verian

Summary Report: Cyber Security Behaviours in Australia

Summary Report: Outline of key findings from research conducted for the Australian Government to inform the development of a communications strategy on cyber security behaviours in Australia

C301008140

Prepared June 2026

Contents

Introduction **3**
Background 3
About this summary report 3
Executive Summary **4**
Key Insights **5**
Reduced urgency and inconsistent action 5
Behavioural vulnerability was widespread, driven by inconsistent behaviours, contextual decision-making and different underpinning mindsets 6
Behaviours were dominated by a 'two tier' system of assessing risk and context 7
The barriers and motivators to address 9
The key implications for communications and behaviour change 10
Specific findings: 'at risk' and vulnerable audiences 11
Appendix **12**
Research approach, methodology and interpretation 12

Introduction

Background

For most Australians, being online is integral to our lives, and is often deeply embedded into how we live, communicate, transact and socialise. As recognised in the *2023–2030 Australian Cyber Security Strategy* (the Strategy), cyber security is a whole-of-society challenge, rather than a purely technical or systems-led issue, with responsibility shared across government, industry, businesses and individuals. Strengthening the capability of Australians to protect themselves online is therefore a central pillar of national policy. A secure digital environment is not only critical to protecting individuals, but also to maintaining trust in online services, supporting productivity, and enabling continued growth of the digital economy.

While cyber security represents a systemic challenge, many of the most effective protective actions still sit at the individual level; such as maintaining strong and unique passphrases/passwords, using controls such as multi-factor authentication (MFA), updating software, and recognising/reporting suspicious activity. However, these behaviours are not yet consistently embedded in everyday life, and many Australians find cyber security difficult to think about and navigate, and safe practices are not always front of mind. Against this backdrop, the Strategy recognises the need for sustained, long-term awareness-raising activity to change and build resilience over time.

About this summary report

Mixed methods developmental/exploratory research was undertaken across December 2024 and January 2025, with an additional module of quantitative research undertaken in August 2025 to further understand the impacts of cybercrime on Australians and the prevalence of behaviours that expose people to risk. For further background, the Appendix of this report provides greater details on the research design, data collection, methodology and notes on interpretation.

This summary report focuses on the key audience-led insights which were used to progress continued communications with the Australian public about the topic of cyber security, and the key communication and behavioural levers needed to support sustained, protective behaviour change.

The overall trends, behavioural dynamics and insights across the Australian community are expected to be broadly relevant to stakeholders seeking to strengthen cyber security education, behavioural interventions, regulation and service design across a range of contexts.

Executive Summary

Across the community, several overlapping, mutually reinforcing dynamics were influential in shaping how Australians thought and felt about cyber security, and in turn, the behaviours that they did or did not put in place in practice.

While the community was not ignorant or fatalistic, and awareness of 'what to do' was generally high, a number of key perceptions and external/contextual influences were present, which acted to suppress willingness and the ability to consistently engage in cyber secure behaviours.

The key or core behavioural and attitudinal dynamics included:

- **Reduced sense of personal agency**
  As stronger cyber security protections were becoming increasingly 'built-in' to many critical services and digital/online platforms, responsibility was perceived to subtly shift away from the individual, and towards service providers and businesses. This had the tendency to reduce the perceived need to proactively know or do more (beyond what systems already required or were perceived to 'mandate').

- **Complexity and cognitive burden**
  Cyber security was widely seen as important, but also technical, difficult to maintain, and effortful. The core challenge was not simply understanding individual actions to take, but in practice, maintaining them consistently across a growing number of accounts, devices and interactions.

- **Fragmented framing of the issue**
  People were more likely to think in broader terms about staying safe online (of which cyber security was seen as just a component) meaning that a conventional framing or way to talk about the issue could feel limited, or risk reinforcing perceived barriers about cyber security being complex and technical.

- **Desensitisation and low proactive engagement**
  Awareness of cybercrime was relatively high, but this often did not translate into active information-seeking or preventative action unless prompted by a breach, a warning or a system requirement.

- **Reactive rather than preventative habits**
  Protective action was most often triggered by external prompts rather than sustained habits built up as routine. This left people more likely to respond 'in the moment' or make trade-offs or choices to maximise speed or convenience, rather than always building and maintaining repeatable habits that reduce risk over time.

