Cyber Security Consumer Behaviour Tracker 2026

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 been conducted every year since 2022. Comparisons to results of previous years are included where applicable.

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.

National Cyber Security Centre

TRA

What we did

A quantitative tracking survey

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

Fieldwork ran from 20th November – 30th November 2025.

The survey interviewed a nationally representative sample of n=1,011 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%.

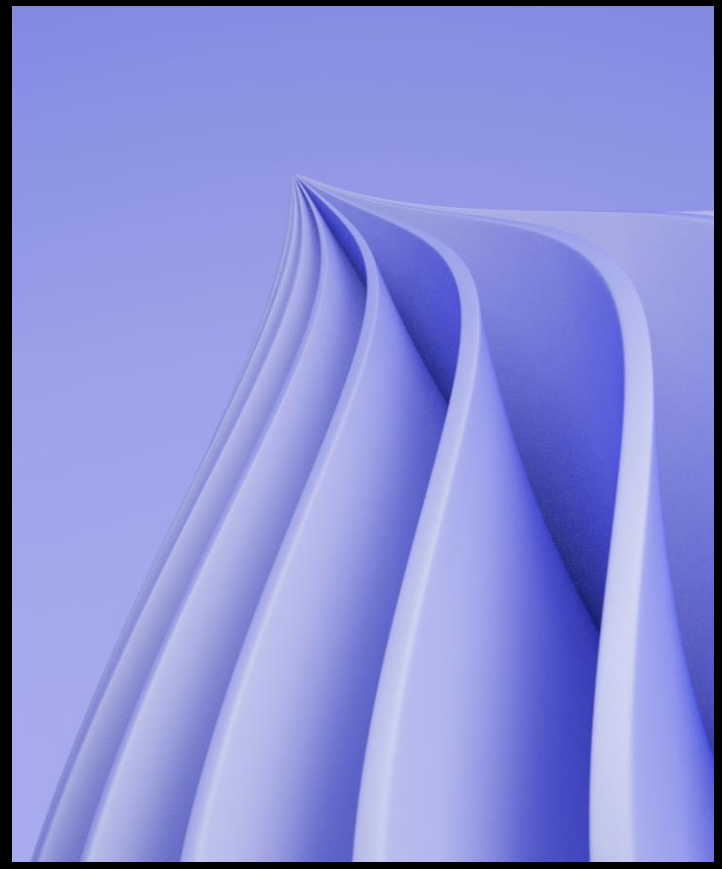
Contents

Story in a nutshell

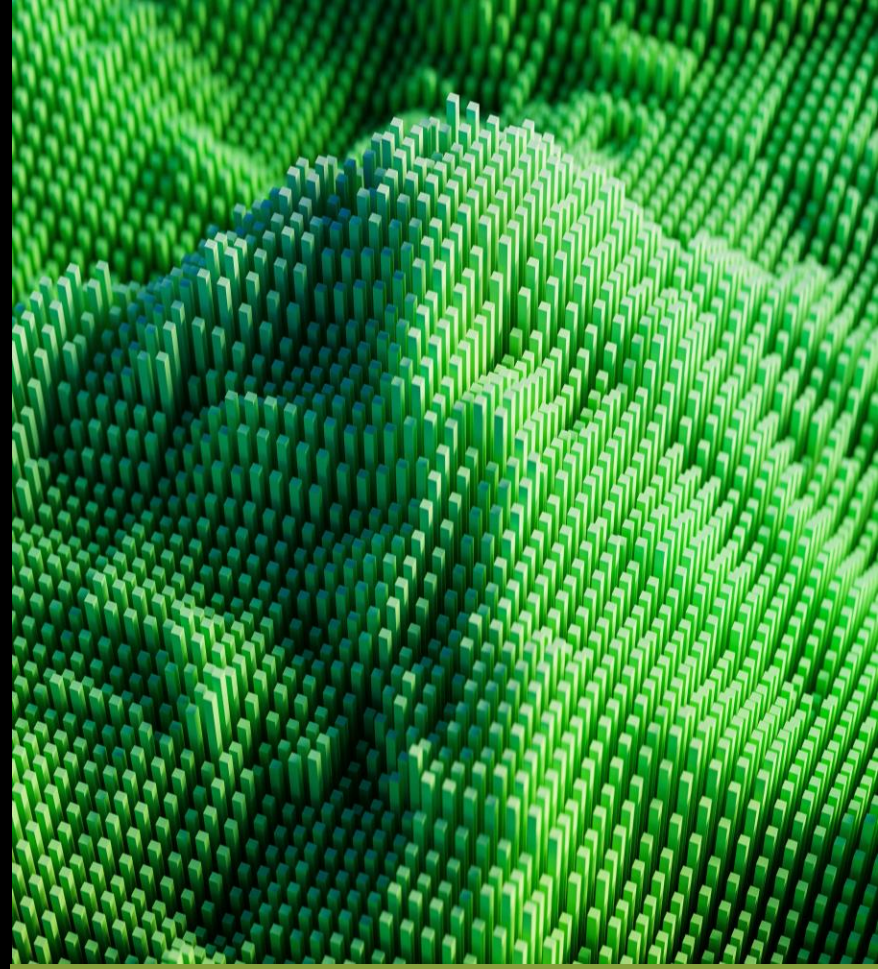
Cyber security continues to be prevalent in national conversations.

Awareness of threats remains high. Exposure to threats is broadly similar year on year, with some reduced impact, and we're seeing encouraging movement in some preventative actions.

However, there continues to be a significant impact on New Zealanders, and barriers such as low levels of perceived vulnerability and low motivation remain in place.



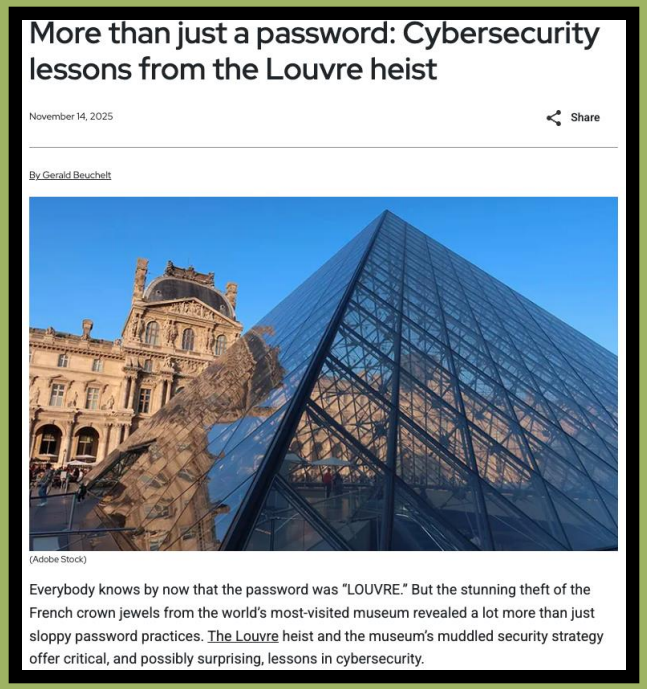
The current landscape



1

Cyber security has remained prominent in the national discourse

2025 has seen prominent cyber security campaigns across multiple banks, and numerous stories in the news about high profile breaches.



