



2023 Annual Māori Population Survey Report

**KANTAR PUBLIC**

# Contents

- Background and methodology
- Key findings
- Technology usage
- Keeping protected online
- Awareness of rights and options
- Experience of unwanted digital communications
- Accessing support services
- Perpetrators
- Reporting harmful content
- Appendix

3

8

11

14

22

25

33

39

44

51

# Background and methodology

# Background



Netsafe is an independent, not-for-profit organisation with a mission to promote online safety among New Zealanders.

In order to effectively meet New Zealanders' needs, Netsafe commissions an annual survey to understand the ongoing role of technology in people's lives and their experiences online. Each survey measure contains a mix of questions: (a) core questions which don't change over time, and (b) topical questions, focused on providing detailed information about an issue.

The 2023 survey was focused on:

- Understanding the digital behaviour of New Zealanders,
- Assessing awareness of rights and options under the Harmful Digital Communications Act,
- Measuring awareness and use of support services for unwanted digital communications,
- Gaining insight into the experiences of unwanted communications for New Zealanders, and the impact these have on those who receive them,
- Understanding the experiences of Māori as perpetrators of harmful digital communications.

# Reporting



This year, the following reports have been produced:

1. APS 2023 results
2. Trended results for APS core questions 2017-2023
3. Online hate speech – 2023 results and trends in 2018-2023
4. Māori population 2023 results

This report focuses on the Māori population 2023 results.

# Methodology



518 Māori completed an online survey between 12 and 28 June 2023. The sample of survey participants were sourced from Kantar Public's online research and panel partners. The sample was structured to be representative of the population by terms of age, gender, and region.



Average survey length: 19 minutes



Response rate: 38%

# Methodology

The overall results have been weighted to 2018 Census figures for Māori to align the data with Census counts for age, gender, and region.

	Unweighted sample proportion	Weighted sample proportion
16 to 17 years old	7.5%	5.8%
18 to 29 years old	27.6%	29.0%
30 to 39 years old	10.0%	17.6%
40 to 49 years old	16.6%	17.3%
50 to 59 years old	13.9%	15.4%
60 to 69 years old	12.7%	9.3%
70 + years old	11.6%	5.4%
Male	52.5%	48.1%
Female	47.1%	51.5%
Gender diverse	0.4%	0.4%

	Unweighted sample proportion	Weighted sample proportion
Northland	3.1%	8.1%
Auckland	35.7%	23.5%
Waikato	9.2%	13.9%
Bay of Plenty	5.8%	11.5%
Gisborne/Hawke's Bay	4.2%	9.0%
Taranaki/ Manawatu-Whanganui	7.2%	9.9%
Wellington	12.4%	9.7%
Tasman/Nelson/Marlborough/ West Coast	3.9%	2.6%
Canterbury	11.9%	7.3%
Otago/Southland	6.4%	4.5%

# Key findings



# Key findings – Māori population

## Digital competency



Nearly three quarters of Māori *never or rarely* require assistance with digital technology.

Older Māori and wāhine Māori, are more likely than average to require assistance at least occasionally.

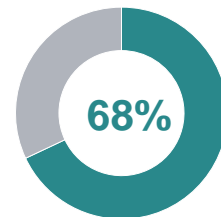
Most are competent in *searching the internet for what they want ...* and most are *communicating respectfully and contributing in a positive manner* (although, less so for some younger people).

Confidence drops slightly when it comes to managing *privacy, passwords, basic security settings* and *knowing how to filter online material* – particularly for older people.

## Keeping protected online



Most believe they know at least a fair amount about keeping safe and secure online.



Over two thirds have taken action to protect themselves or others online in the past year.

Concern about *online safety / security issues* and wanting to *avoid unwanted approaches from others* are the most common drivers for action.

## Awareness of rights and options

Around half of all Māori are aware of their rights and options under the HDC Act.

The **illegality** of online behaviour that intentionally causes harm to a person

**65%**  
AWARE

Ability to **lodge a complaint** about upsetting digital communications with an agency appointed by Government to help

**67%**  
AWARE

There are a set of **legal principles** that people are required to follow when communicating with others online

**49%**  
AWARE

Deliberately **causing harm** with digital communications is punishable with imprisonment or a fine

**59%**  
AWARE

# Key findings – Māori population

## Unwanted digital communications



**Forty-six percent have received unwanted digital communications in the past year.**

Those who identify as LGBTQI+, neurodiverse, and those with a long-term disability or long-term health issues are **most likely** to have received unwanted communications.



**Thirty-nine percent of recipients say these communications have had a negative impact on their life.**

## Accessing support services

23%



**Just under a quarter of those who experienced unwanted digital communications contacted some type of support service.**

Support is typically sought from an internet platform/provider such as Facebook or Google, or the police.



Of those who contacted a support service, **forty-three percent** found it helpful.

Those who sought help from an internet platform/provider were more likely than average to have found it unhelpful, and those who sought help from the police were more likely to have found it helpful.

## Perpetrators



**Nine percent of Māori admit to having sent or shared at least one type of unwanted digital communications.**

**Most** have also been victims of digital harm.

The communications they sent or shared commonly either attempted to get *revenge*, to *make a joke*, or to *embarrass* someone.

Sixty percent of the time, perpetrators were sending unwanted communications to people they know.

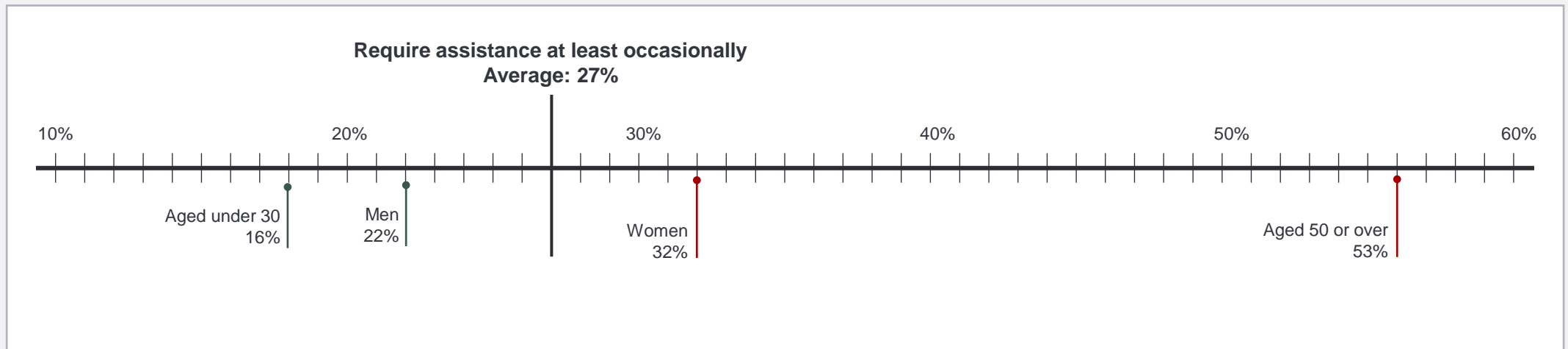
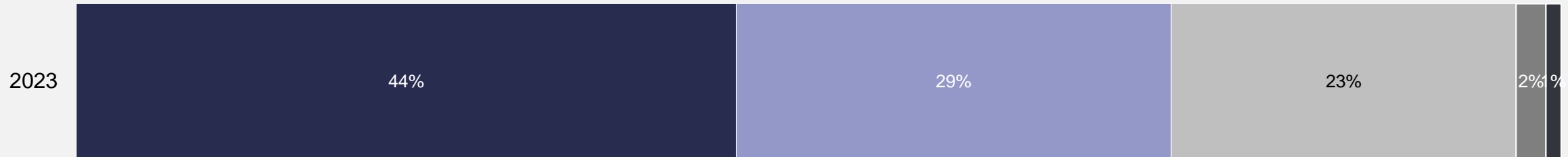
# Technology usage

# Digital competency

Nearly three quarters (73%) of Māori rarely or never require assistance when using digital technology. Older Māori (and to a lesser degree wāhine Māori) are more likely than average to require assistance at least occasionally.

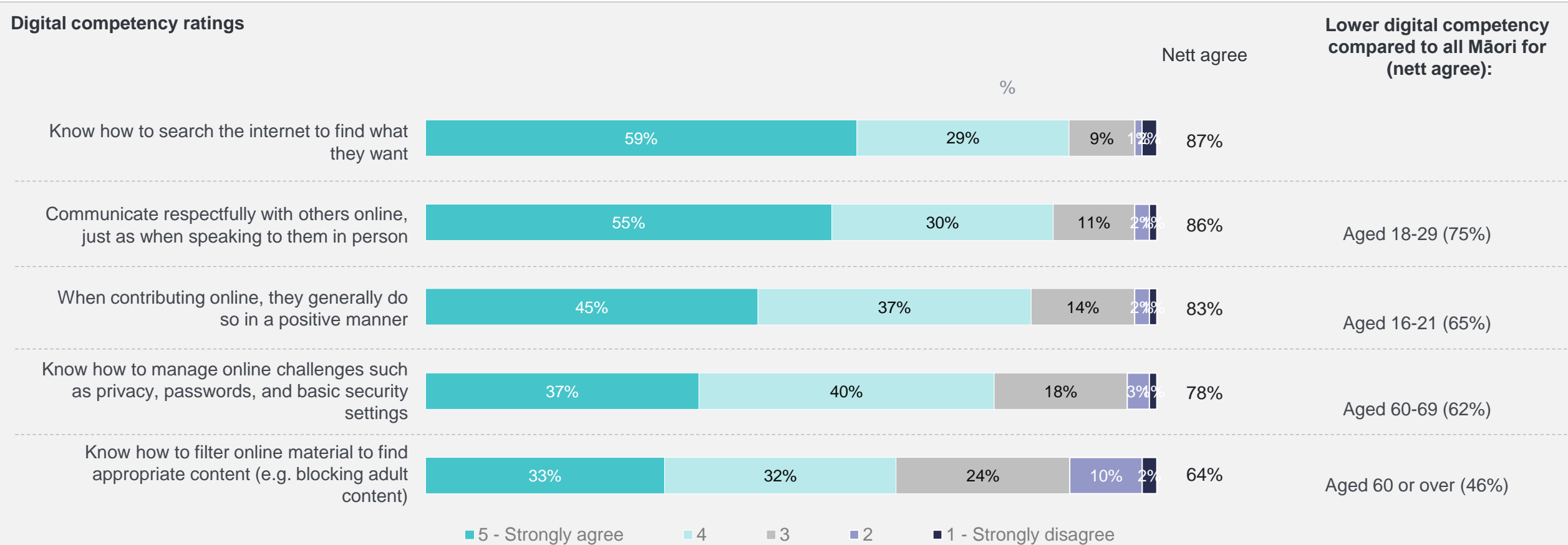
## Competence using digital technology

■ I very rarely or never require assistance ■ I rarely require assistance ■ I occasionally require assistance ■ I frequently require assistance ■ I usually or always require assistance



# Specific digital competency

Most are competent in searching the internet for what they want, communicate respectfully, and contribute in a positive manner. Confidence drops slightly when it comes to managing privacy, passwords, and basic security settings and knowing how to filter online material – particularly for older people.

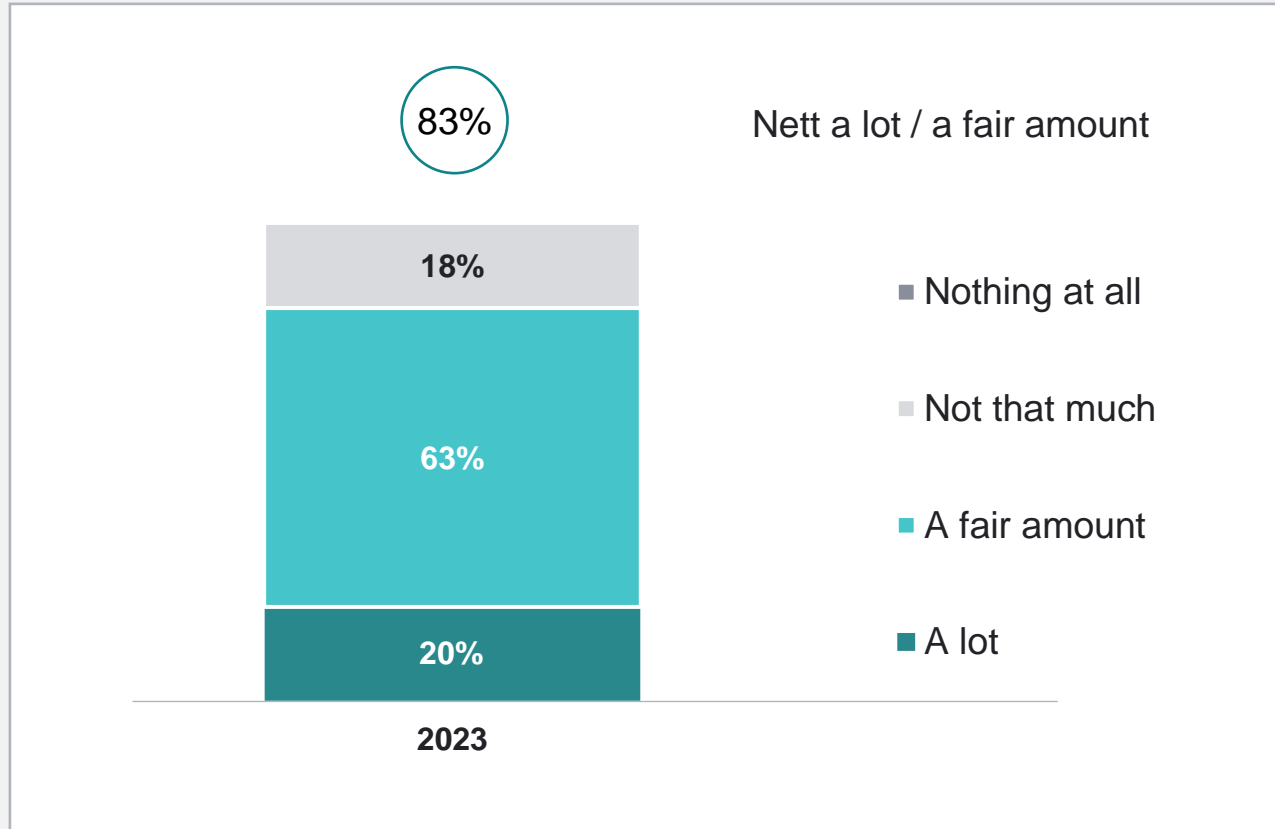


# Keeping protected online

# Knowledge of online safety

Most know **a lot** or a **fair amount** about keeping safe and secure online.

