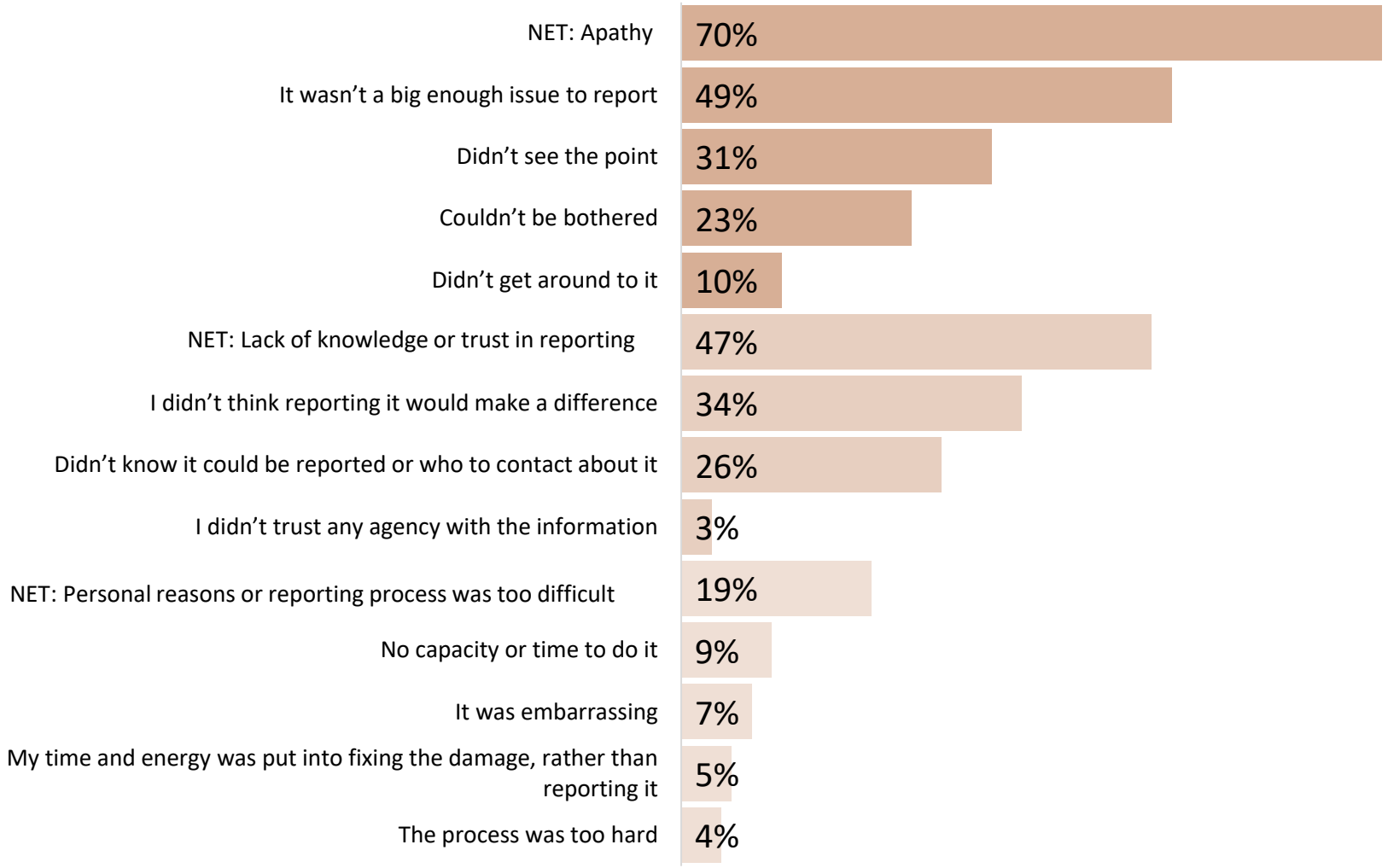


CYBER_ACTIONS: Regarding the cyber threats, online security attacks and crimes you experienced, in what way were you affected?
Source: Number of incidents reported to NCSC sourced from NCSC’s Q3 report.
Base: People who experienced a cyber threat 2024 n=523.

Apathy is a key reason for not reporting

18-34s tend to say that they couldn't be bothered (35%) more than 35-54 (23%) and 55+ year olds (15%).