- **Behavioural vulnerability heavily influenced by context**
  Behavioural vulnerability was widespread across the population, with most Australians (87 per cent) falling into moderate or higher vulnerability segments when assessed against the consistency of their actual behaviours. In practice, this reflected a strong 'two tier' pattern, where people were much more likely to apply protections in high-stakes settings such as banking or government services, but more likely to deprioritise safety in everyday contexts such as social media, online shopping or public Wi-Fi.

The main implication is that to make Australians safer in practice, there is a need to rebuild agency, find ways to simplify the behavioural 'ask' and make it feel achievable, and encourage more consistent actions across the full range of people's digital lives.

Key Insights

Reduced urgency and inconsistent action

In late 2024, when primary research commenced, it followed on from several high-profile national data breaches and cyber incidents which had impacted millions of Australians in the preceding years (including but not limited to large scale breaches impacting telecommunications and health insurance customers).

> ***"It makes me feel really helpless… it's happened twice now, information leaked to [the] dark web… it really sucks because it's not vanity-based products or services and so I feel helpless and disheartened and like it is just an inevitability nowadays… even though these massive companies [are] investing millions they can't even protect me and I'm doing all the right things."***

While these incidents remained salient and memorable across the community, these were also increasingly perceived as 'historical'. The scale and breadth of these breaches - having affected millions of Australians – also impacted on sentiment in an apparently confounding way. Repeated exposure to information about systemic cybercrime, interacting with other ways that people were exposed to the issue, had not necessarily created urgency, but instead a degree of desensitisation, diminishing self-efficacy, and a low sense of control:

> ***"We never really see [it]…I mean, we hear of these scenarios where things are being hacked, but really, I've never seen or felt [it or] been shocked by actually seeing it really happen, like hearing the stories of hackers who do it, so it still feels very distant."***

> ***"Why would they go after me when there's banks or those big companies with so much more?"***

The issue was also not fundamentally about low awareness or exposure: as at August 2025, 41 per cent of Australian adults stated that they had personally experienced a cyber incident or actual cybercrime. Among those personally impacted, scam texts, emails and phishing attempts (45 per cent), compromised personal data due to data breaches (37 per cent), loss of money (31 per cent), or hacked online (22 per cent) or social media accounts (19 per cent) were most common.

While most Australians recognised cybercrime as a growing and worrying issue, it was also often seen as an inevitable feature of modern life. This drove a very clear norm: while people were not deliberately choosing to be complacent, the broader context could leave space for people to question the purpose of why they should do more, within a domain that could often feel technical, complex and hard to stay on top of. Additionally, it placed the issue in a more reactive space, where engagement was generally more passive, and likely to be triggered by external events.

> ***"A lot of the advice I get, I'm not looking for it… I see something pop up on social media or my bank makes me do something I didn't have to before… or someone changes their terms and conditions, only then would I actually engage with it."***

Behavioural vulnerability was widespread, driven by inconsistent behaviours, contextual decision-making and different underpinning mindsets

Qualitative data demonstrated that despite a widespread desire to be cyber secure, behavioural impediments and points of friction made it harder for Australians to consistently adopt behaviours that would improve their cyber safety or reduce their risks across a complex mix of digital environments, devices and settings. To support understanding and knowledge of the audience, a security vulnerability index was used as part of the research, in order to fully understand 'real world' patterns of behaviour across people's digital and online lives. As opposed to simply asking people about their own self-perceptions, attitudes, beliefs or risk factors (which introduces the possibility that respondents cannot reliably self-assess their own level of risk), the index focused on adoption of cyber security behaviours in practice.

In short, the index sought to understand across the population:

- what steps to stay cyber secure were people actually undertaking?
- how frequently were people actually maintaining cyber safe behaviours?
- were people more or less consistent or inconsistent in how they apply controls and protections, and if so, in what contexts or situations?
- what were the moments or choices where people were tolerating risk and/or potentially exposing themselves to higher risk across their digital lives?