## Personal knowledge of online safety

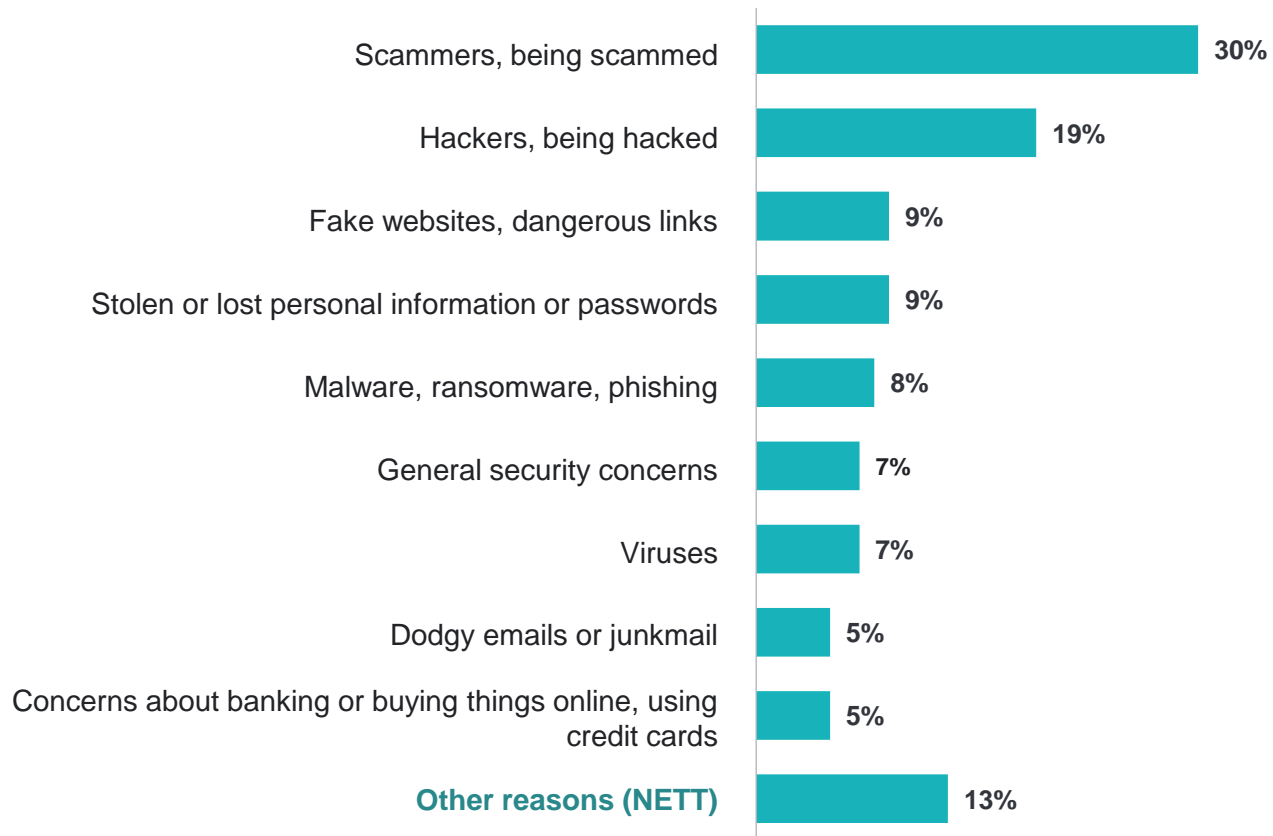


**Māori aged 50-59 (6%), and those who identify as neurotypical (17%) are less likely than average to know a lot about keeping safe and secure online.**

# Biggest concerns and perceived risks about going online

When asked about the main challenges or risks of going online, scammers / being scammed is the most common concern followed by getting hacked. Older Māori are more likely than average to be concerned about receiving dodgy emails (18% vs 5%), and financial security online (16% vs 5%).

## Biggest concerns/risks about going online



**Tāne Māori** are less likely than average to be concerned about being hacked online (**15%**), while those living in **Wellington** are more likely than average to be concerned about malware or spyware being used against them (**16%**).

Māori **aged 70 and over** are more likely than average to have concerns about dodgy emails or junk mail (**18%**), and online financial transactions or financial security (**16%**).



# Concerns and risks about going online in their own words...

*"Getting hacked, having info leaked online, getting scammed, being catfished."*

**Wahine, 16-29 years, Otago/Southland**

*"Being hacked, someone taking my identity, someone accessing my personal information"*

**Tāne, 60-69 years, Auckland**

*"Inappropriate advertising - e.g. things that are sexual or pornographic; scams that get you to pay too much money for something or pay money towards something that doesn't exist; inappropriate people messaging or online relationships with people who are not what they seem; cyberbullying and other harmful messages or content. "*

**Wahine, 16-29 years, Taranaki/ Manawatū-Wanganui**

*"Viruses actively looking for weakness in security software, cookies, phishing, emails being skimmed for personal info, identity theft, fake websites."*

**Tāne, 50-59 years, Auckland**

*"Downloading a file that is dodgy can mean you might get hacked or a virus."*

*I think the main risk though is how bad online security and data sharing is [...] only around 43% of websites allow you to opt out of data collection and even then, they have been proven time and time again to still track, keep, and sell your data. Even the MOST tech savvy users, the most aware users and the most prepared users cannot escape their information being taken, tracked, bought and sold. "*

**Tāne, 16-29 years, Wellington**

*"Information being stolen/shared, phishing, constant advertisements popping up."*

**Wahine, 30-39 years, Northland**

*"Not trusting the links that are present to purchase online products through. Divulging too much information. "*

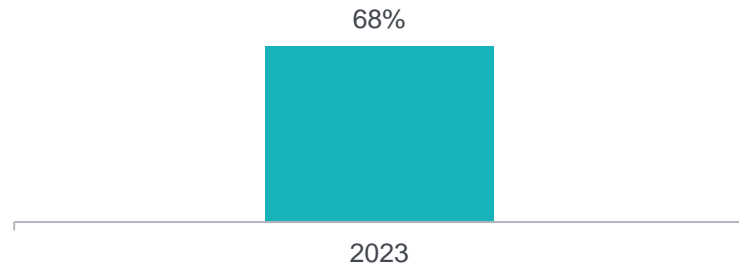
**Wahine, 40-49 years, Waikato**

# Action taken to protect self or others online

Two thirds of Māori have taken actions in the past 12 months to protect themselves or others online. Half of those who took action cited concern for online safety and security issues as a contributing reason.

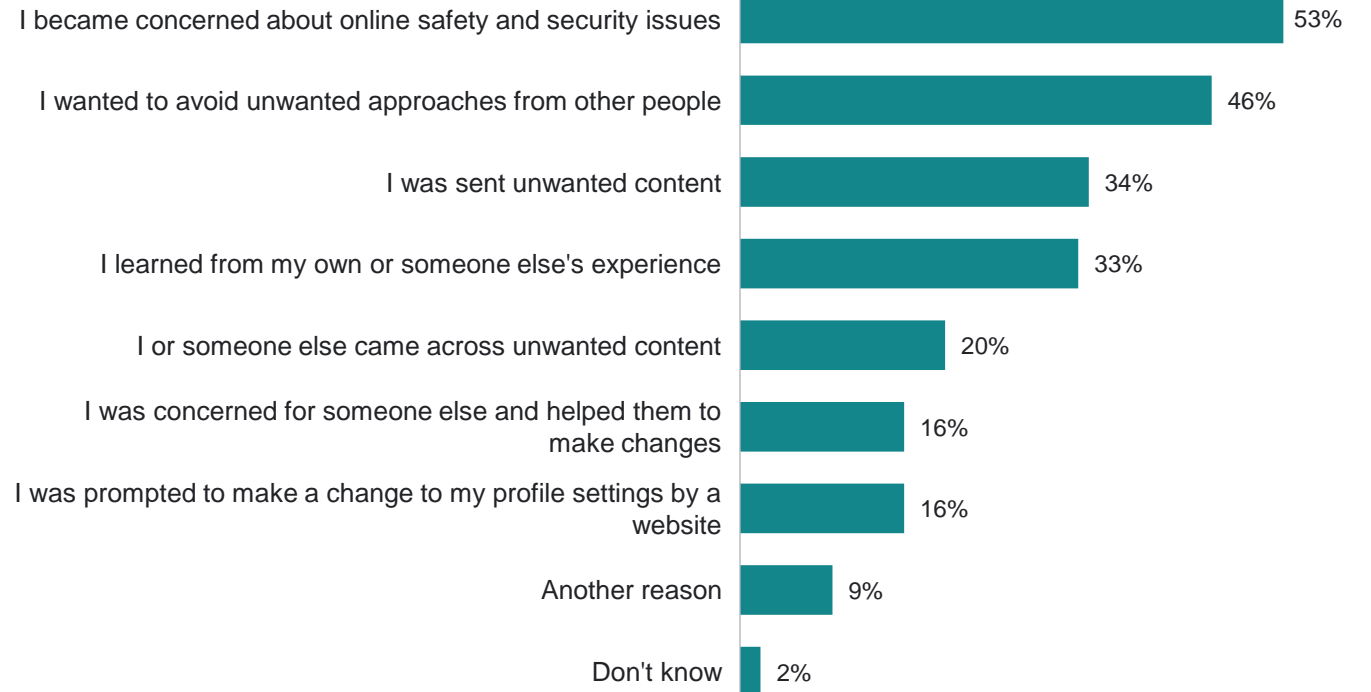
**68%**

have taken action to protect themselves or others online in the past 12 months



Those **aged 30-39 (85%)** are more likely than average to have taken steps to protect themselves or others online in the past year.

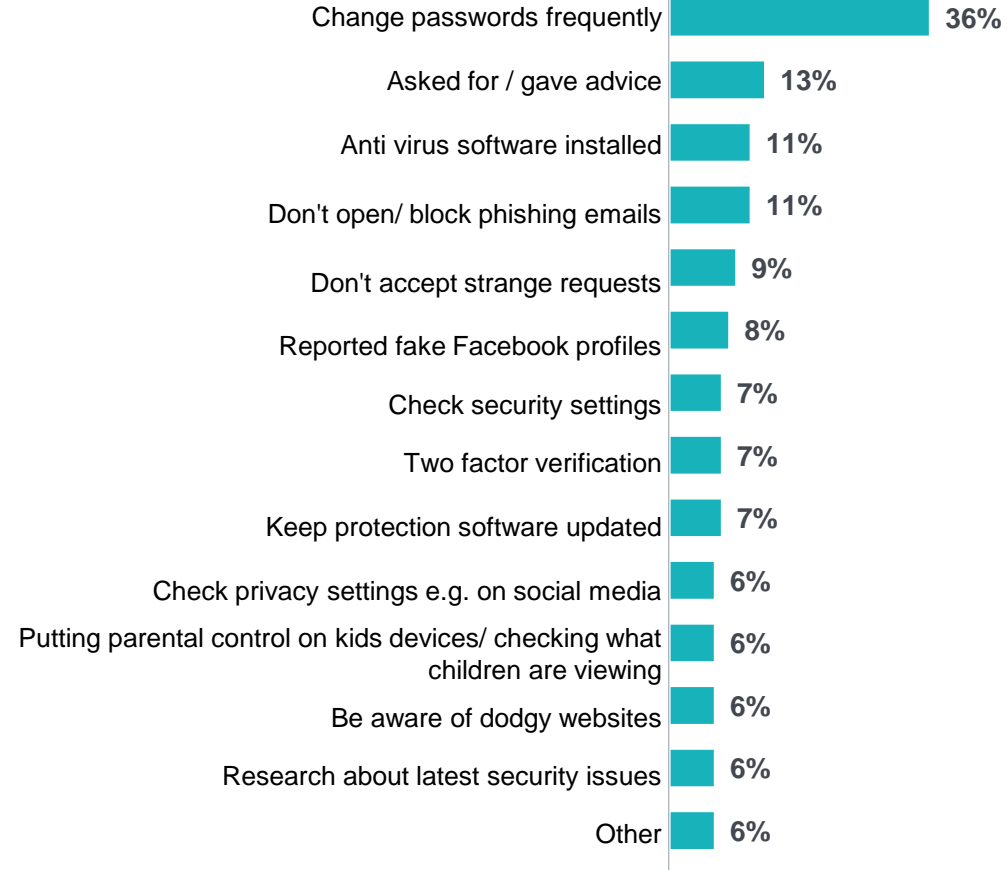
## Reasons for taking action to protect self and others online



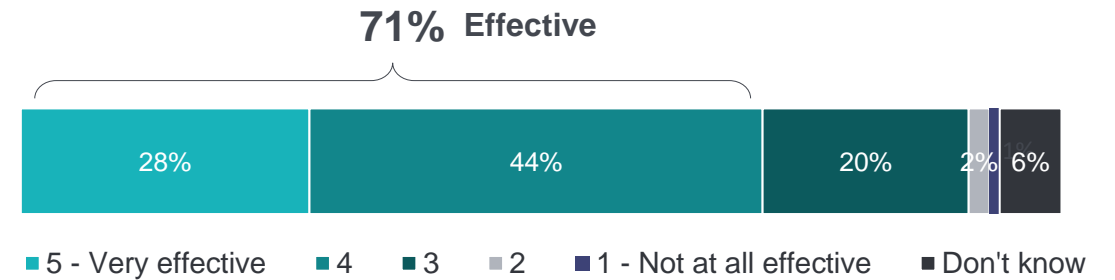
# Action taken to protect self or others online

The type of protective actions taken are quite varied with *regular changing of passwords* the most common. Most (71%) perceive the protective measures they took to be effective.