Reasons for not reporting cyber threats experienced



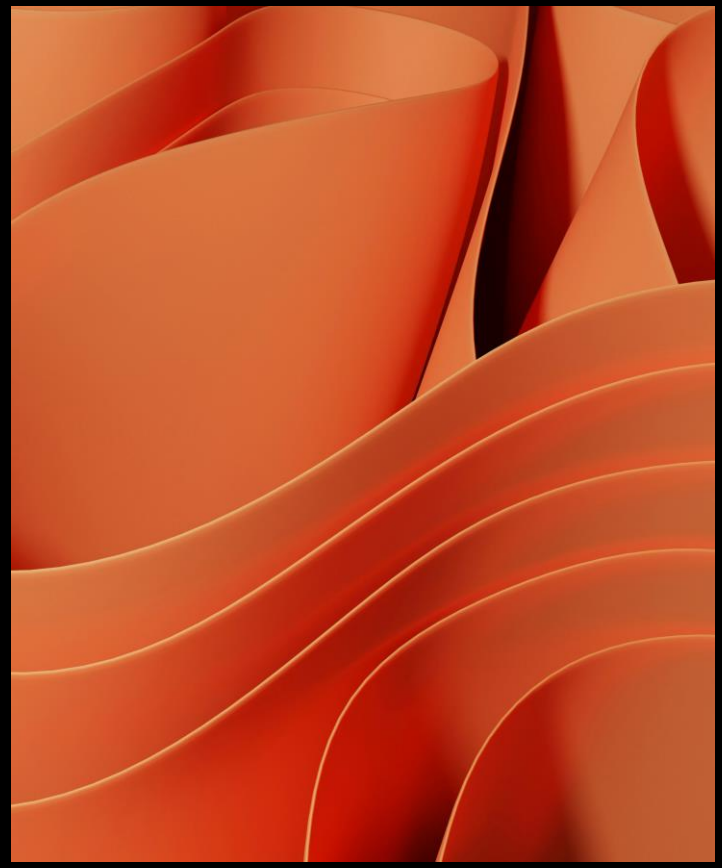
NO_REPORT: You said that you have experienced at least one type of cyber threat, attack or crime but did not report it. Which of the following reasons best describes why it wasn't reported?
Base: People who didn't report a cyber threat 2024 n=232; 18-34s n=59; 35-54s n=87; 55+ n=85.

TRA // National Cyber Security Centre

Implication

Growing confidence around cyber security isn’t yet translating to less harm, or the reporting of cyber attacks

- Severe harm is experienced when people are financially exploited. This is also causing significant damage in other areas.
- As cyber attacks become more complex, the knowledge required to identify and deal with them appropriately is also growing.