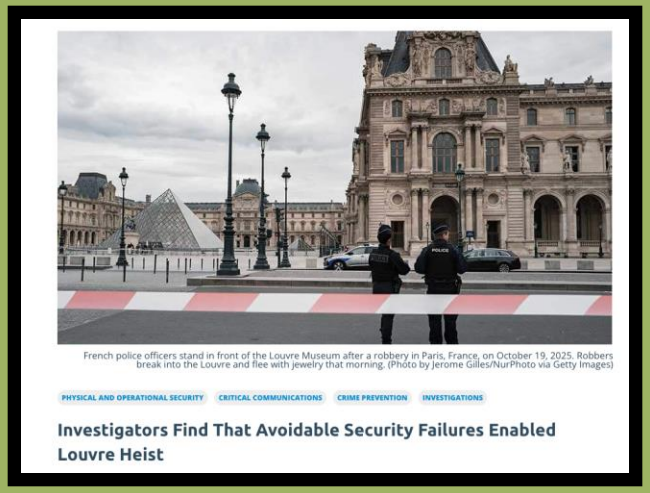
More than just a password: Cybersecurity lessons from the Louvre heist

November 14, 2025 Share

By Gerald Beuchelt

(Adobe Stock)

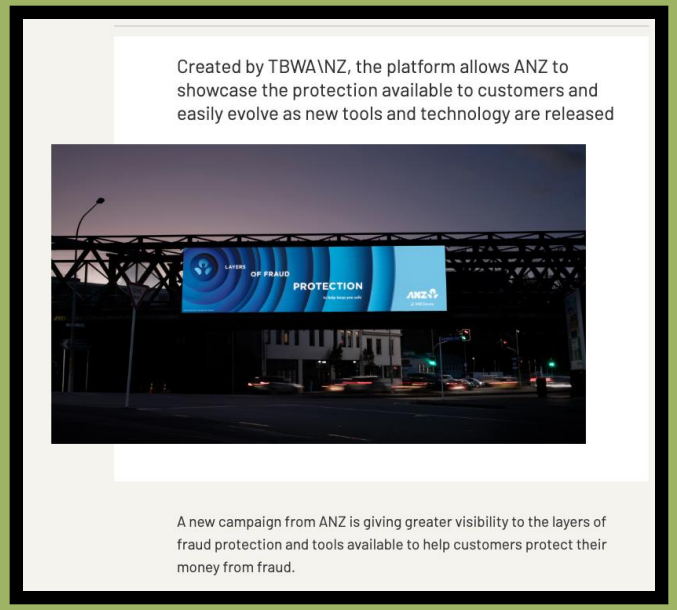
Everybody knows by now that the password was "LOUVRE." But the stunning theft of the French crown jewels from the world's most-visited museum revealed a lot more than just sloppy password practices. The Louvre heist and the museum's muddled security strategy offer critical, and possibly surprising, lessons in cybersecurity.



French police officers stand in front of the Louvre Museum after a robbery in Paris, France, on October 19, 2025. Robbers break into the Louvre and flee with jewelry that morning. (Photo by Jerome Gilles/NurPhoto via Getty Images)

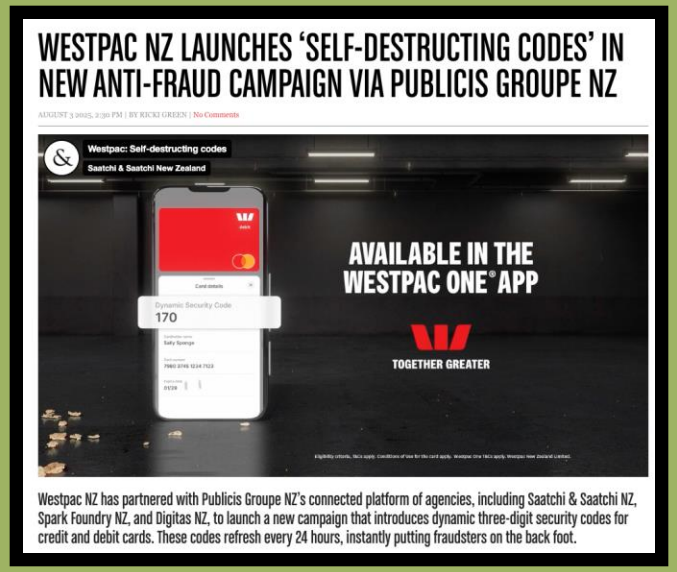
PHYSICAL AND OPERATIONAL SECURITY CRITICAL COMMUNICATIONS CRIME PREVENTION INVESTIGATIONS

Investigators Find That Avoidable Security Failures Enabled Louvre Heist



Created by TBWA\NZ, the platform allows ANZ to showcase the protection available to customers and easily evolve as new tools and technology are released

A new campaign from ANZ is giving greater visibility to the layers of fraud protection and tools available to help customers protect their money from fraud.



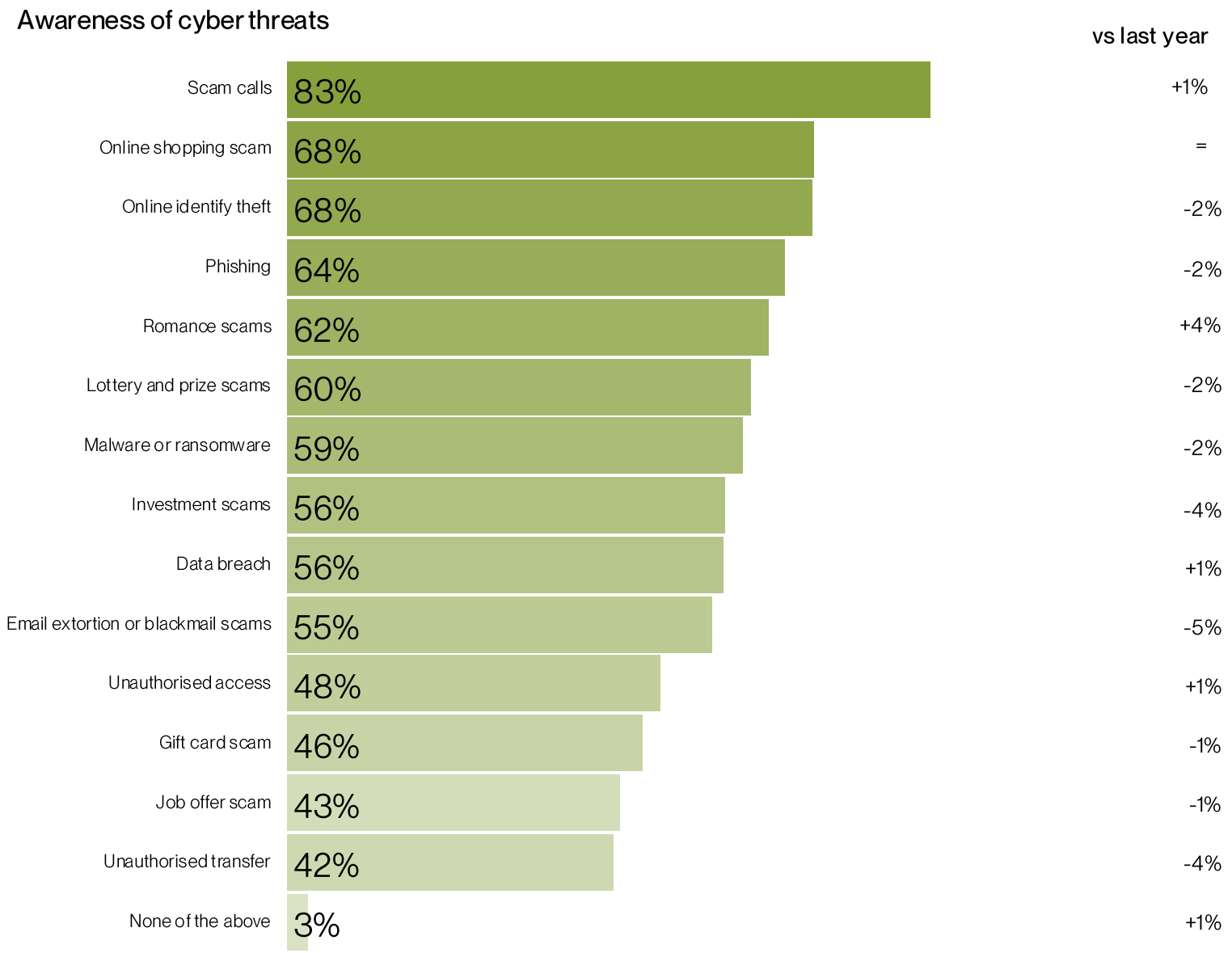
WESTPAC NZ LAUNCHES 'SELF-DESTRUCTING CODES' IN NEW ANTI-FRAUD CAMPAIGN VIA PUBLICIS GROUPE NZ

AUGUST 3 2025, 2:30 PM | BY KICKI GREEN | No Comments

Westpac NZ has partnered with Publicis Groupe NZ's connected platform of agencies, including Saatchi & Saatchi NZ, Spark Foundry NZ, and Digitas NZ, to launch a new campaign that introduces dynamic three-digit security codes for credit and debit cards. These codes refresh every 24 hours, instantly putting fraudsters on the back foot.