## Protective actions taken



## Perceived effectiveness of protective actions taken



# Action taken to protect self or others online

The main reason people don't take any action is a sense that they've *already done everything they can* to protect themselves and others online. One in five *don't know what actions to take* and just over one in ten haven't acted because they either *feel safe from all risk and harm online* or it is just *not a priority*.

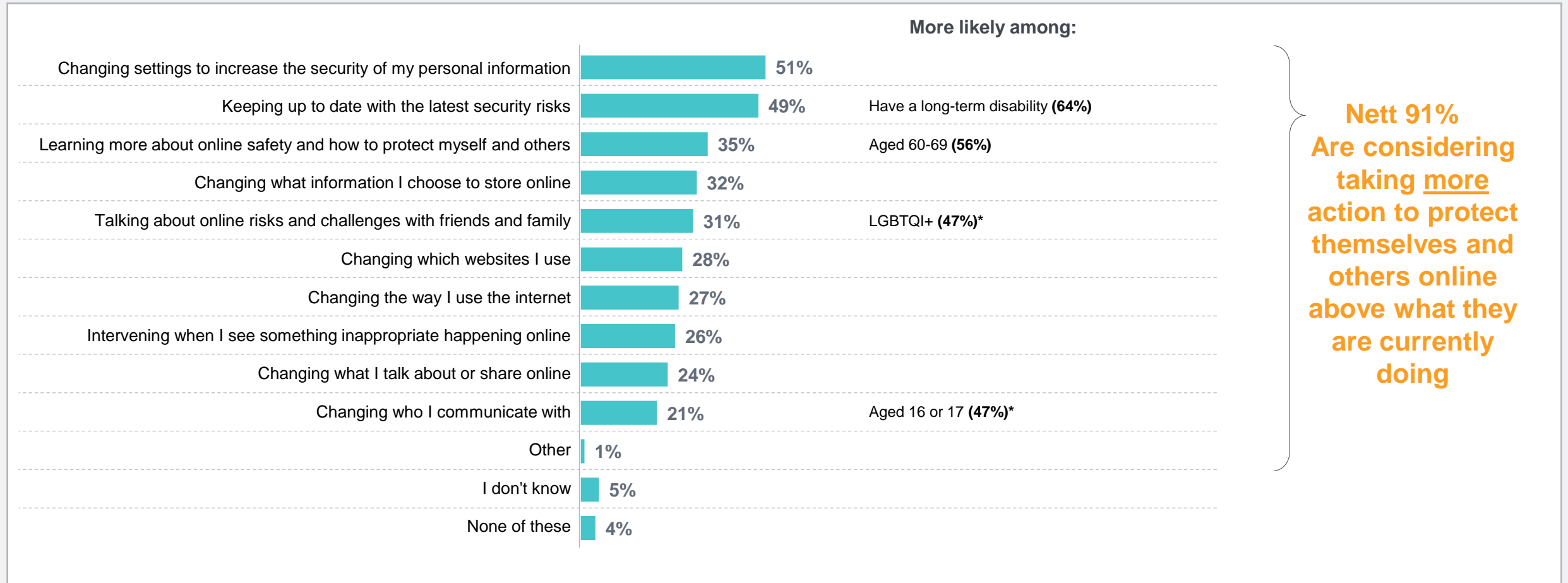
## Reasons for not taking action



# Consideration of future protective actions

Nine in ten are considering taking **more** precautions in the future to protect themselves or others from online harm. Ways of doing this vary with *updating security settings* and *keeping informed about the latest security risks* being most common.

## Consideration of taking protective online actions in future (actions that are not currently being taken)



\* Caution small base size – results are indicative only.

Base: All Māori respondents (n=518)

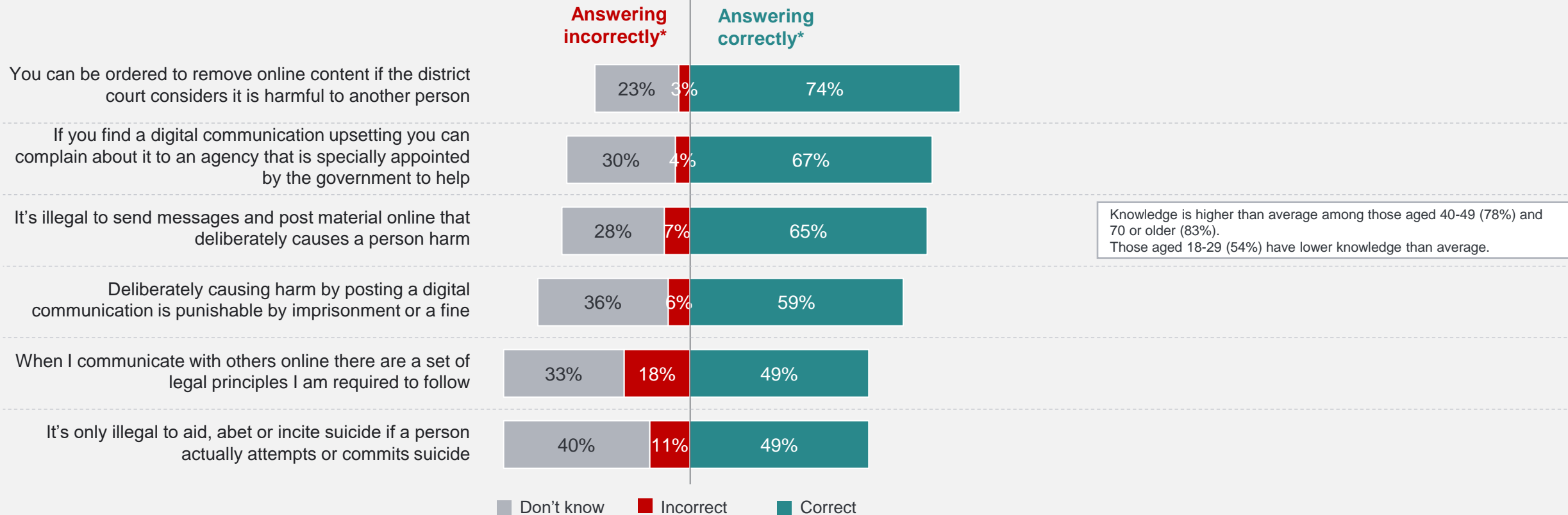
Source: Q15. Now thinking ahead to the next 12 months, which of the following precautions would you consider taking to protect yourself and others from potential online risk or harm? Please only select the things you are not currently doing to protect yourself and others online.

# Awareness of rights and options

# Awareness of legislation

Around half of all Māori are aware of legislations set in place in Aotearoa around their rights and responsibilities online. Younger people aged 18-29 years are less likely than average to know that it is *illegal to message or post material online that deliberately causes a person harm*.

## Awareness of NZ legislation



\* Caution small base size – results are indicative only.

Note: All statements are true, except for 'it's only illegal to aid, abet, or incite suicide if a person actually commits suicide' – this is false.

Base: All Māori respondents (n=518).

Source: Q17. Now thinking about your rights and responsibilities under current New Zealand legislation, please indicate whether you think the following is true or false. If you are not sure, then please tick 'Don't know'.

# Most important principles when communicating online

When asked what digital communications **should not** include, *encouraging some to harm themselves* is most mentioned followed by *sharing intimate images/recordings of someone without their permission*, and *sharing indecent or obscene content*.

## Digital communication should not\*...

	Rated in top 3 (combined)
Try to get someone to hurt themselves (e.g. self-harm, commit suicide)	62%
Share intimate images or recordings of someone without their permission	45%
Include indecent or obscene content (e.g., extreme violence or sexually explicit)	43%
Share other personal information about someone without their permission	33%
Threaten to hurt someone or damage their property	28%
Insult someone because of their personal what they look like, their lifestyle, where they come from or what they believe in	26%
Be used as a way to get back at someone by harassing them	21%
Encourage other people to send messages to someone as a way to try and harm them	17%
Make a false allegation about someone	13%
Include content that most people would agree is offensive to the person receiving it	10%

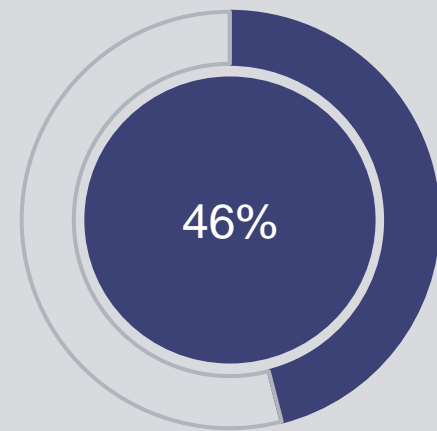


# Experience of unwanted digital communications

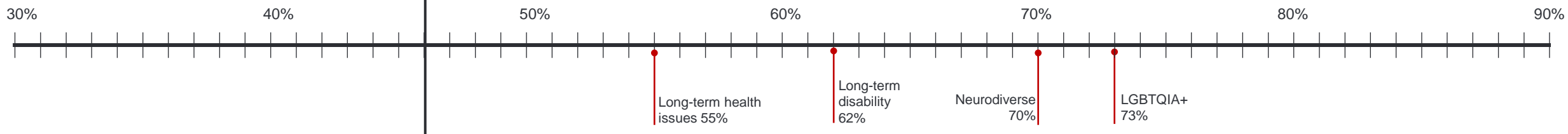
# New Zealanders' experience of unwanted digital communications

Just under half (46%) of all Māori have experienced unwanted digital communications in the past year. This is more common among those who identify as LGBTQI+, neurodiverse, and those with a long-term disability or long-term health issues.