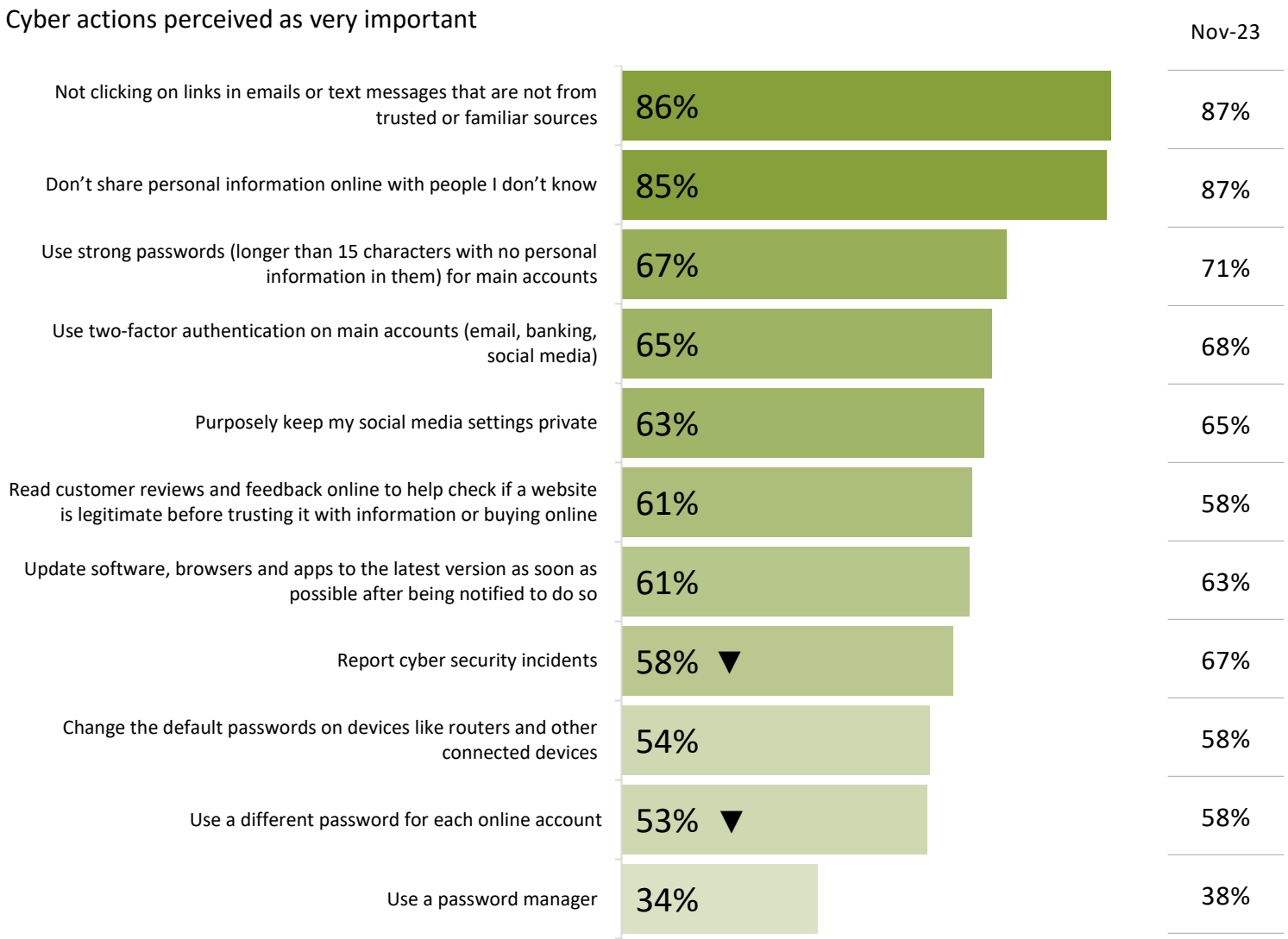


Cyber security attitudes & behaviours

3

The majority of New Zealanders see cyber security actions as very important

Females and 55+ year olds think these actions are more important, compared to other demographic groups.



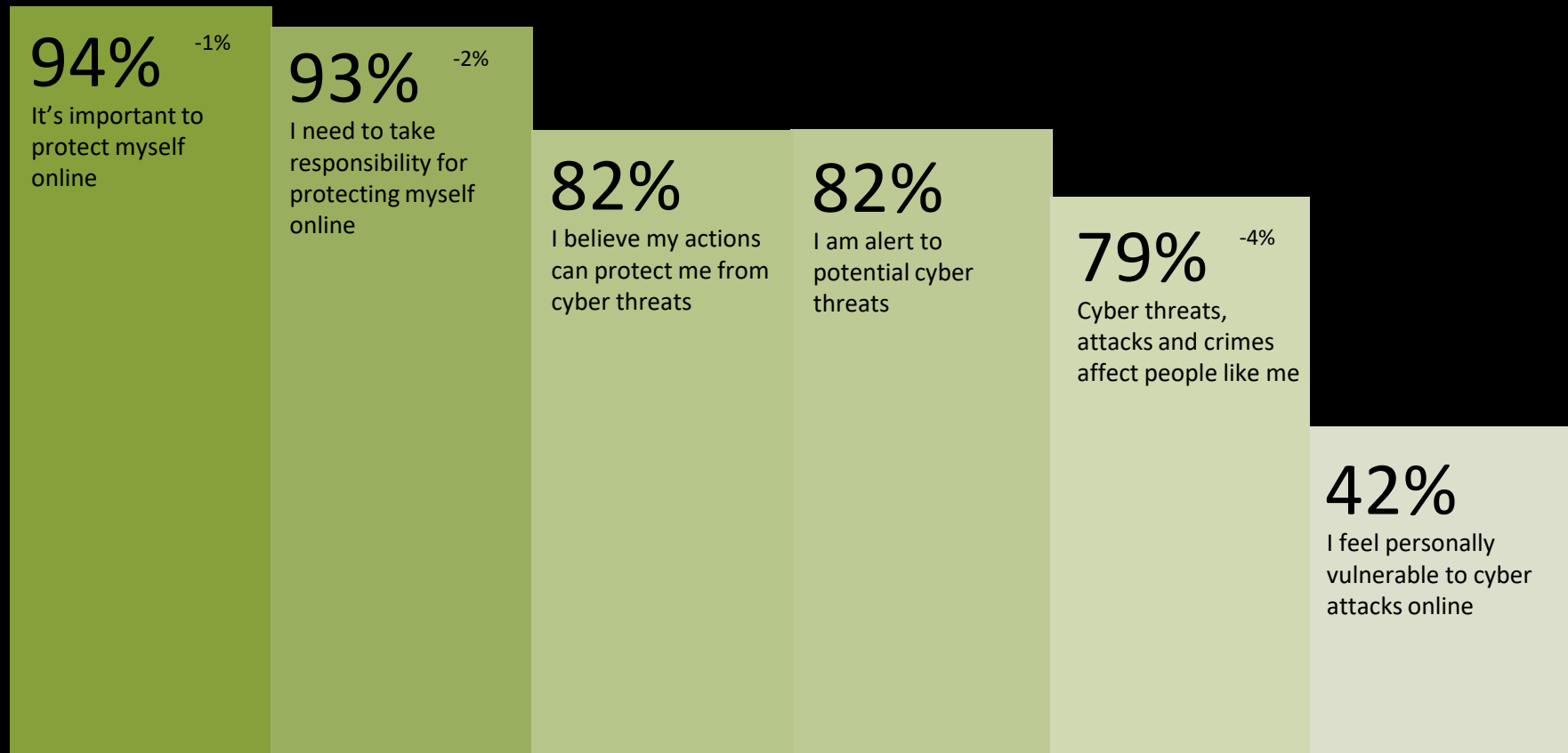
CYBER_IMPORTANCE: There are a number of security steps people can put in place to keep themselves more secure online. From this list can you please tell us how important you believe these are?
Base: Total sample 2023 n=1,023; 2024 n=1,006.