Awareness of common cyber threats remains high among the general population

With no significant increases or decreases, the average number of scams and threats people are aware of remains at a similar level to last year.



CYBER_AWARE. From this list of cyber threats, cybercrime and online security, can you please tell us which (if any) you are aware of?
Base: Total 2024 n=1006, Total n 2025=1011

Awareness of scams by age group shows demonstrates that older participants are significantly more likely to be aware of many scams

Which of the following scams are you aware of?

	18 - 24 years	25 - 29 years	30 - 34 years	35 - 39 years	40 - 44 years	45 - 49 years	50 - 54 years	55 - 59 years	60 - 64 years	65 - 69 years	70 - 74 years	75 years and over
Scam calls	72%▼	88%	84%	80%	76%	78%	86%	85%	92%▲	87%	90%▲	85%
Online shopping scam	59%	64%	67%	59%	57%▼	71%	71%	74%	78%▲	77%▲	77%	70%
Online identify theft	58%	66%	68%	55%▼	62%	67%	76%	77%	79%▲	81%▲	75%	62%
Phishing	48%▼	49%▼	64%	48%▼	59%	74%▲	69%	76%	81%▲	68%	75%▲	70%
Romance scams	40%▼	58%	60%	50%▼	57%	66%	70%	80%	76%▲	76%▲	80%▲	55%
Lottery and prize scams	53%	60%	60%	56%	55%	62%	65%	67%	75%▲	62%	61%	48%▼
Malware or ransomware	47%▼	50%	57%	50%	56%	59%	68%	64%	65%	65%	75%▲	61%
Investment scams	44%▼	59%	50%	44%▼	51%	46%	66%▲	61%	73%▲	69%▲	71%▲	59%
Data breach	46%	58%	58%	45%▼	52%	54%	63%	69%▲	72%▲	66%	56%	43%▼
Email extortion or blackmail scams	40%▼	58%	62%	44%▼	51%	57%	60%	73%▲	63%	60%	56%	43%▼
Unauthorised access	33%▼	47%	50%	40%	43%	43%	52%	62%▲	61%▲	58%	64%▲	42%
Gift card scam	42%	59%▲	53%	40%	42%	52%	46%	37%	52%	52%	46%	34%▼
Unauthorised transfer	35%	40%	39%	29%▼	37%	47%	45%	55%	49%	55%▲	47%	38%
Job offer scam	52%	58%▲	47%	40%	39%	40%	46%	42%	44%	44%	39%	22%▼

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?
AGE_GPS: How old are you?

TRA NCSC

Base = Total n=1011 18-24 years n=65, 25-29 years n=75, 30-34 years n=134, 35-39 years n=82, 40-44 years n=96, 45-49 years n=75, 50-54 years n=89, 60-64 years n=76, 65-69 years n=81, 70-74 years n=70, 75 years and over n=98

▲▼ Significantly higher/lower than other groups

Experience of cyber issues also remains consistent

We have seen no significant change overall in the number of New Zealanders who have experienced an issue in the last 6 months.

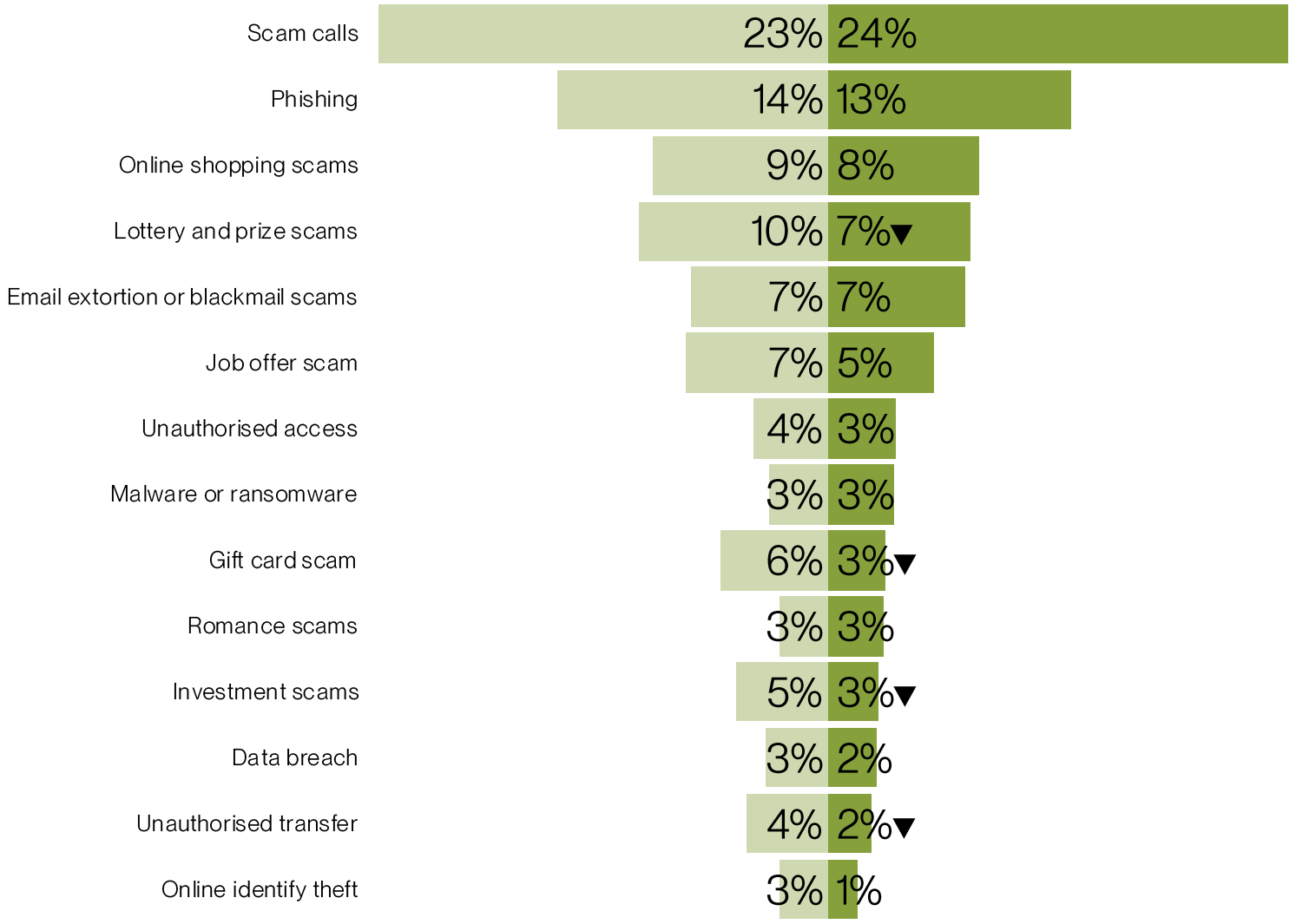
48%

Experienced a threat
- 4% since 2024

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 2024 n=1006, Total n 2025=1011

TRA NCSC

Personal experience of cyber threats



▲▼Significantly higher/lower than 2024

The severity of impact and specific types of harm experienced have softened

The proportion of New Zealanders who experienced a detrimental impact from a cyber threat in the last 6 months decreased from 36% to 27%. Specifically, fewer lost time or money, or experienced stress.