Experienced unwanted digital communications in last year

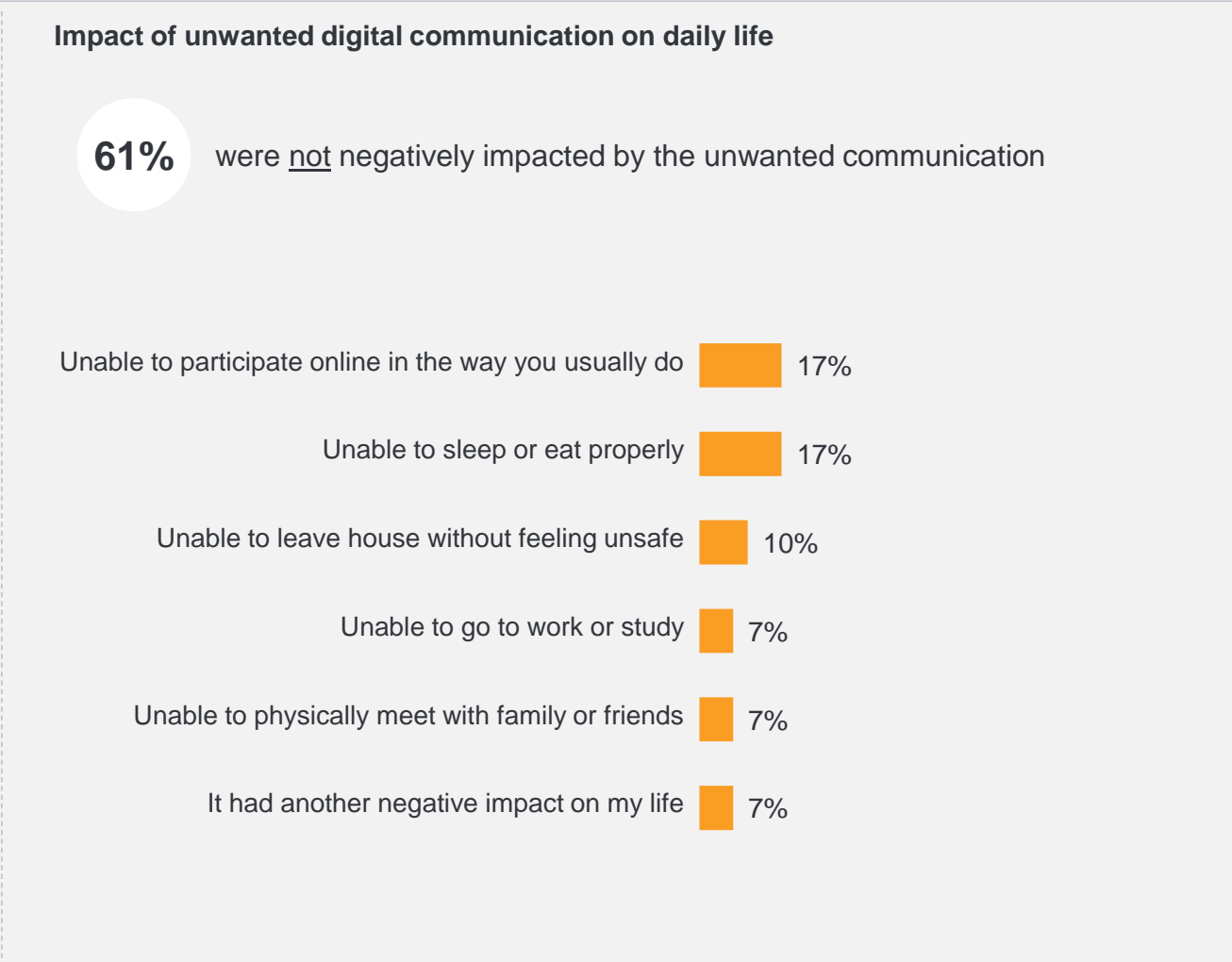
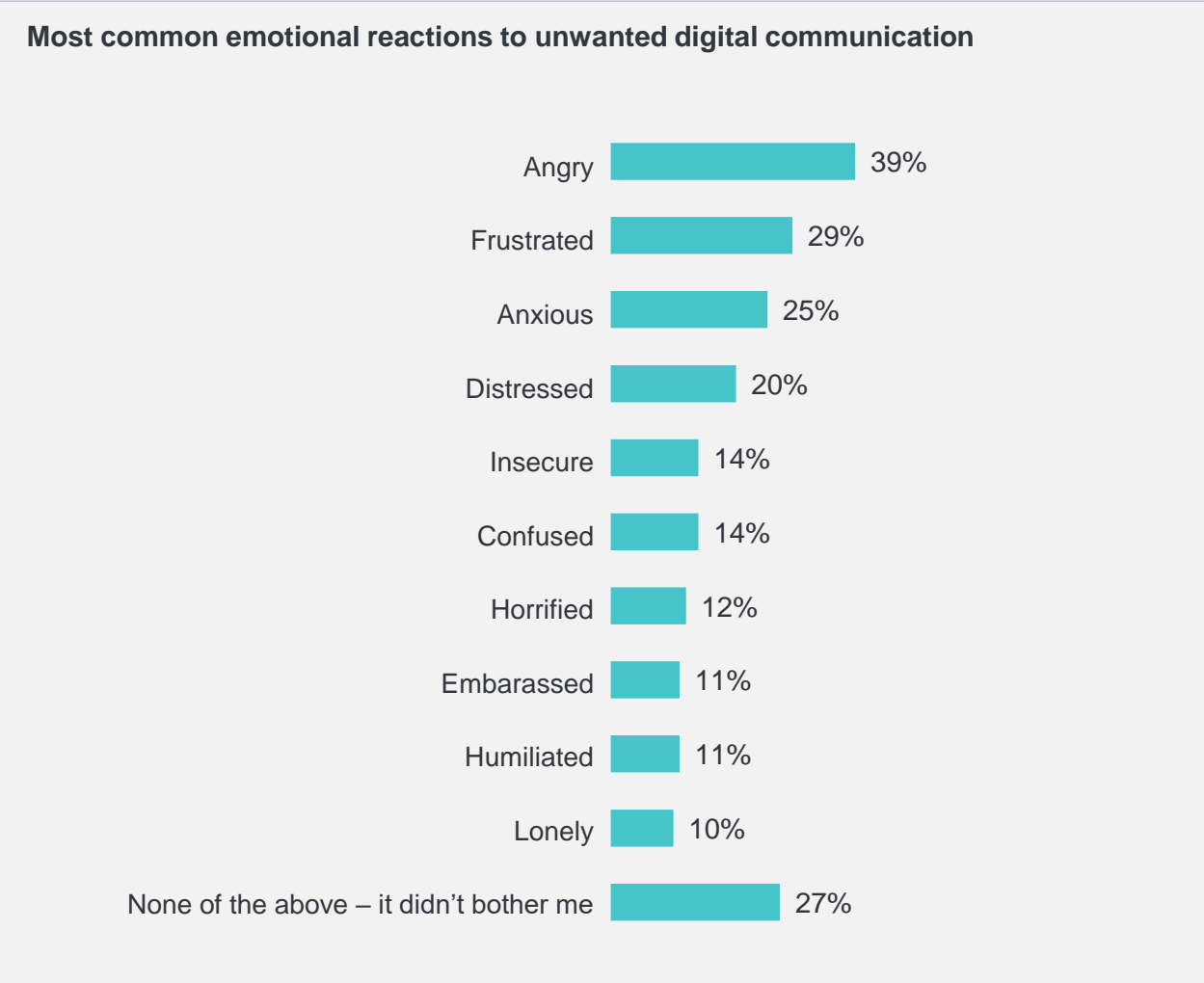


Experience of unwanted digital communications  
Average: 46%



# Impact of unwanted digital communications

Anger, frustration, and anxiety are the emotions commonly felt by people receiving unwanted digital communications, and while most (61%) say they have not been negatively impacted, there are some who have been seriously impacted.

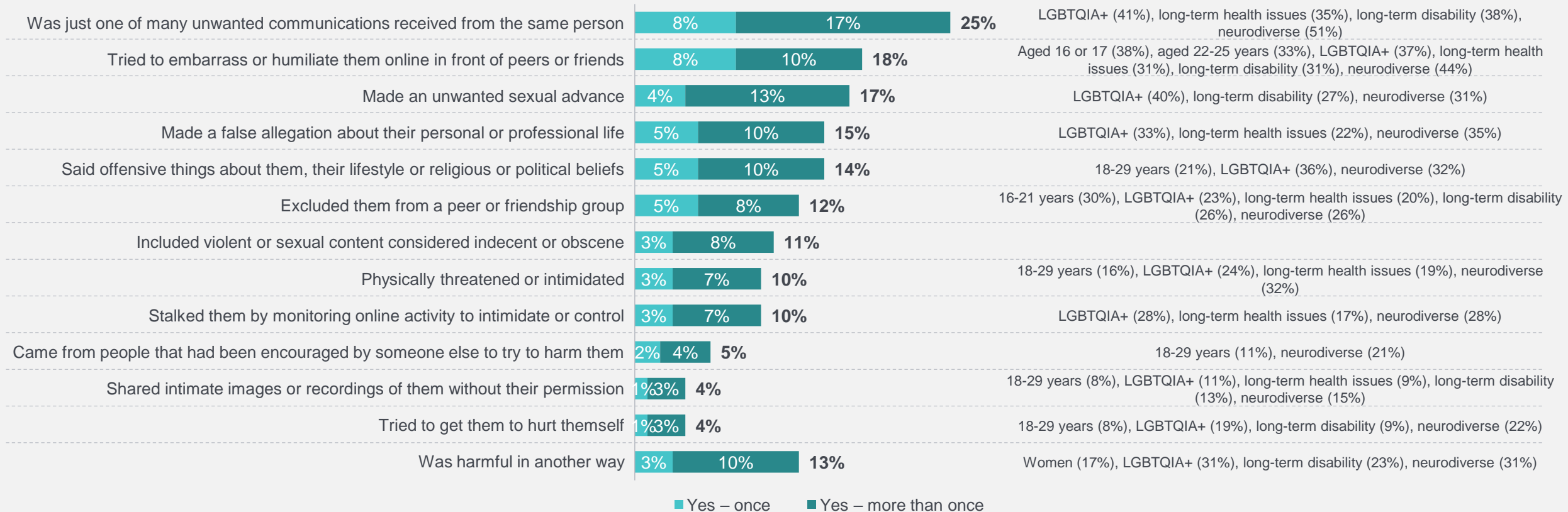


# New Zealanders' experience of unwanted digital communications

The nature and type of unwanted communications people are receiving is quite varied, with *repetitive unwanted communications from the same person* the most common. Other common types of unwanted communications include being *embarrassed or humiliated online*, *unwanted sexual advances*, *false allegations*, *offensive remarks about lifestyle, religious or political beliefs*, *violent or indecent/obscene content*, *physical threats*, *intimidation*, and *stalking*. Younger Māori, LGBTQ+, and those living with a long-term disability or health issue are particularly vulnerable to receiving multiple types of unwanted digital communications in the past year.

## Type of unwanted digital communications

### More likely among the following groups (NETT Yes):

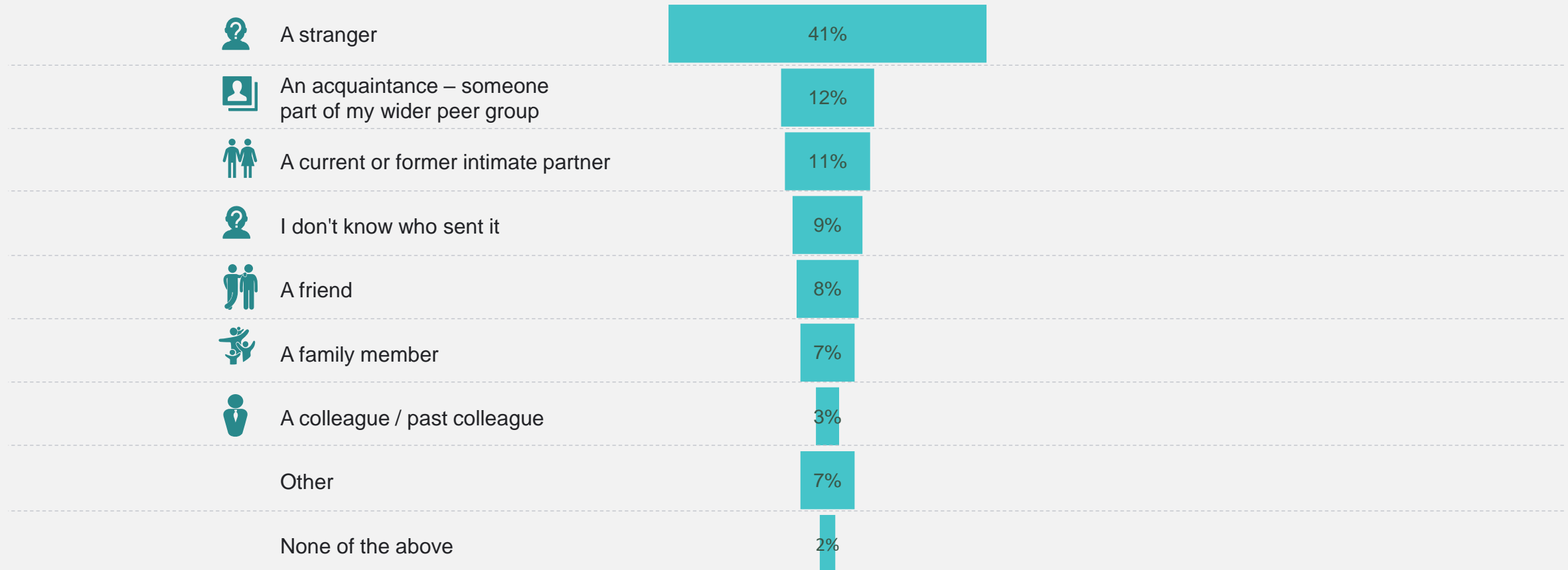


\* Caution small base size – results are indicative only.  
 Base: All Māori respondents (n=518).  
 Source: Q18. In the last 12 months, have you personally received an unwanted digital communication (e.g. email, text, photo, video, or online comment) that...

# Proximity to sender of unwanted digital communication

For many (41%) of those who received unwanted digital communications, the sender was unknown to them. Twelve percent of the time it was sent by an acquaintance, and eleven percent of the time a current or previous partner was the sender.