▲▼ Significantly higher/lower than previous year

There are strong personal beliefs (or norms) that New Zealanders hold around cyber security

Most people recognise the importance of cyber security behaviours, though they don't personally feel vulnerable.

Cyber security beliefs – Personal vs 2023



BELIEFS: Please look at the following statements and indicate how strongly you agree or disagree with each of these.
Note: Statements without a percentage change were added in 2024.
Base: Total sample 2023 n=1,023; 2024 n=1,006.

TRA // National Cyber Security Centre

However, there are much weaker norms around what others are doing. These are known as “socially observable norms.”

Socially observable norms are weaker amongst 55+ year olds.

Cyber security beliefs – Social
vs 2023

68% **-1%**

New Zealanders are concerned with the number of people impacted by cyber attacks

61% **-2%**

New Zealanders think that the actions they take can prevent cyber attacks and crimes

36% **-2%**

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.
Base: Total sample 2023 n=1,023; 2024 n=1,006.

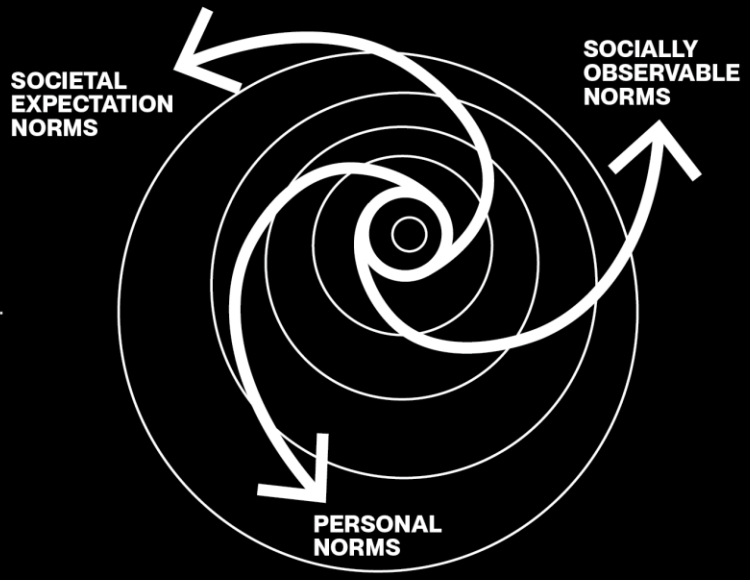
If there's dissonance between personal and socially observable norms, action is less likely to be taken

TRA's Norm Storming framework illustrates this dynamic.
To harness the power of the normative framework, we
need a system that is in balance.

Norm Storming framework

Our herding instinct, coming from unconsciously or consciously observing what others are doing (sometimes described as descriptive norms).

Most people seem to be doing...
I'd feel like the odd one out...



The way people are expected to behave, following customary etiquette and what society or social groups expect of us (sometiems described as injunctive norms).