Severity of harm caused by exposure to cyber threat

	Dec-24	Nov-25
No Impact	22%▼	25%
Minor	18%	13%▼
Moderate	12%	9%▼
Significant	10%	7%▼
Severe	5%	4%
NET: Experienced a threat	52%	48%
NET: Experienced any impact (minor to severe)	36%	27%▼

Type of harm caused by exposure to cyber threat

	Dec-24	Nov-25
It took up my time	23%	18%▼
It was stressful	17%	14%▼
It was embarrassing	11%	9%
I lost money or had to pay money	10%	6%▼
It impacted my mental wellbeing	10%	9%
I lost personal information or data	7%	5%
It damaged my device/s	4%	3%
It impacted relationships with friends or family	4%	3%

▲▼ Significantly higher/lower than previous wave

*Note: Percentages do not tally because people may have answered for multiple threats experienced

TRA NCSC

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?
CYBER_HARM: Regarding cyber threats, online security attacks and crimes you experienced, in what way were you affected?
Total 2024 n=1006, Total n 2025=1011

However a large proportion of New Zealanders continue to be impacted

Harm may be softening
- but crucially, it hasn't gone away.

Half

Of the population still experienced a cyber threat in the last six months

1 in 5

Of those exposed to a threat experienced a severe or significant detrimental impact

1 in 5

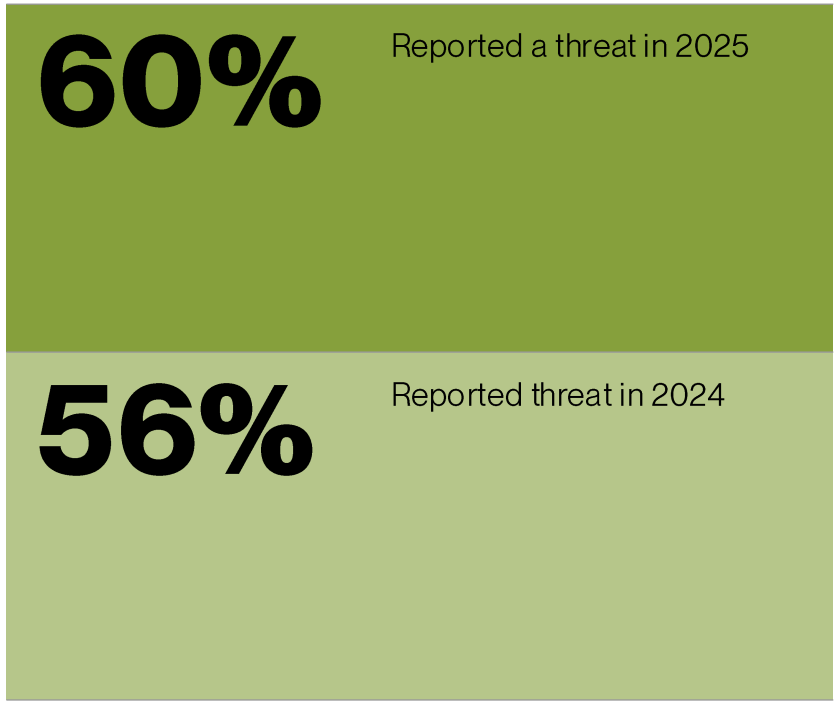
Of those who experienced a detrimental impact (from minor to severe) suffered financial loss

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?
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?
CYBER_HARM: Regarding cyber threats, online security attacks and crimes you experienced, in what way were you affected?
Base: Those who experienced threat 2025 n=277

Many New Zealanders still don't report the threats they experience

We have not seen any significant changes year on year, however those over the age of 55 were significantly more likely not to report a threat.

Proportion reporting cyber threats



Proportion not reporting cyber threats by age

	18 - 34 years	35 - 54 years	55 + years
Didn't report the threat they experienced	32%▼	38%	47%▲

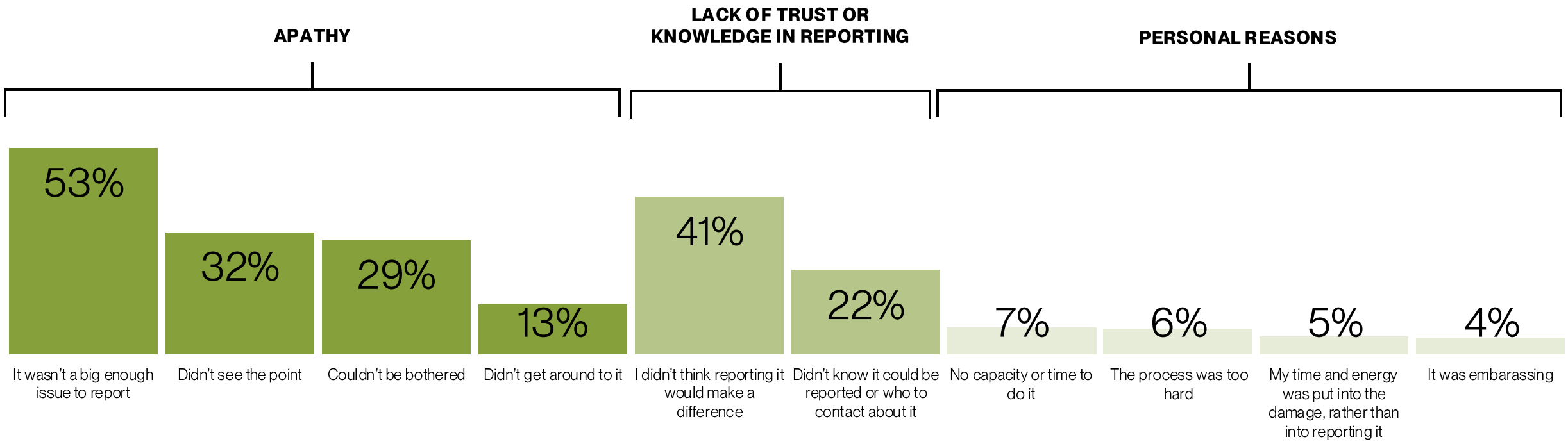
CYBER_ACTIONS: Regarding the cyber threats, online security attacks and crimes you experienced, can you please tell us which actions you took as a direct result?
Base: Those who have experienced at least one threat 2025 n=484, 2024 n=523
Base: Didn't report the threat they experienced 18-34 n=130, 35-54 n=154, 55 years or more n=200

▲▼ Significantly higher/lower than other groups

Among those who didn't report threats apathy was a key barrier

We have not seen any significant changes year on year, suggesting the barriers to reporting threats are consistent

Reason for not reporting cyber threat



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: Those who didn't report threat n=197

Implication

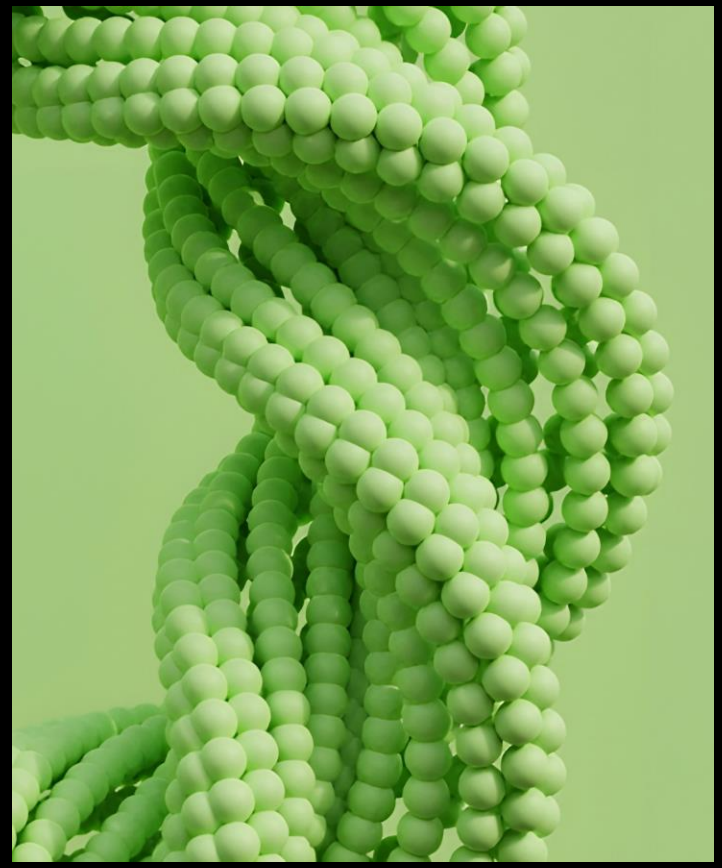
Harm is softening – but exposure to threats remains high and many don't report threats

Positively, in the current environment, exposure to cyber threats and the harm experienced from them isn't getting worse.