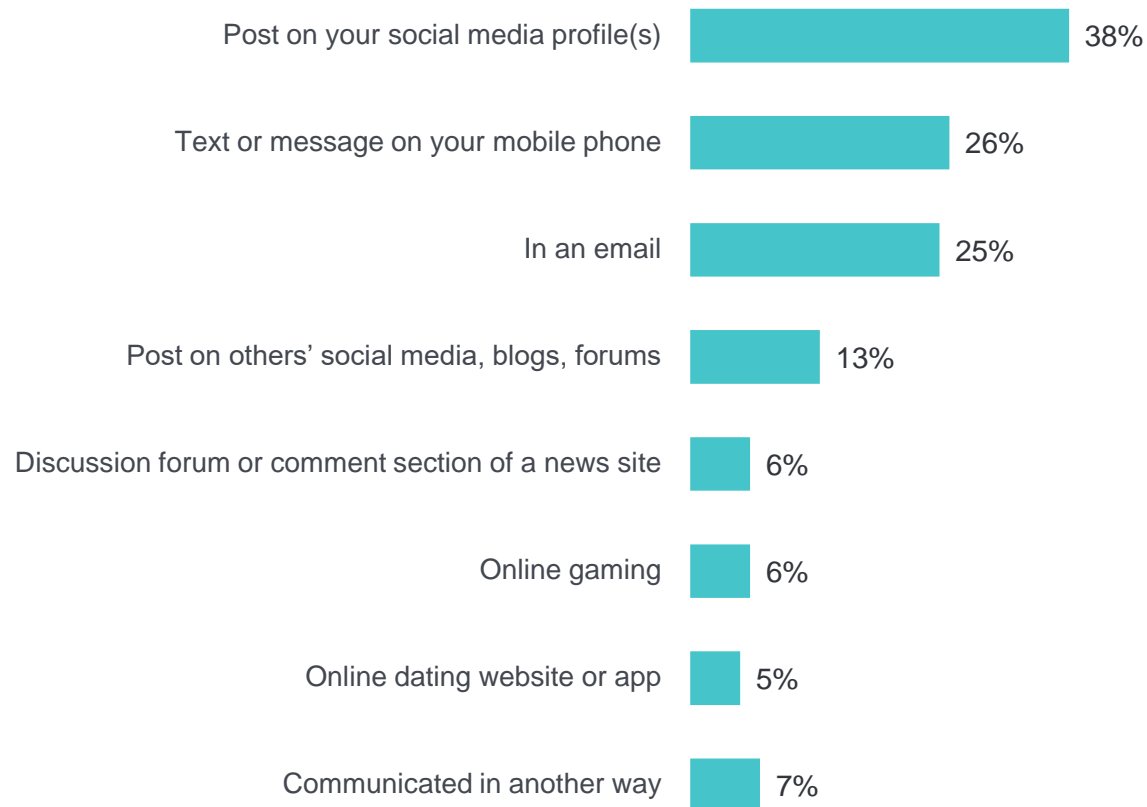
## Sender of unwanted communication



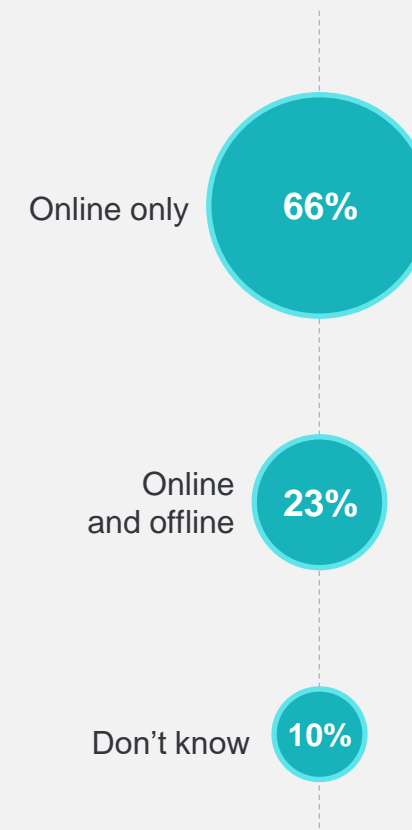
# Channels for unwanted communications and connection to offline events

Of those who received unwanted digital communications in the past year, 38% get it through their social media profiles, and one in four receive it either through their phone or in an email. The unwanted communications are isolated to online platforms for most (66%), but for 23% this is part of a wider issue also happening offline.

## Channel of unwanted digital communication



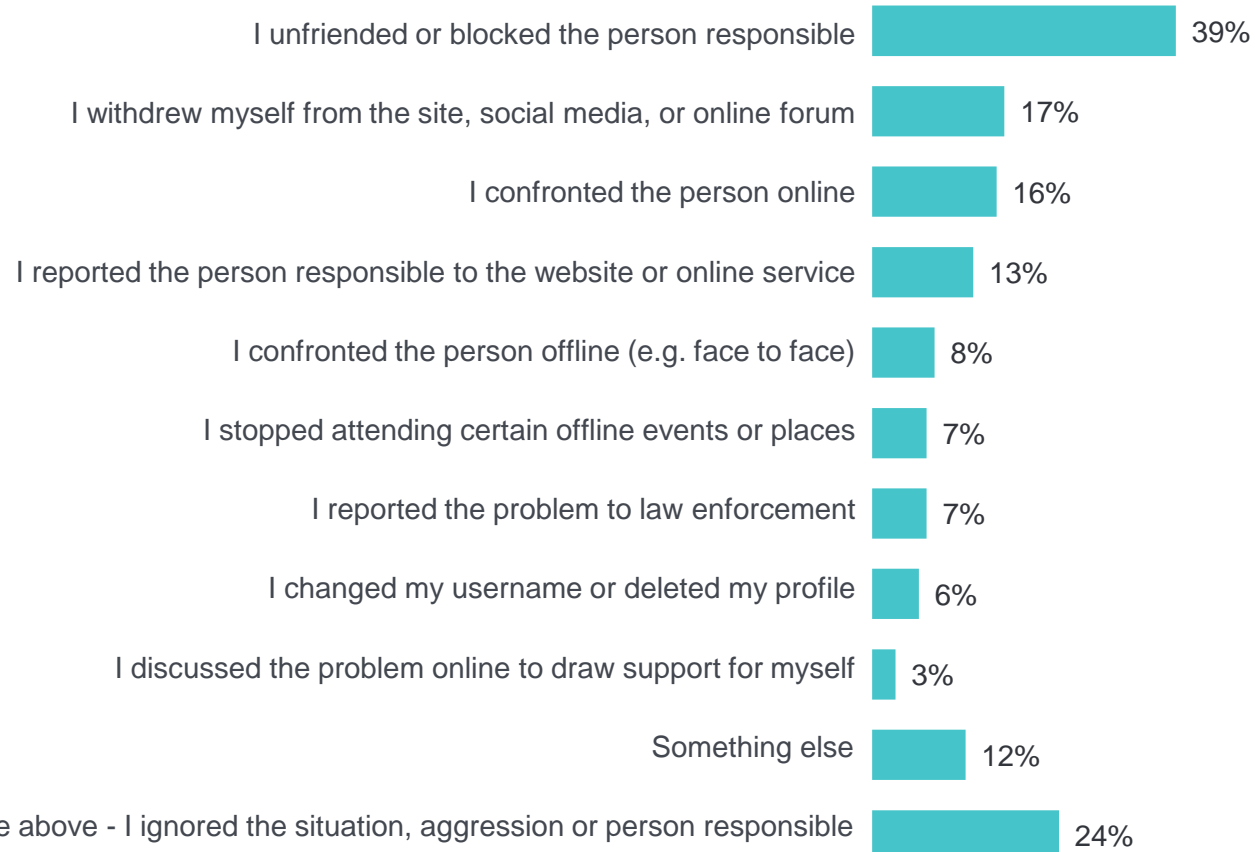
## Part of a wider issue happening offline



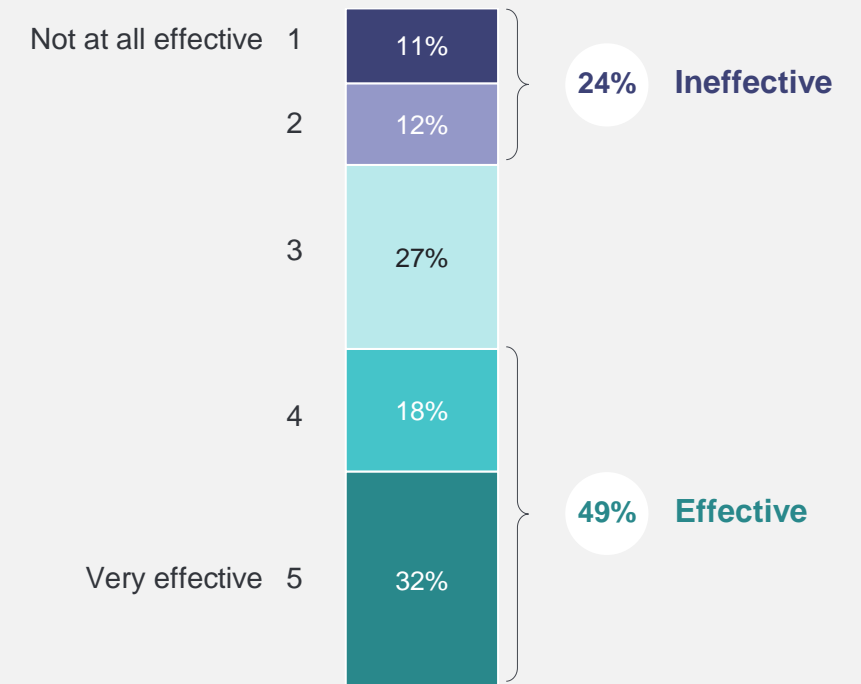
# Responses to unwanted digital communications and perceived effectiveness

The most common responses to unwanted communication are to block or unfriend the person responsible, or ignore the situation or person entirely. Only half (49%) of those who took action say it was effective.

## Response to situation



## Perceived effectiveness of response at changing the situation



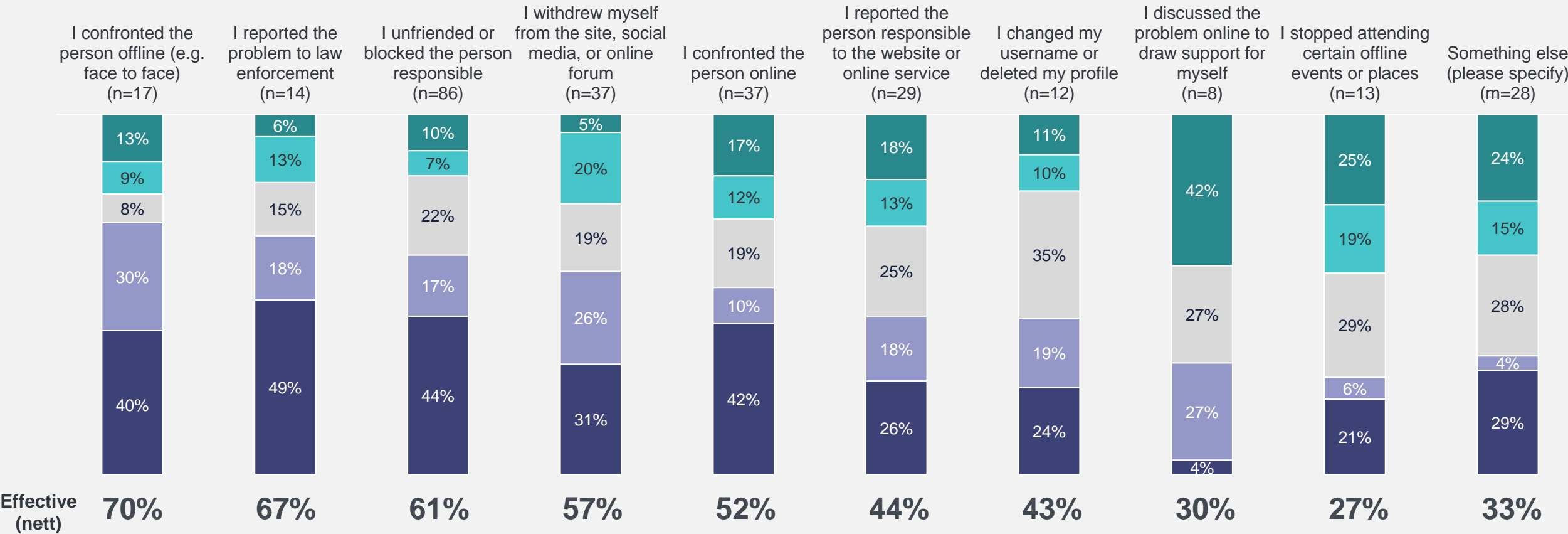
Base: Māori respondents who have experienced an unwanted digital communication and did not ignore the situation (n=178).

# Perceived effectiveness of responses to unwanted digital communications

The responses perceived to be the most effective are either confronting the sender in person, or reporting the incident to law enforcement.

Perceived effectiveness of response of the different reactions

■ 1 - Not at all effective ■ 2 ■ 3 ■ 4 ■ 5 - Very effective



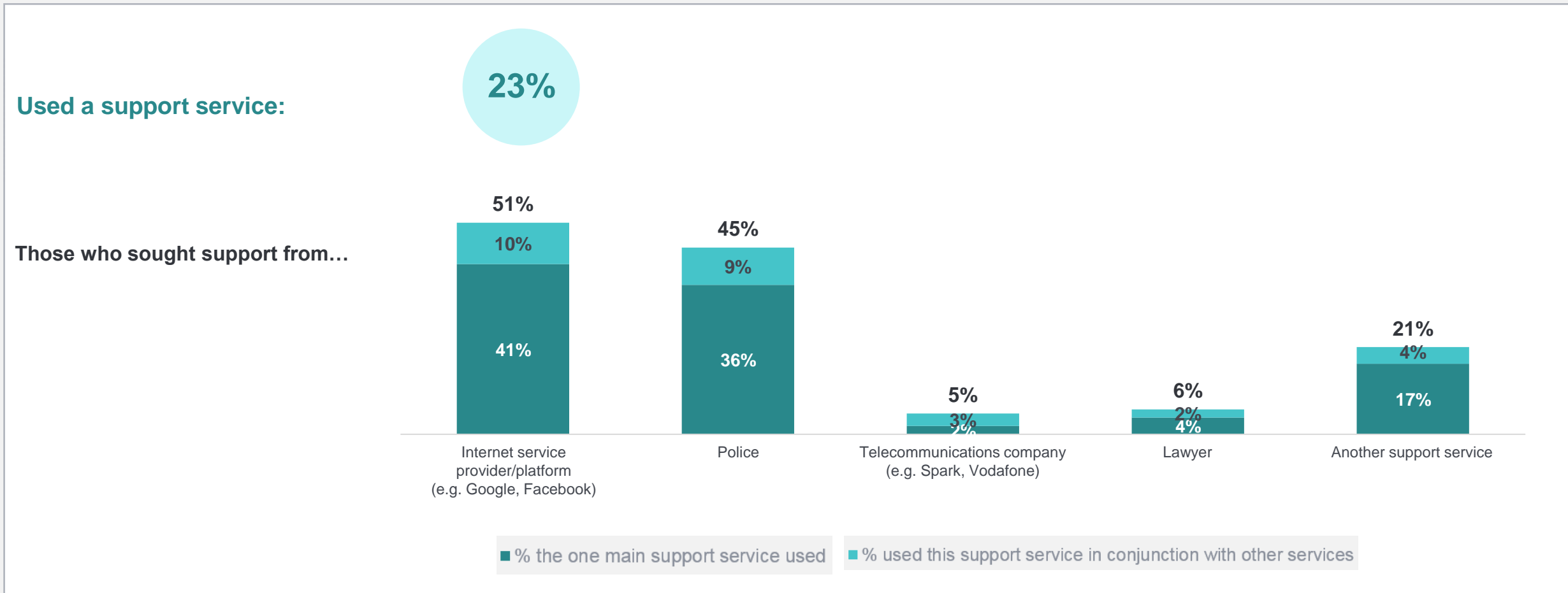
\* Caution small base size – results are indicative only.  
 Base: Māori respondents who had experienced at least one incident of unwanted digital communications in the last year (see chart for bases)  
 Source: Q23. How did you respond to this experience in order to change the situation? Q24. And, overall, how effective was your response(s) at changing the situation?