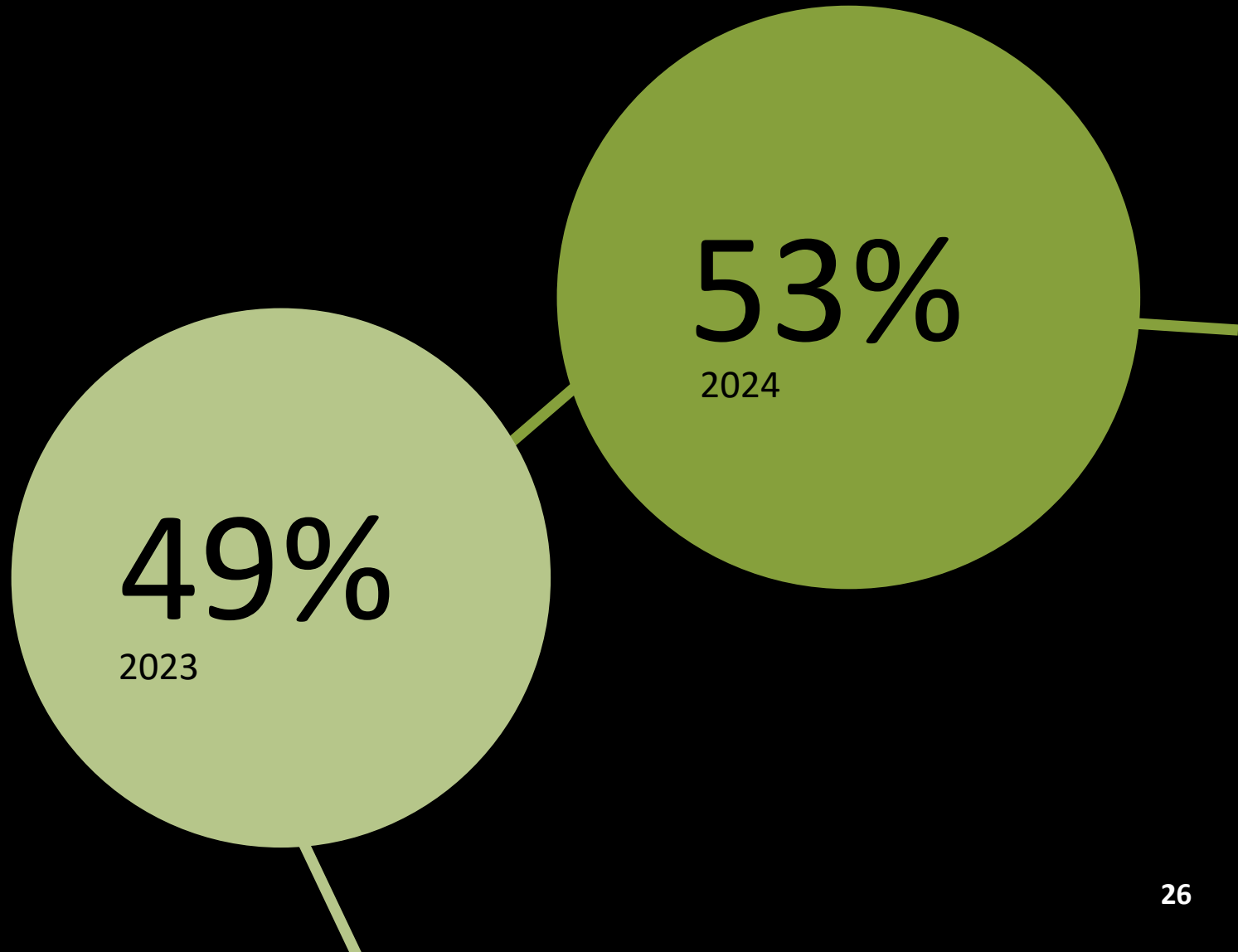
The way we do things around here...
The law of the land...

Our moral compass, obeying our personal beliefs and the expectations we hold for ourselves.

I think it's OK to...
I don't like the idea of...