However, It remains a significant issue for the many New Zealanders who are continuing to be exposed.

When people experience these threats, a significant number are still not taking any action in response. And there are a range of reasons for their inaction.

- How can we further understand dynamics influencing cyber security, to inform how we drive changes in the behaviour of New Zealanders?



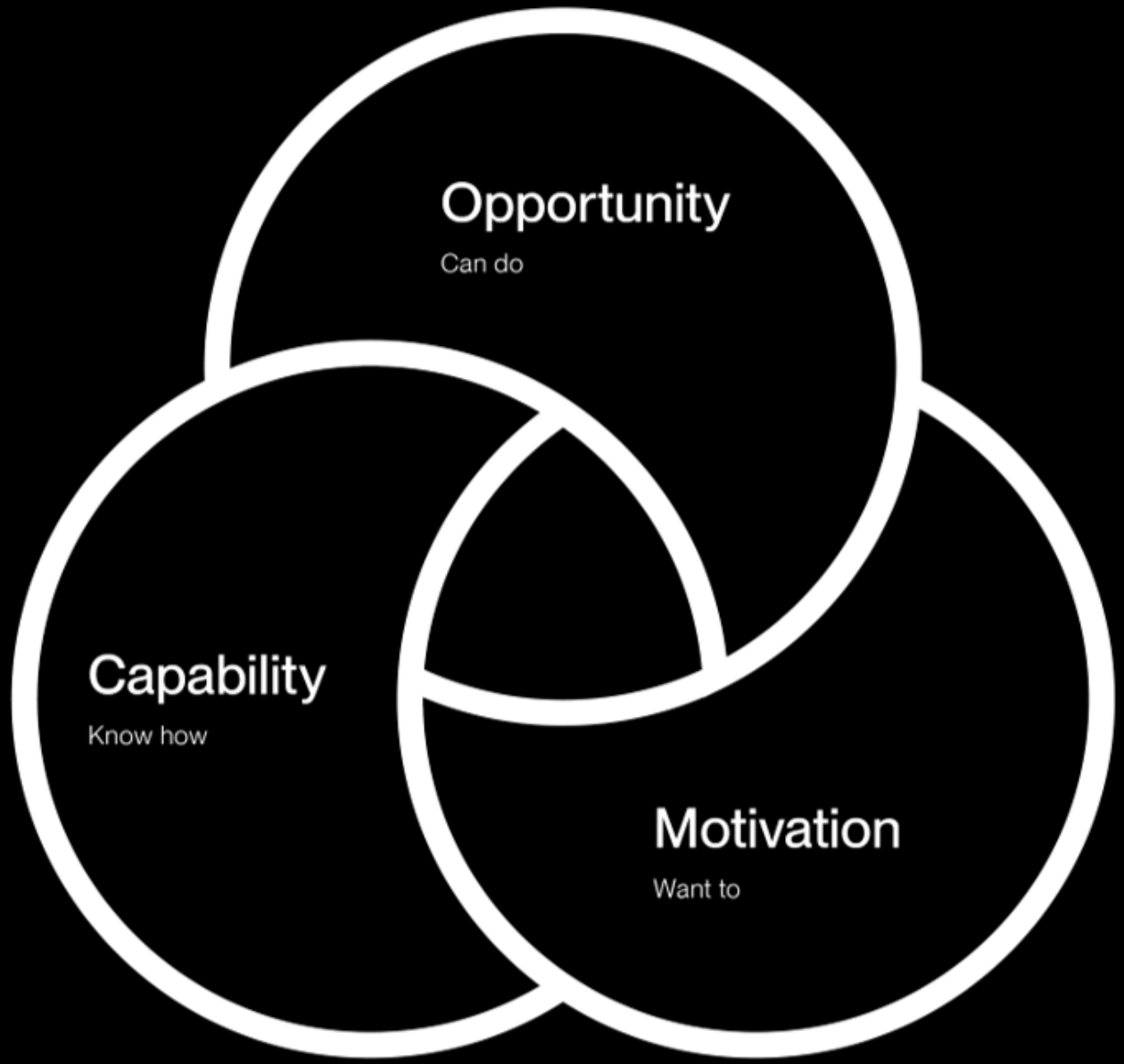
The COM-B framework tells us how we can create lasting behavioural change

The core facets of this are:

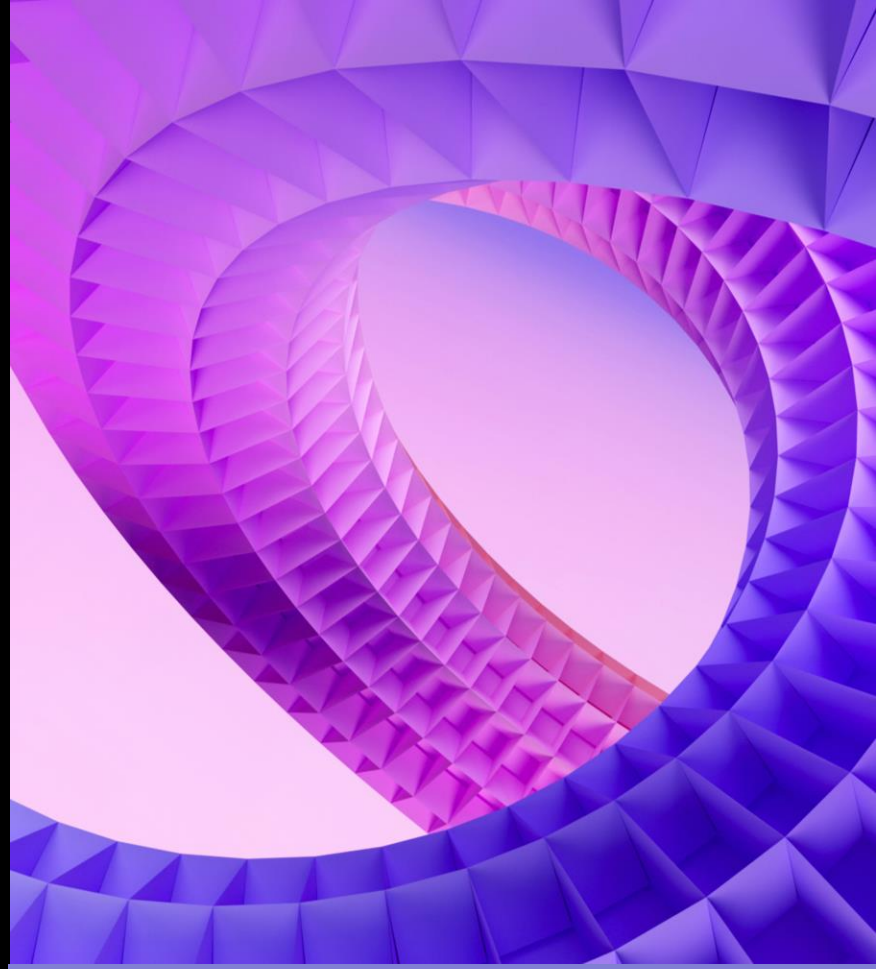
1. Psychological **Capability** – Do people know how to do the behaviour?
2. Environmental **Opportunity** – Can people do the behaviour in their current environment and context?
3. Automatic **Motivation** – Do people want to do the behaviour, instinctually and in the moment?

This means that people need to understand cyber security threats, have the ability to implement safety behaviours, and be motivated to do so.

Let's look at some of the preventative cyber security behaviours that New Zealanders are taking, and the facets that are either enabling or inhibiting these.



Preventative Behaviours



2

We've seen significant shifts in the uptake of some NCSC priority actions

This year has seen a significant increases in the proportion 'always' using two-factor authentication and password managers.