# Accessing support services

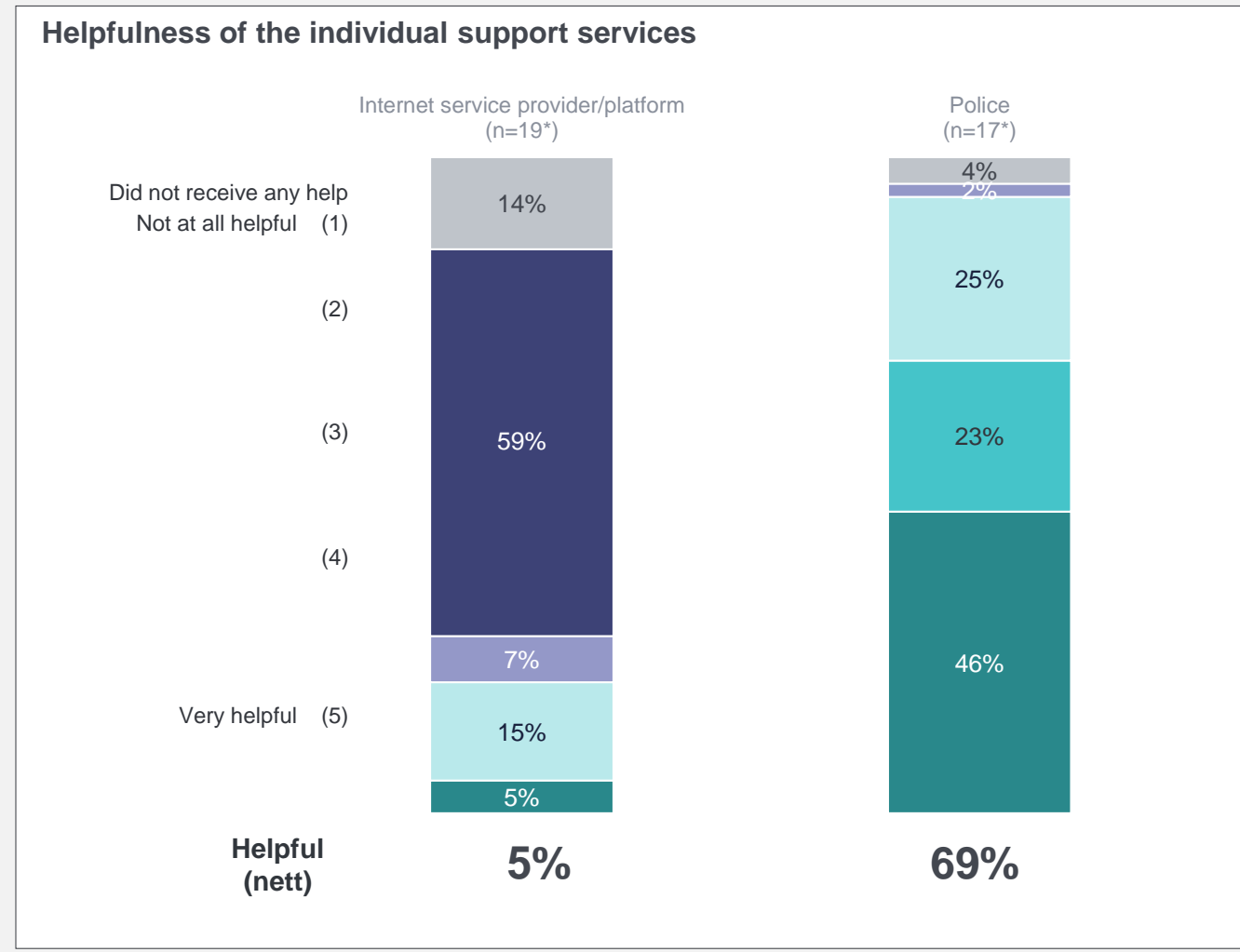
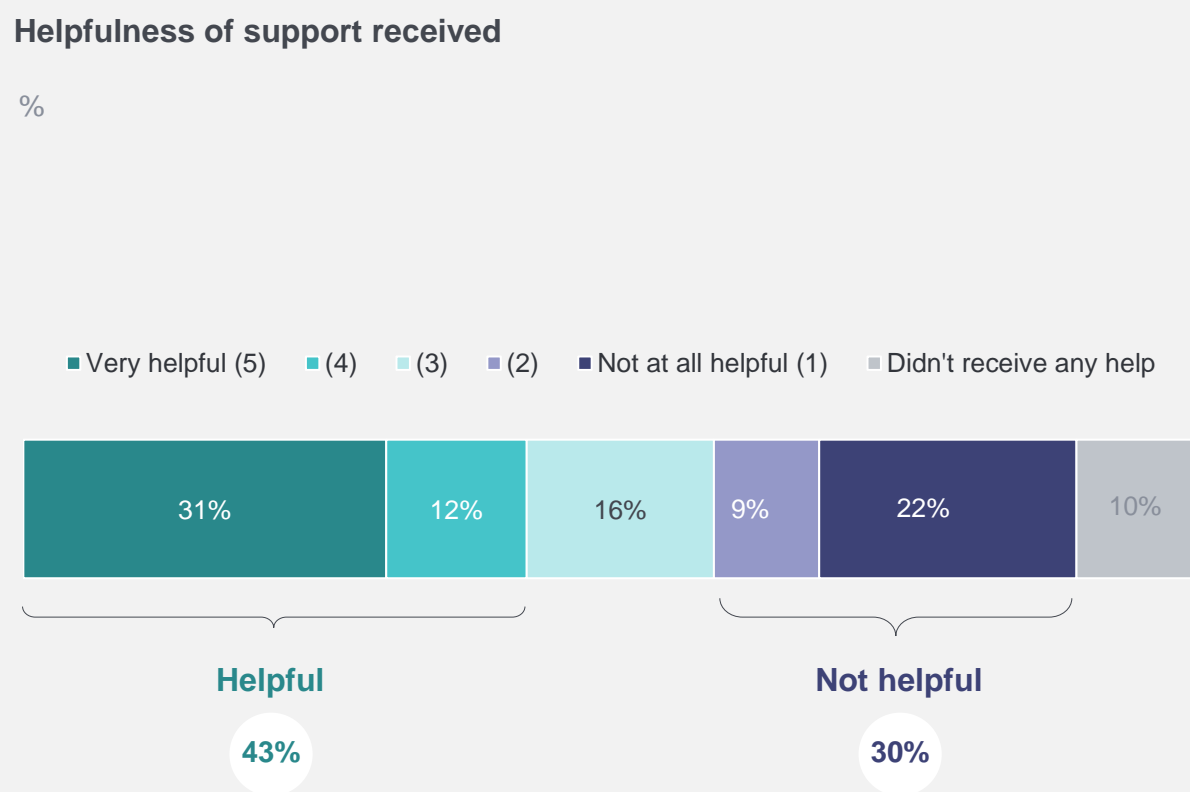
# Use of support services

23% of those who received unwanted communications reached out to a support service, and this tended to be internet service providers/ platforms or the police.



# Helpfulness of support services

Overall, 43% of those who sought support from a service found it helpful. However, those who sought support from an internet service provider or platform were almost thirteen times more likely to have found it unhelpful (66%) than helpful (5%). Those who sought support from the Police were far more likely to have found it helpful than unhelpful (69% vs 2%).



# Reasons support was not helpful in their own words...

*"Anytime you report anything on Facebook whether it be harassment, bullying, or a scammer, you can report it all you like and nothing gets done, they say it's not offensive or the fact it's a scam and it stays up"*

**Wahine, 30-39 years, Taranaki / Manawatū-Wanganui**

*"Computer generated response, they just don't have the time or actually care!!"*

**Tāne, 50-59 years, Bay of Plenty**

*"They said it did not go against community standards."*

**Wahine, 40-49 years, Taranaki / Manawatū-Wanganui**

*"The police made me feel as though I was in the wrong by believing the people that were spreading this information were the victims."*

**Tāne, 50-59 years, Taranaki / Manawatū-Wanganui**

*"They sided with the other person and allowed them to keep posting, it didn't hit their "threshold" to do anything."*

**Tāne, 30-39 years, Canterbury**

We also asked what further support people would like for themselves and their whānau when online. Many mentioned specific support and education for both their elderly whānau and their tamariki.

*"Parental supervision when online for kids is difficult. We are working with our children to identify good habits at a young age."*

**Tāne, 40-49 years, Waikato region**

*"General (more accessible information) on how to be safe. I think information for older or vulnerable people about deep fakes/AI being able to replicate voices or images, might be more susceptible to newer types of scams."*

**Wahine, 30-39 years, Auckland**

*"Some education for older people i.e., 65+ around being safe in the cyber and phone sphere"*

**Wahine, 16-29 years, Wellington**

*"Kids to have blocks on stupid content."*

**Tāne, 40-49 years, Auckland**

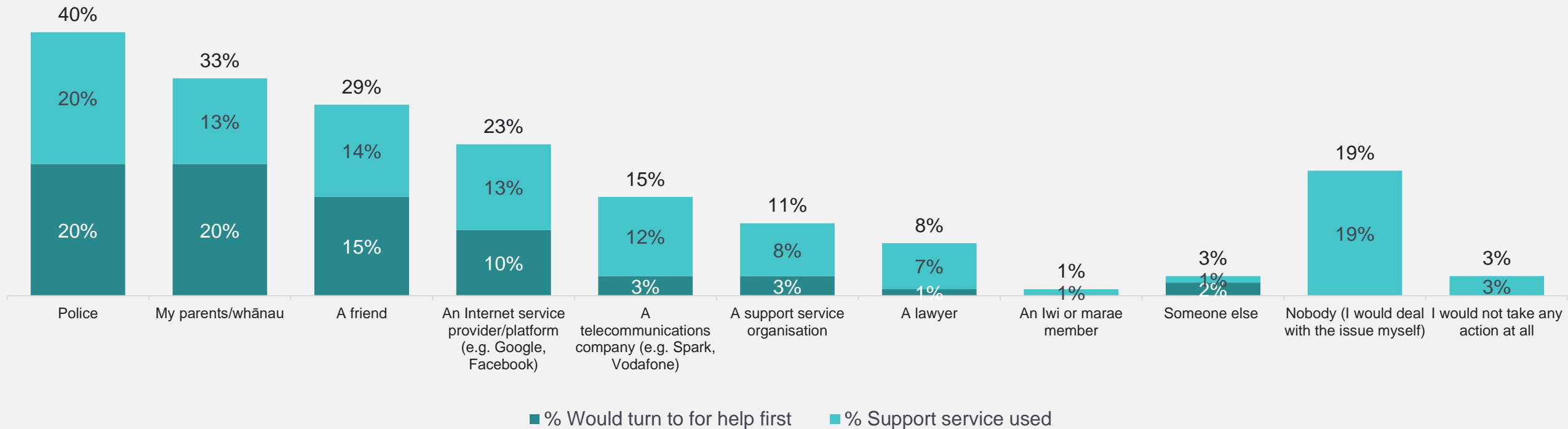
*"I think more strong education and support through New Zealand schools."*

**Wahine, 40-49 years, Canterbury**

# Future consideration (for those who have not experienced unwanted communications)

For those who have not experienced unwanted communications in the past year, 40% say they would contact the *police*, and around 1 in 3 would reach out to *whānau* (33%) or a *friend* (29%). One in five (19%) wouldn't seek help from anyone, preferring to deal with it themselves.