There has been some progress made with people's cyber security behaviours

% who engaged in new cyber security behaviours in last 6 months



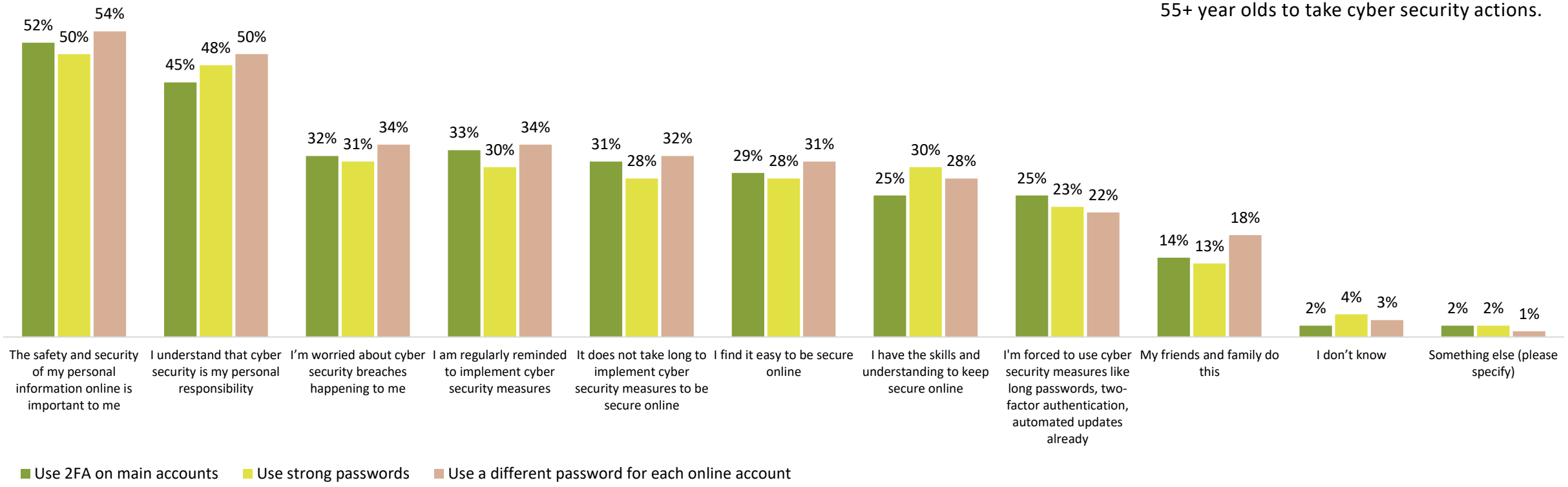
▲▼ Significantly higher/lower than previous year

NEW_BEHAV: In the past six months, have you taken any new actions to keep yourself more secure online?
Base: Total sample 2023 n=1,023; 2024 n=1,006.

And safety and security of personal information are the key motivators of those doing so

Motivations in taking cyber security actions

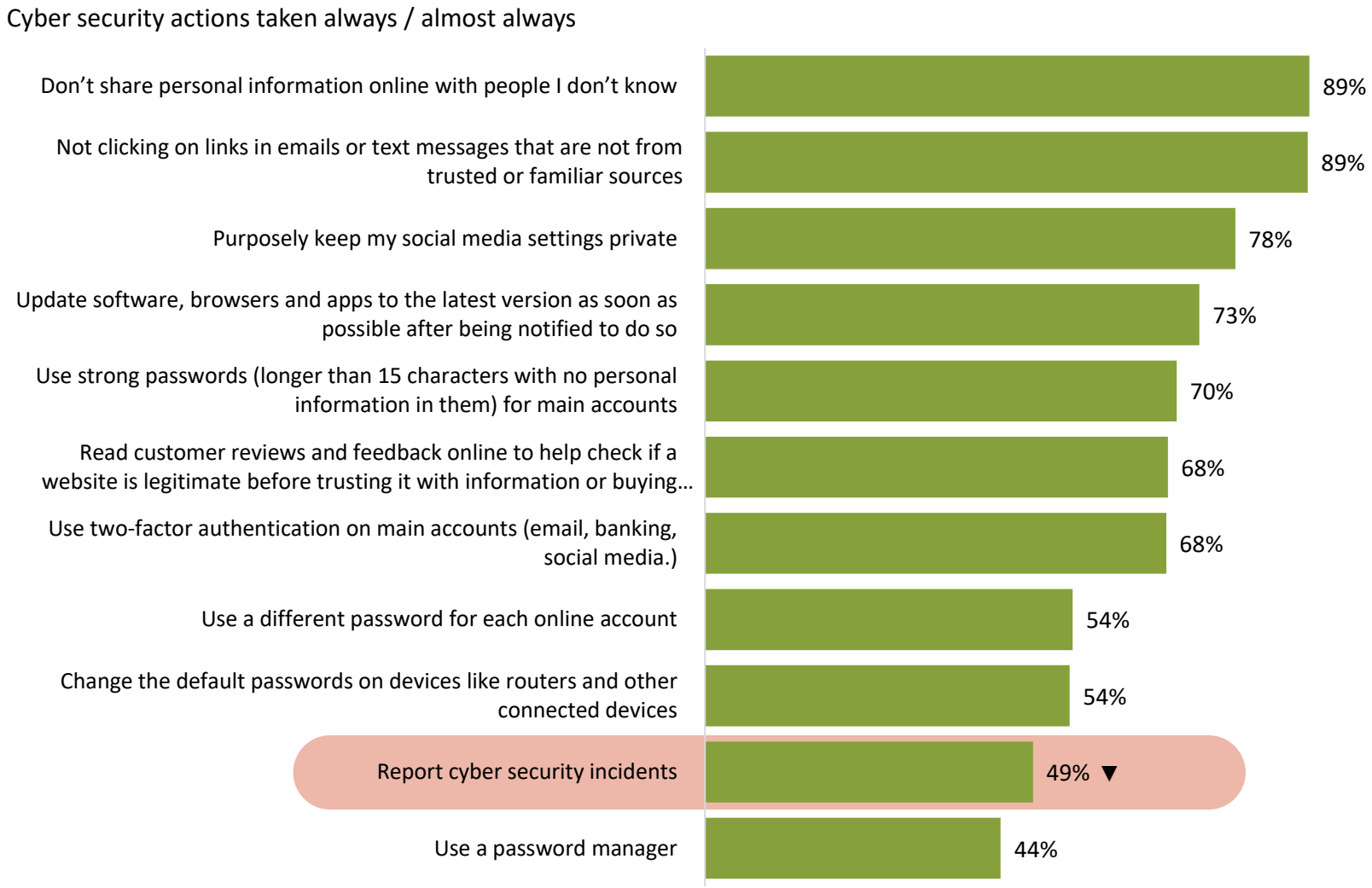
The safety and secutiry of personal information online is a bigger motivator for 55+ year olds to take cyber security actions.