Preventative actions taken 'always'

	Dec-24	Nov-25
Don't share personal information online with people I don't know	69%	70%
Not clicking on links in emails or text messages that are not from trusted or familiar sources	66%	66%
Purposely keep my social media settings private	54%	56%
Update software, browsers and apps to the latest version as soon as possible after being notified to do so	45%	43%
Use strong passwords (longer than 15 characters with no personal information in them) for main accounts	40%	41%
Read customer reviews and feedback online to help check if a website is legitimate before trusting it with information or buying online	39%	41%
Use two-factor authentication on main accounts (email, banking, social media.)	38%	43%▲
Change the default passwords on devices like routers and other connected devices	30%	34%
Report cyber security incidents	29%▼	29%
Use a different password for each online account	29%	32%
Use a password manager	24%	32%▲
Use Passkeys (a unique, encrypted login key unlocked with your device's security login)	-	31%

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 :' Always'
Base: Total 2024 n=1006, Total n 2025=1011

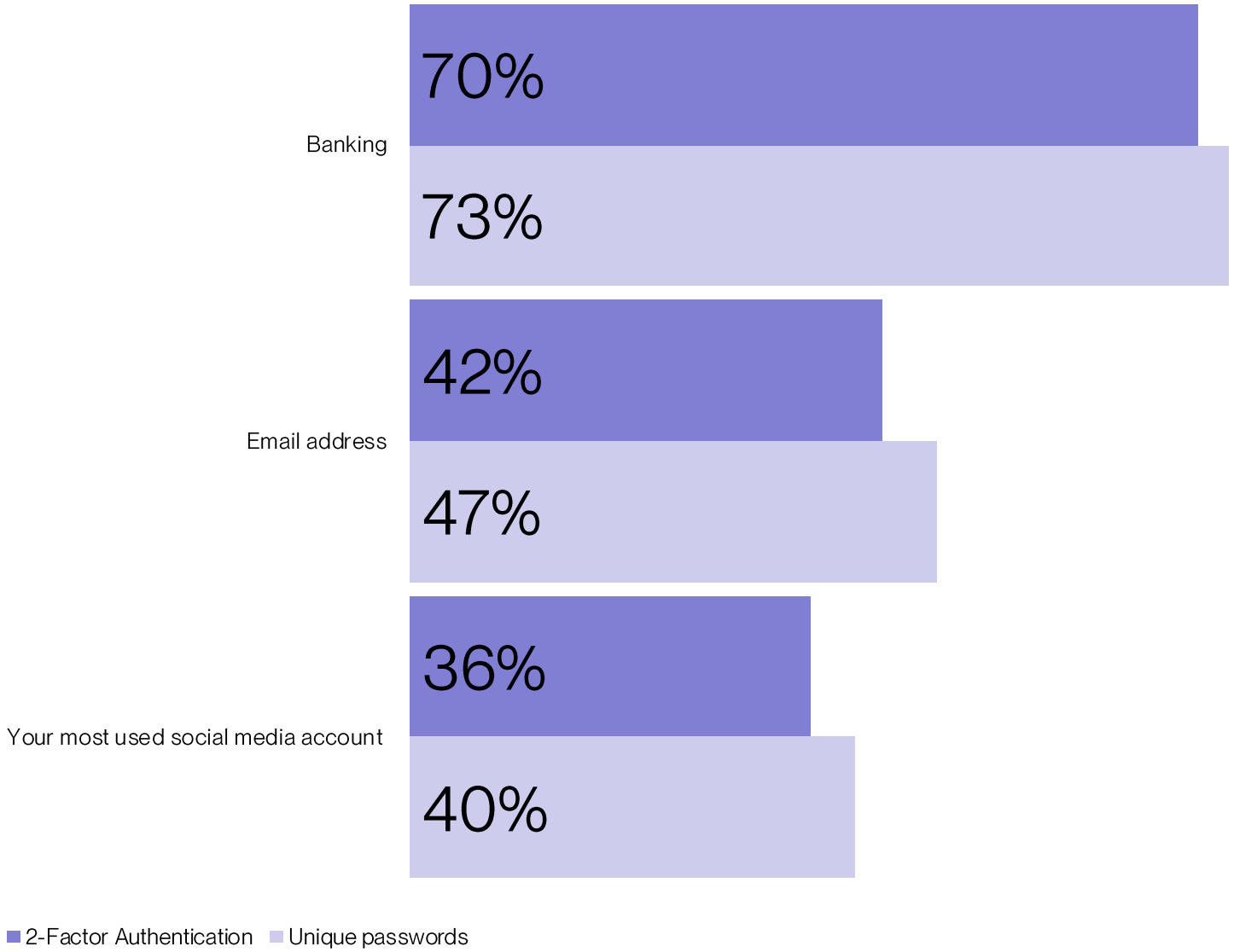
▲▼ Significantly higher/lower than previous wave

People exercise the safest behaviours with their finances

Two-factor authentication and unique passwords were most commonly used on banking accounts, ahead of email and then social media accounts.

ENABLED_2X- Do you have Two-Factor Authentication enabled on any of the following accounts?
UNIQUE_X- On which of the following accounts do you use a unique password, that you don't reuse elsewhere?
Base: Those who report to use two factor authentication n=967, Those who report to use strong passwords n=987

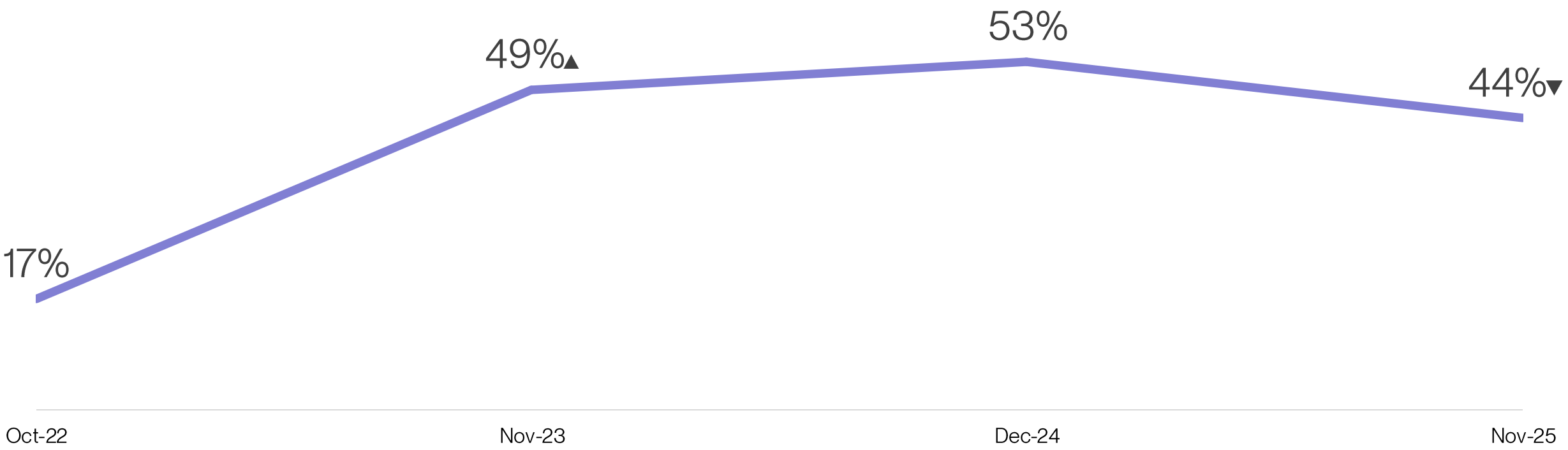
Two-factor authentication & unique passwords usage on:



New actions are less frequent as behaviours begin to embed

This year has seen a significant decrease in the proportion of people taking up new online security behaviours.