## Support services in future situations involving unwanted digital communications

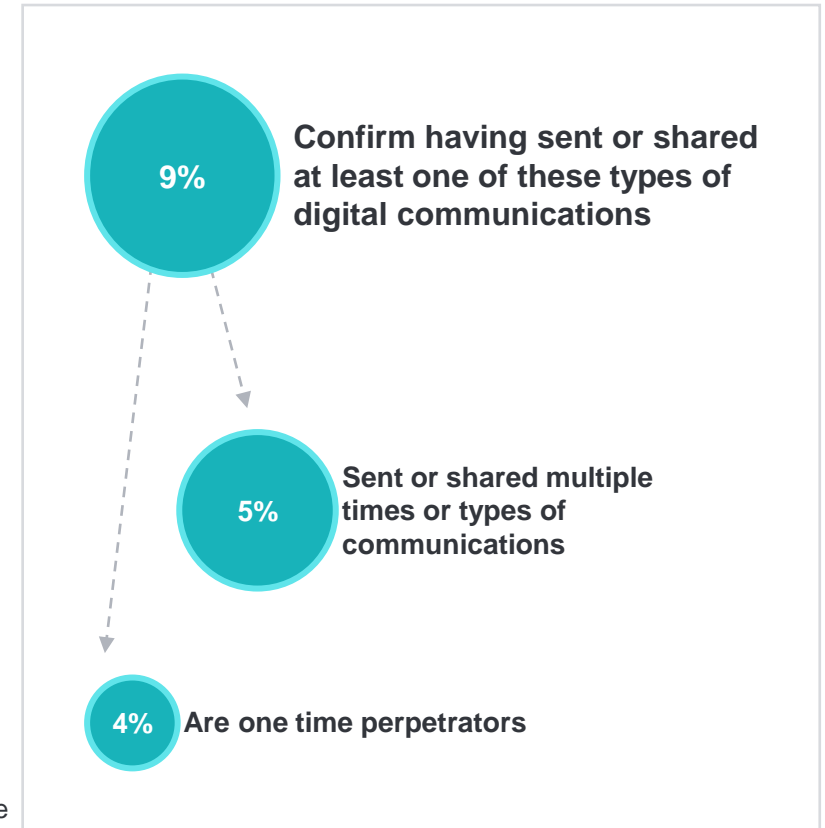


# Perpetrators

# Sending or sharing unwanted digital communications

Nine percent of Māori admit to having sent unwanted digital communications to someone in the past year, and five percent admit to having done it on multiple occasions.

## Sent or shared digital communication(s) that...

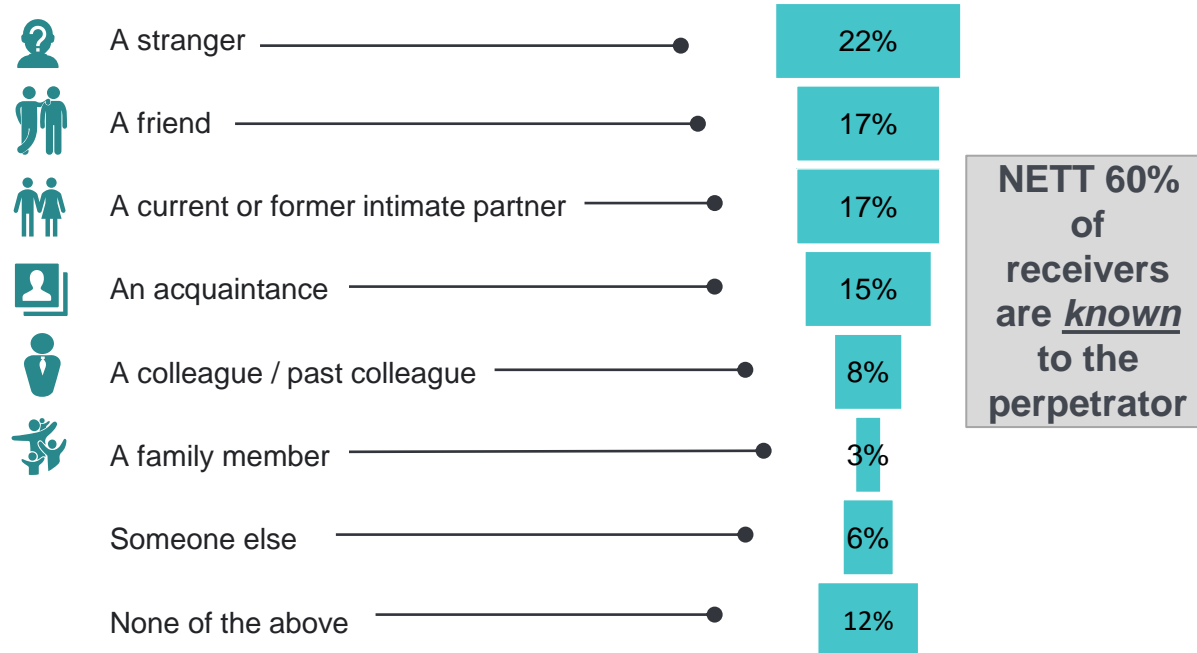




# Proximity to victim of unwanted digital communication and connection to offline events

Receivers of unwanted communications are almost three times as likely to be known by the perpetrator (60% are either a friend, family member, current or former partner, acquaintance or colleague) than to be a stranger (22%). 38% of the time, the communications were part of a wider issue offline.

## Receiver of unwanted communication(s)



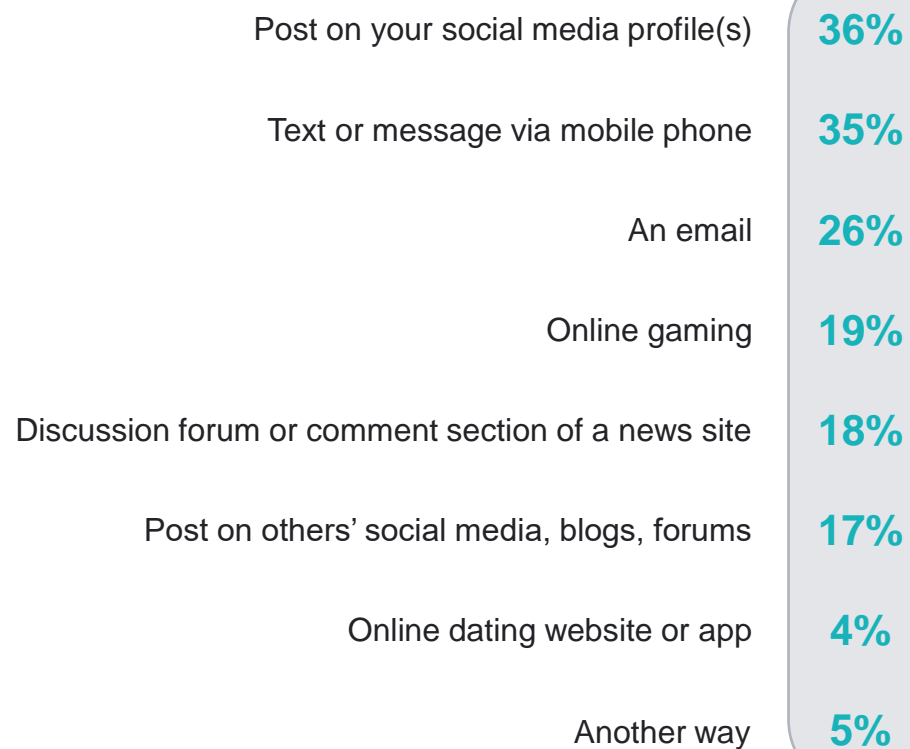
## Online actions part of a wider issue happening offline



# Channels and reasons for unwanted communications

Social media, text, and emails were the most common communication methods used by perpetrators. Most cited reasons for sending unwanted communications include *revenge*, *to make a joke*, or to *embarrass their victim*.

## Communication method used

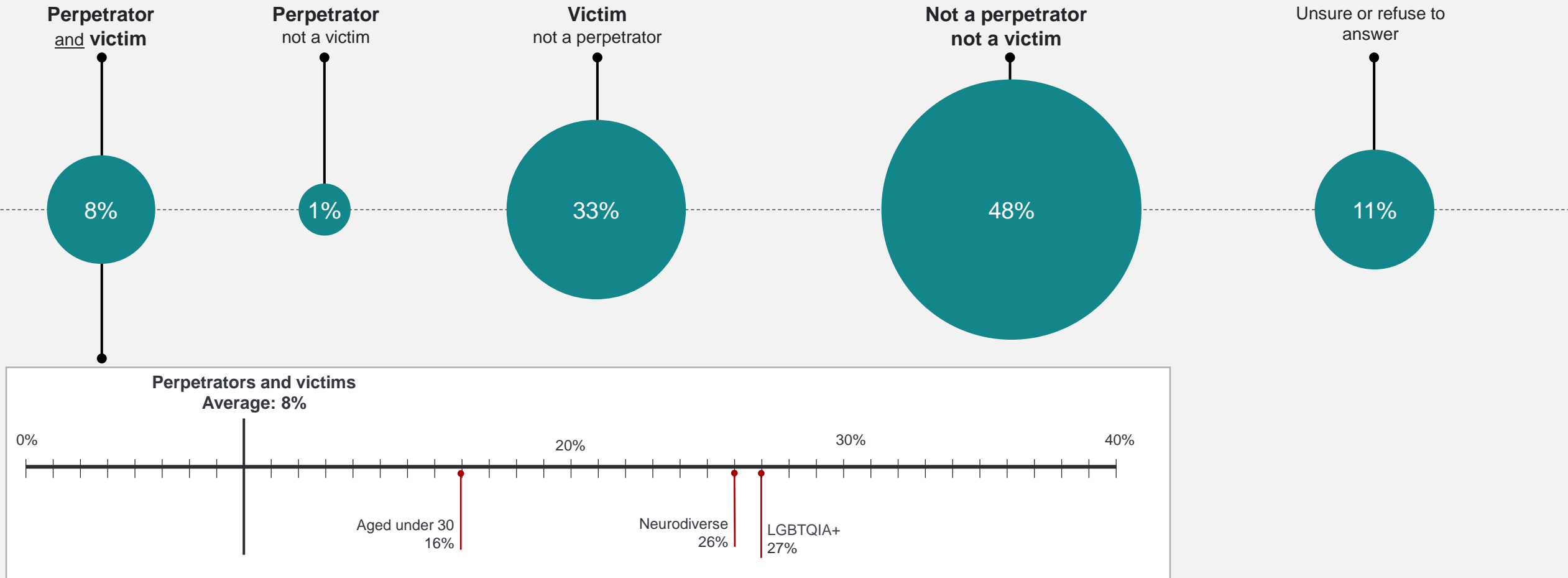


## Reason for communication



# Overlap between victims and perpetrators

Most perpetrators are also victims of digital harm. Younger Māori, those who identify as neurodiverse, and who are LGBTQI+ are all more likely than average to be both victims and perpetrators.



\* Caution small base size – results are indicative only.

Base: All Māori respondents (n=518)

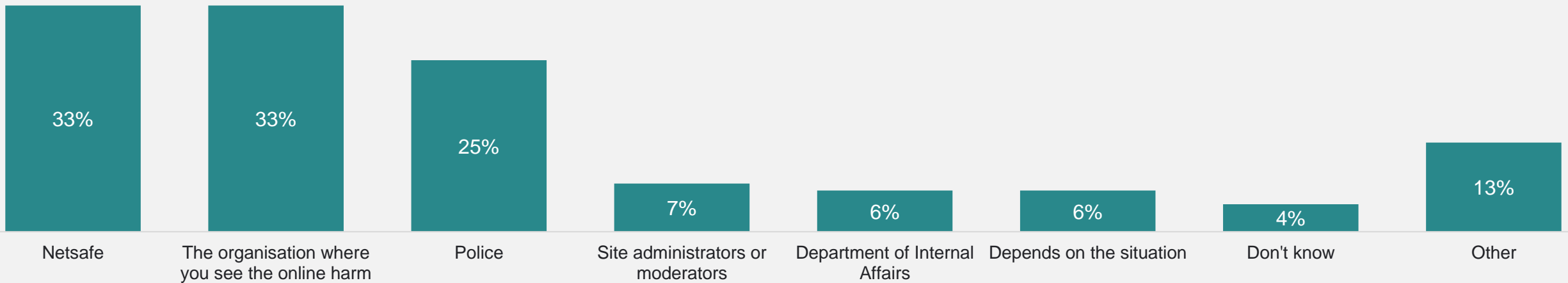
Source: Q54. In the last 12 months, have you personally sent or shared a digital communication (e.g. email, text, photo, video, or online comment) that: Q18. In the last 12 months, have you personally received an unwanted digital communication (e.g. email, text, photo, video, or online comment) that...