WHY_MOTIVATORS: For behaviours above where you answered always or almost always, please tell us what motivated you into doing that action.
Base: Key actions taken always / almost always, use 2FA on main accounts 2024 n=687; use strong passwords 2024 n=705; use a different password 2024 n=552.

While the gains of last year have been maintained for most actions, again there's been a decrease in reporting cyber security incidents

All other actions grew significantly last year and have held steady this year.

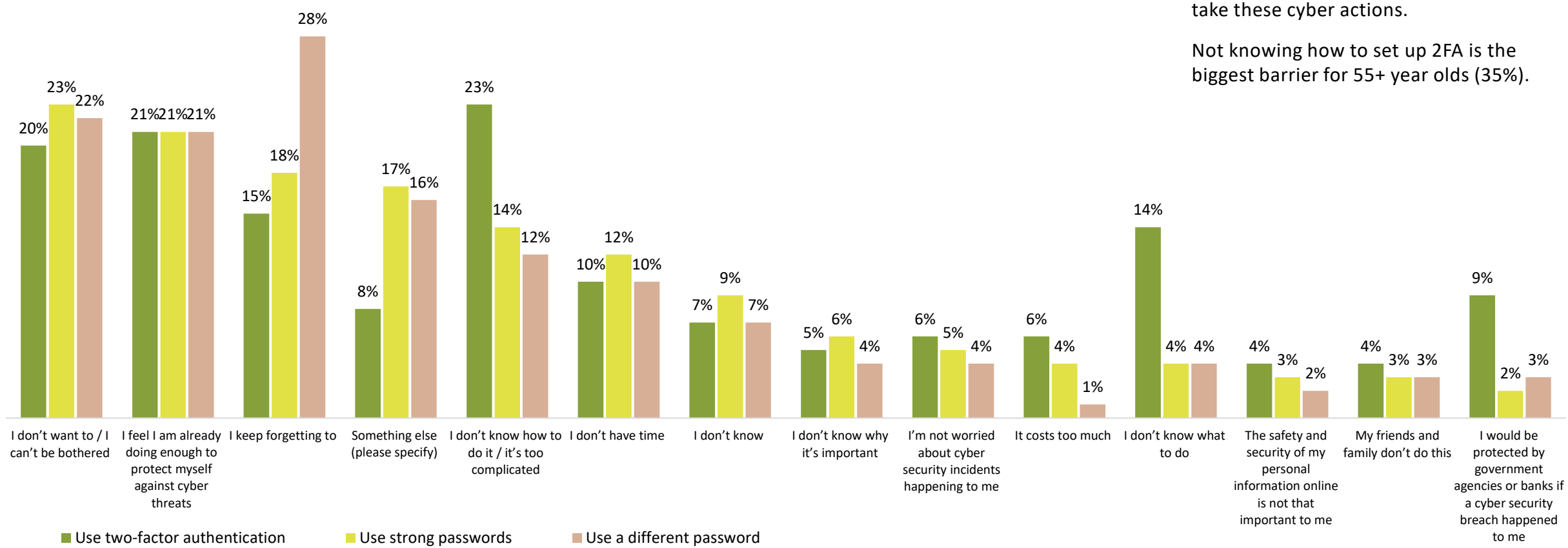


CYBER_ACTIONS2: From this list of security steps, can you please tell us how often you currently do them?
Base: Total sample 2022 n=1,051; 2023 n=1,023; 2024 n=1,006.