Started a new cyber security behaviour in the last six months



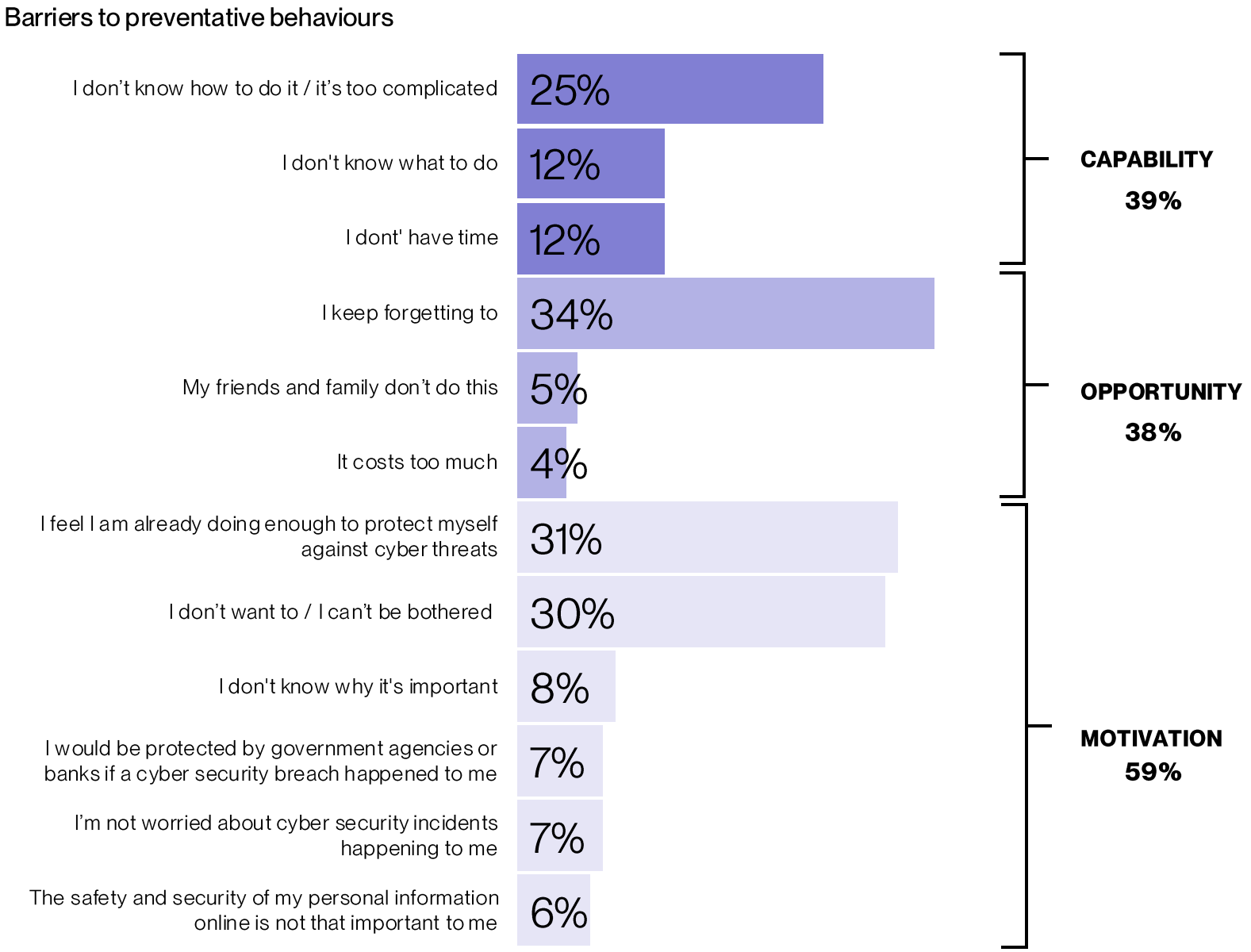
NEW_BEHAV: In the past six months, have you started to use any new online security behaviours that you were not carrying out previously?
Base: Total 2024 n=1006, Total n 2025=1011

▲▼ Significantly higher/lower than previous wave

Sitting under motivation, apathy is starkly evident

Reluctance to do key cyber security actions comes from a feeling of 'I can't be bothered' and 'I am doing enough already'; these areas are key for us to focus on.

WHY_BARRIERS. For behaviours above where you answered sometimes, rarely, or never, please tell us what is stopping you from doing that action. Base: Those who never, rarely or sometimes use two-factor authentication, strong, unique passwords (Nov 25') n=562



Actions are beginning to change – but motivation to act is held back by perceived unimportance

- We are starting to see shifts in behaviour at a total level, but progress is limited by why people do or don't feel motivated to act, rather than their knowledge in how to act.
- COM-B helps pinpoint where behaviour change is stalling: not due to a lack of understanding (Capability) or constraints in daily life (Opportunity), but low Motivation driven by a belief that cyber security is not personally relevant.
- This points towards a need to reinforce messaging that increases personal relevance, highlights real-world consequences, and normalises protective behaviours, more so than adding more instructions, education, or tools.
- To do this effectively, we need to understand the specific beliefs New Zealanders hold about cyber security, and where these beliefs are undermining perceived importance.

So how are the beliefs of New Zealanders evolving?

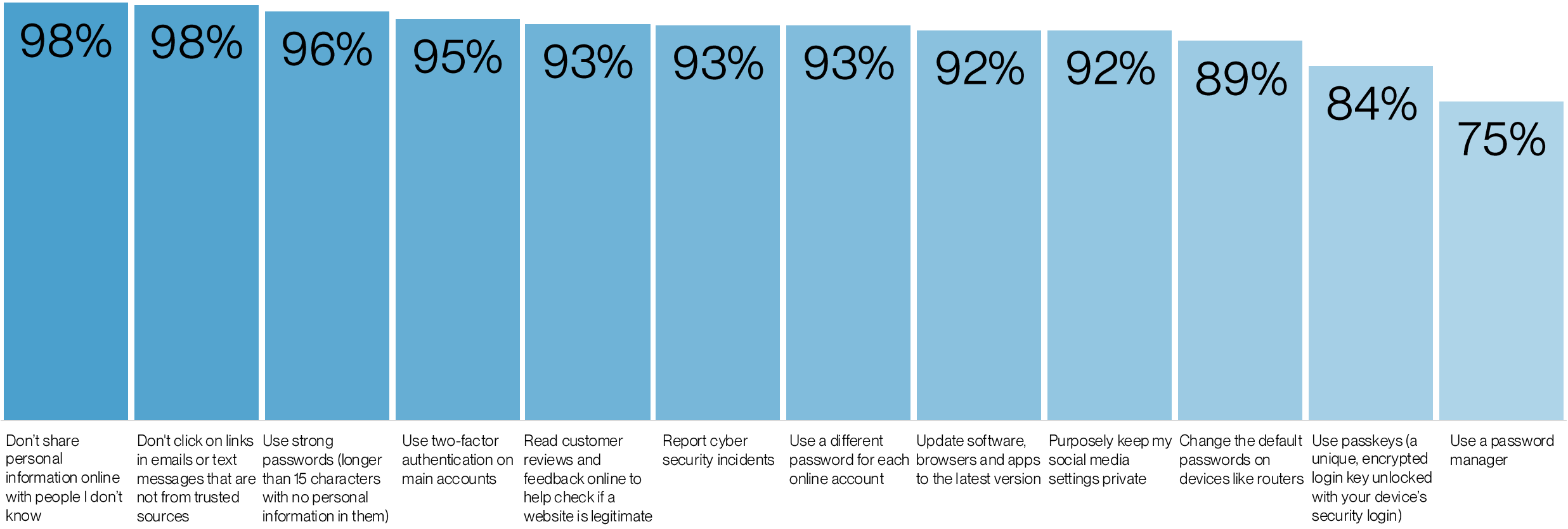
Beliefs of New Zealanders

3

New Zealanders are in agreement on the importance of cyber security

Their attitudes about the importance of cyber security are almost unanimous across actions – and we haven't seen any change in this year on year.