# Reporting harmful content

# Knowing where to go

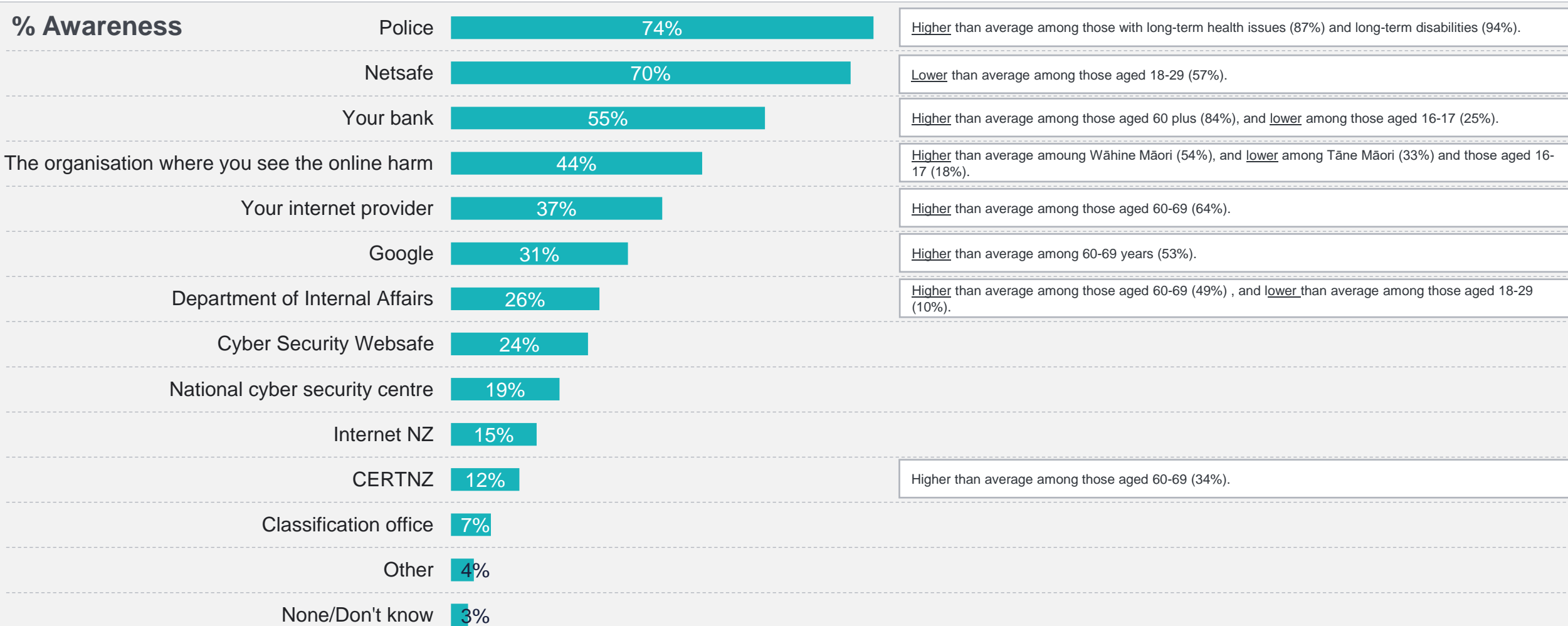
A third of Māori who knew where to report unwanted digital communication would turn to Netsafe, or the organisation where they saw the content. One in four would turn to the Police.

## % Recall



# Awareness of organisations for reporting harmful online content

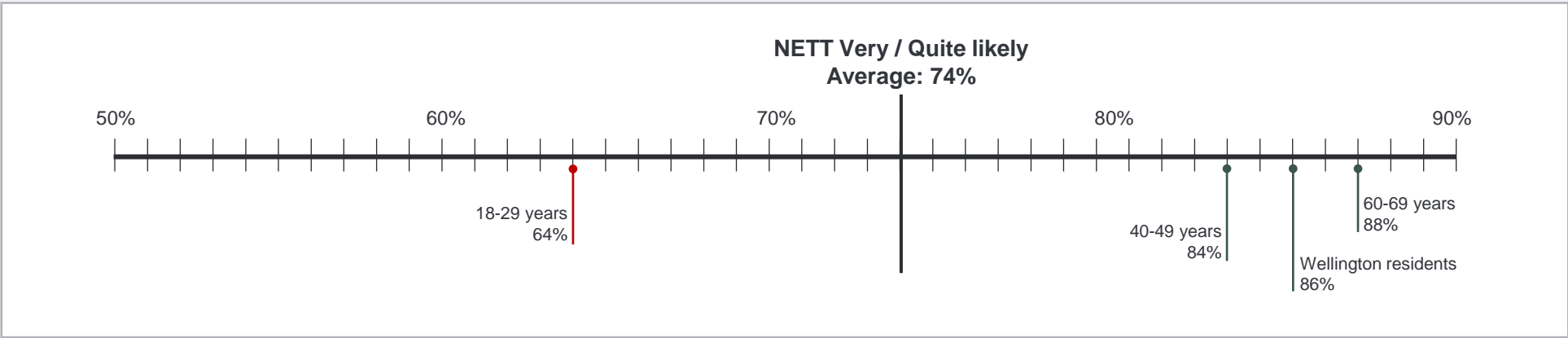
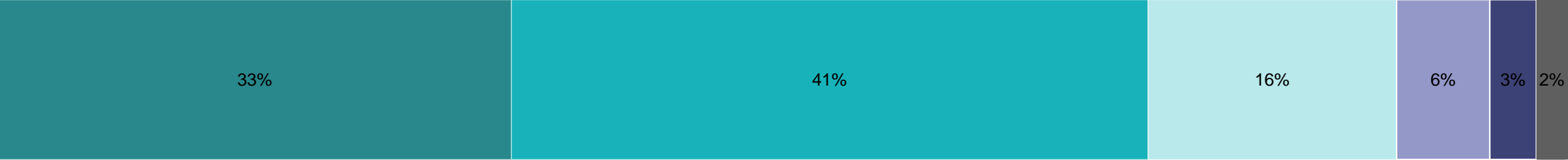
Most recognise the police (74%) and Netsafe (70%) as places to report online harm. Banks are another known organisation for reporting online harm, particularly amongst older Māori, who tend to be aware of multiple organisations to report online harm.



# Likelihood to report harmful online content

Three quarters of Māori are likely to report harmful online content. Middle aged and older and those living in Pōneke are more likely than average to report while those aged 18 to 29 are less likely to do so.

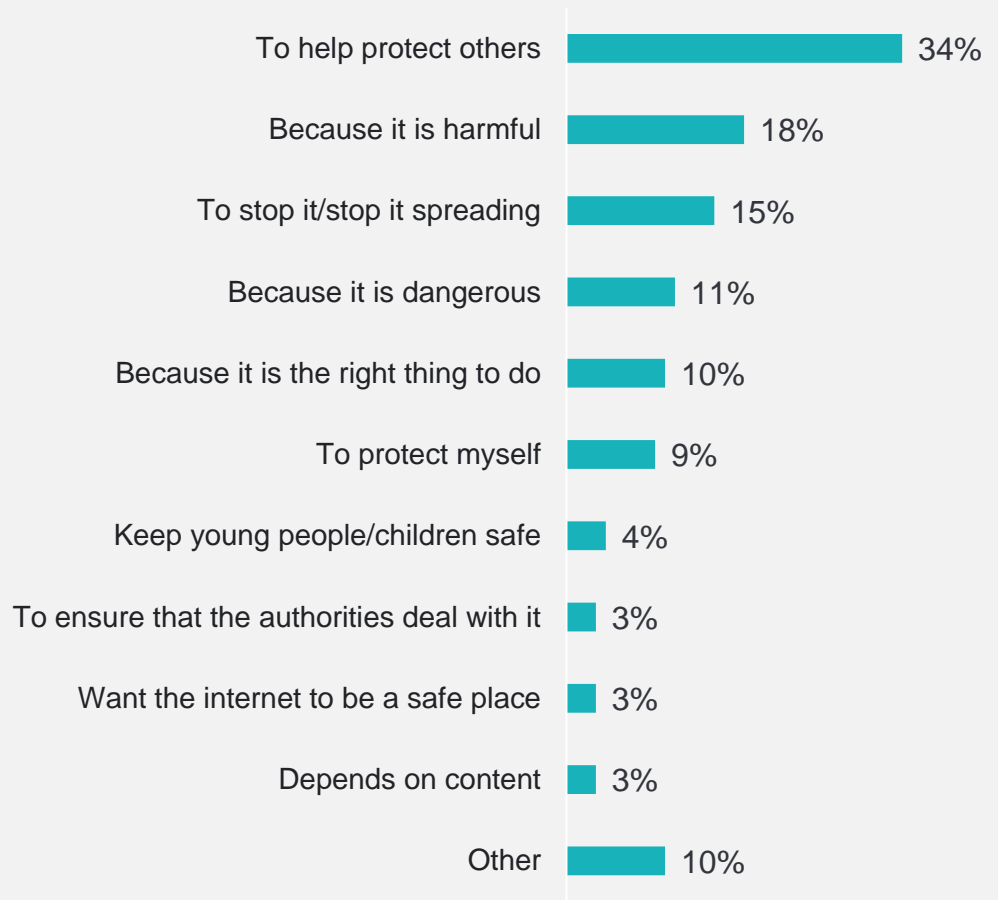
■ Very likely  
 ■ Quite likely  
 ■ Neither likely nor unlikely  
 ■ Quite unlikely  
 ■ Very unlikely  
 ■ Not sure



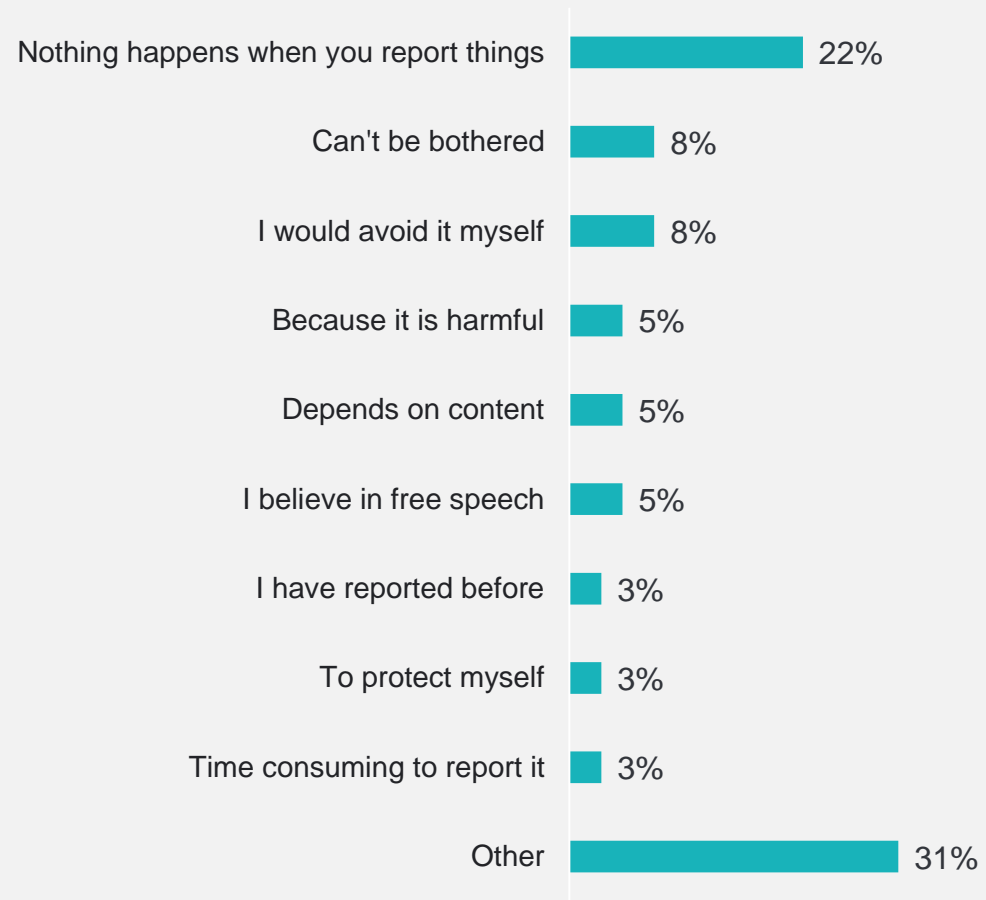
# Reasons for being likely or unlikely to report harmful content

Of those who are likely to report online digital harm the main reason for doing so is to *protect others*. Many see it to be *harmful / dangerous*, and others would report it to *protect themselves*, to help *stop it from spreading*, or because it is the *right thing to do*. The main reason some people are unlikely to report harmful content is because they believe *nothing ever happens when you report things*.

## Reasons likely to report



## Reasons unlikely to report





**FOR FURTHER INFORMATION PLEASE CONTACT:**

**Gabrielle Po Ching and Alexis Ryde**

Kantar Public  
Level 9, Legal House, 101 Lambton Quay, Wellington  
PO Box 3622, Wellington 6140

Phone (04) 913 3000  
[www.kantarpublic.co.nz](http://www.kantarpublic.co.nz)

# IMPORTANT INFORMATION

## Research Association NZ Code of Practice

Colmar Brunton practitioners are members of the Research Association NZ and are obliged to comply with the Research Association NZ Code of Practice. A copy of the Code is available from the Executive Secretary or the Complaints Officer of the Society.

### **Confidentiality**

Reports and other records relevant to a Market Research project and provided by the Researcher shall normally be for use solely by the Client and the Client's consultants or advisers.

### **Research Information**

Article 25 of the Research Association NZ Code states:

- a. The research technique and methods used in a Marketing Research project do not become the property of the Client, who has no exclusive right to their use.
- b. Marketing research proposals, discussion papers and quotations, unless these have been paid for by the client, remain the property of the Researcher.
- c. They must not be disclosed by the Client to any third party, other than to a consultant working for a Client on that project. In particular, they must not be used by the Client to influence proposals or cost quotations from other researchers.

### **Publication of a Research Project**

Article 31 of the Research Association NZ Code states:

Where a client publishes any of the findings of a research project the client has a responsibility to ensure these are not misleading. The Researcher must be consulted and agree in advance to the form and content for publication. Where this does not happen the Researcher is entitled to:

- a. Refuse permission for their name to be quoted in connection with the published findings
- b. Publish the appropriate details of the project
- c. Correct any misleading aspects of the published presentation of the findings

### **Electronic Copies**

Electronic copies of reports, presentations, proposals and other documents must not be altered or amended if that document is still identified as a Colmar Brunton document. The authorised original of all electronic copies and hard copies derived from these are to be retained by Colmar Brunton.

Colmar Brunton™ New Zealand is certified to International Standard ISO 20252 (2012). This project will be/has been completed in compliance with this International Standard.