▲▼ Significantly higher/lower than previous year

This again shows up in an apathy towards taking action

Barriers to taking cyber security actions (2024)



18-34 year olds are more likely than other age groups to say they don't have time to take these cyber actions.

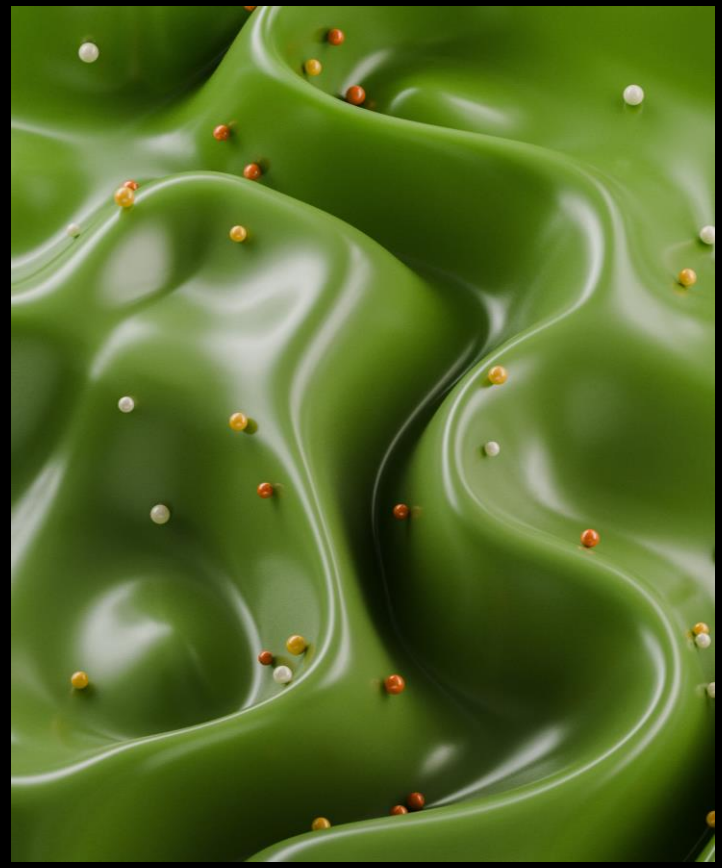
Not knowing how to set up 2FA is the biggest barrier for 55+ year olds (35%).

WHY_BARRIERS: For behaviours above where you answered sometimes, rarely, or never, please tell us what is stopping you from doing that action.
Base: Key actions taken sometimes / rarely / never, use 2FA on main accounts 2024 n=296; use strong passwords 2024 n=299; use a different password 2024 n=451.

Implication

Progress is being made but weak socially observable norms are inhibiting more widespread action

- If people don’t see or believe that others are taking key actions like 2FA, as well as unique, long and strong passwords; and reporting incidents, they are less likely to take those actions themselves consistently.
- It’s like a reverse social pressure.
- This is impacting wider public vulnerability.



Appendix

Online threats

The following wording was displayed to respondents.

Online shopping scams – Buying something from a website and not receiving it or receiving a lesser item

Lottery and prize scams – Receiving emails about a fake lottery, prize, or grants

Investment scams – Offer to participate in an investment opportunity that doesn't exist, including fake cryptocurrency exchanges

Job offer scam – Offer of employment where scammers ask for money and/or information to secure a role

Gift card scam – Receiving an email asking to buy gift cards (like iTunes, Amazon, Steam etc.) on behalf of someone else

Unauthorised transfer – Credit cards and/or bank accounts being used without people's knowledge

Unauthorised access – Email, social media, phone or other online accounts being used or accessed without account holder's knowledge

Scam calls – Someone pretending to be a technical assistant from a legitimate organisation such as a bank, trying to get access to a computer

Romance scams – Where a fake online identity attempts a romantic relationship with someone and persuade them to give or invest money

Online identify theft – Someone accessing personal information and using it for identity fraud

Data breach – Personal and/or financial data being stolen

Malware or ransomware – Downloading malicious software accidently

Phishing – Receiving a text message or email from someone pretending to be a trusted person or organisation asking to click on a link or open a document

Email extortion or blackmail scams – Receiving a message claiming to have private information and threatening to release it if money isn't paid

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?