Importance of preventative actions (Very and somewhat important)



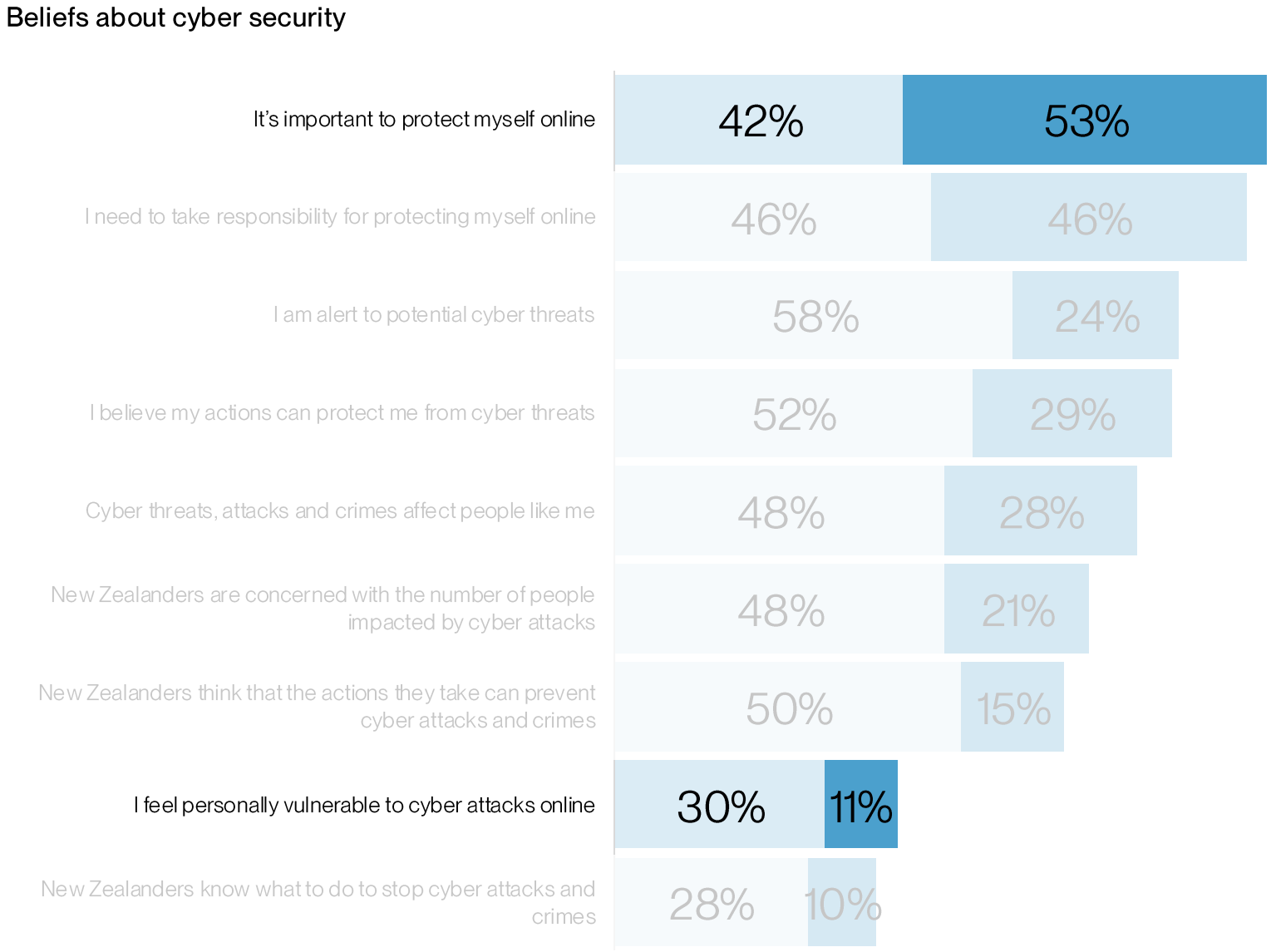
TRA NCSC

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 think they are.
Base: Total (Nov 25') n=1011

However – and crucially – they don't feel personally vulnerable

While 95% think it's important to protect themselves online, only 41% think they are personally vulnerable to cyber attacks. We have seen no significant changes year on year to this.

BELIEFSr: X- Please look at the following statements and indicate how strongly you agree or disagree with each of these
Base: Total (Nov 25') n=1011

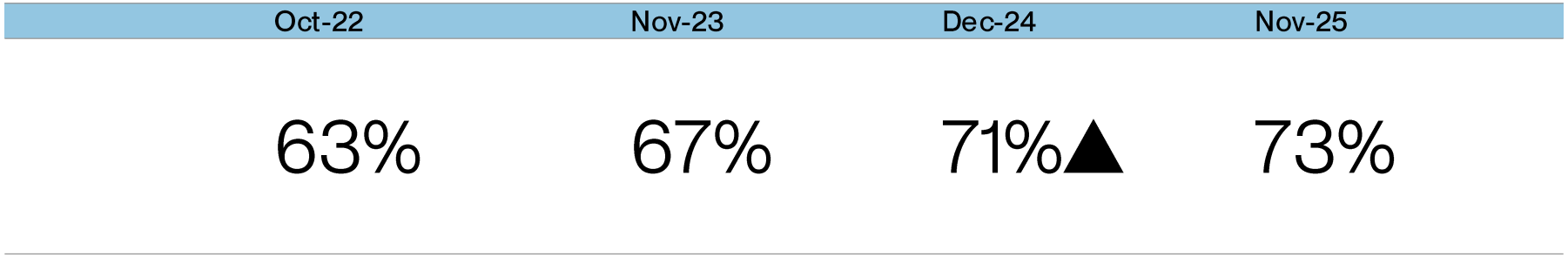


This is also reflected in continued high personal confidence

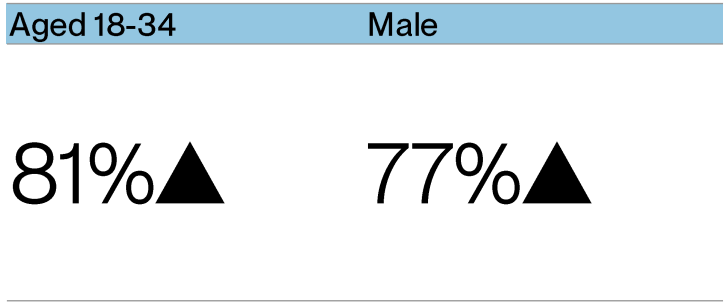
Confidence in their own ability to protect themselves has risen by 2% this year.

Younger people and males were significantly more likely to feel 'quite' or 'very' confident.

Confidence about personal cyber security – 'Quite Confident' and 'Very Confident'



Confidence about personal cyber security by demographics– 'Quite Confident' and 'Very Confident' (2025)



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…
Base: Total (Nov 25') n=1011
Quite confident & Very confident, 18-34: n=217
Quite confident & Very confident, Male n=358

And we know that vulnerability is motivating – those who do feel vulnerable are significantly more likely to take actions

Those who felt personally vulnerable were significantly more likely to take on more cyber actions than those who didn't.

Preventative actions taken 'always' and 'almost always' by those who feel personally vulnerable

	Do not feel personally vulnerable	Feel personally vulnerable
Don't share personal information online with people I don't know	90%	88%
Not clicking on links in emails or text messages that are not from trusted or familiar sources	86%	88%
Purposely keep my social media settings private	77%▼	83%▲
Update software, browsers and apps to the latest version as soon as possible after being notified to do so	71%▼	79%▲
Use strong passwords (longer than 15 characters with no personal information in them) for main accounts	66%▼	75%▲
Read customer reviews and feedback online to help check if a website is legitimate before trusting it with information or buying online	69%	73%
Use two-factor authentication on main accounts (email, banking, social media.)	70%	73%
Use a different password for each online account	54%▼	65%▲
Change the default passwords on devices like routers and other connected devices	50%▼	61%▲
Report cyber security incidents	43%▼	56%▲
Use a password manager	47%▼	56%▲

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 tell us how often you currently do them? 'Always' and 'Almost Always' by BELIEFS: X- Please look at the following statements and indicate how strongly you agree or disagree with each? Net Agree / Don't agree with "I feel personally vulnerable. Base Net agree 'I feel personally vulnerable' 2025 n=416 | Net don't agree 'I feel personally vulnerable' n=595

▲▼ Significantly higher/lower than other group

Appendix

Cyber 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 oropen 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