When mapped against this index, only a small minority of Australian adults (13 per cent) were in the 'low vulnerability' category (meaning they were very regular in maintaining key protective behaviours, and mostly or almost always avoided risky behaviours, or contexts that can create a higher risk of falling victim to cybercrime). In contrast, a much higher number (44 per cent) of adults were indexed as moderately vulnerable, and a similarly sized cohort (42 per cent) indexed as high vulnerability. Moderate and higher vulnerability effectively meant increased exposure to risk in two related ways: overall, it aligns to a lower frequency of regularly undertaking key protective behaviours, paired with a higher tendency to act in ways that are known to increase exposure to digital/cyber risk (e.g. using unsecured public Wi-Fi, turning off security settings to access certain online content, deprioritising data protection in social media accounts, etc). Analysis and triangulation of data showed that the emotional drivers that sat behind this were complex – with four distinct prevailing emotive mindsets about cyber security present across the Australian community:

- *Helpless:* People whose primary barrier was low motivation/low sense of purpose; believing that whether or not they could fall victim to cybercrime was beyond their immediate control, often leading to disengagement and low information seeking.
- *Denial:* People with this default mindset didn't dispute the severity or risk of the issue, but tended to hold the belief that they didn't have much to lose financially/online, and couldn't imagine being targeted by cybercrime.
- *Overconfident*: People in this cohort were typically the most knowledgeable about what to do in practice, but they had a strong tendency to cut corners, seek convenience, or make trade-offs around riskier behaviours in some contexts.
- *Overwhelmed:* This segment comprised more basic users of technology who were often older; they could feel intimidated and overloaded, often meaning that instead of trying to upskill, they were choosing to move to 'offline' or use other behaviours to minimise their exposure to online risks.

Behaviours were dominated by a 'two tier' system of assessing risk and context

Being safe and cyber secure remained important to Australians, but it was clear that strong contextual and situational cues were significant in shaping people's mindsets and behaviours in practice.

Even among those who strongly valued being safe online, there was a tendency to apply behaviours or protections selectively, depending on whether a situation or interaction felt more or less important, risky or consequential. This produced a clear and very strong 'two-tier' behavioural pattern, where risks might be recognised, but compartmentalised into 'mandatory' versus 'discretionary/optional' behaviours or protections:

- Almost universally, people reported that they were much more cautious and diligent in contexts perceived as high stakes, such as banking, government services or using work-related systems (including where other people's data or information might be at risk). These were also the 'places' that also tended to feel inherently safer, by virtue of many services and platforms requiring people to actively employ or 'turn on' features such as multi-factor authentication, enforcing more complex passwords, etc.

- However, in contexts or environments perceived as more routine, lower value or lower consequence, such as social media, email, online shopping or decisions to use public Wi-Fi, Australians were more likely to seek convenience/speed, reuse or employ low complexity passwords, and/or to deprioritise other protective behaviours. This is likely because the behavioural friction associated with being cyber secure can feel even more noticeable in 'lower stakes' contexts or digital interactions. Some of this behaviour was conscious and driven by context, although part of the decision-making was also driven by automatic mental shortcuts (i.e. automatic appraisal, along the lines of: 'what I do in social media is unrelated to my overall cyber security').

A key impact is that many people did not implicitly connect that being more vulnerable in 'low stakes' contexts might introduce risk in the 'higher stakes' parts of their lives – such as their identity, finances, devices or other important personal data being compromised.

> ***"I would probably say with the more important sort of stuff, like myGov [Australian Government's online service platform], I'm probably pretty good, but a lot of the other stuff, like online shopping…I'm like, meh, I use all the same passwords."***

This mindset sometimes drove higher risk behaviours, and was often self-reinforced or exacerbated by confidence that stronger systems, and platform-level protections were already providing sufficient protection in some settings.

> ***"MFA is compulsory most of the time… the sentiment is good but the behaviour may not be relevant … is there something else we have more control over?"***

In practice, the most frequently implemented practices and behaviours tended to be more visible, immediate and often linked to times when systems or contextual cues prompted or forced behavioural consideration. These also tended to be things/steps that people could easily anchor as clearly linked to their device or cyber security, and which they can do reasonably quickly/immediately:

- thinking carefully before clicking links/attachments (81 per cent of adults do this all or most of the time)
- locking devices with a PIN/passphrase (73 per cent of adults do this all or most of the time)
- installing software updates (72 per cent of adults do this all or most of the time)
- using multi-factor authentication when it is available (66 per cent of adults do this all or most of the time).

By contrast, behaviours that required more ongoing effort, maintenance, or proactive management were less common. These included much lower levels of agreement that people undertake these steps all or most of the time:

- setting up automatic backups / software updates (43 per cent)
- checking and updating privacy or location settings (41 per cent)
- using a password manager (35 per cent).

While Australians strongly agreed that key behaviours such as using strong passwords (86 per cent), enabling MFA (83 per cent) and securing devices with passwords (81 per cent) would be effective in protecting their cyber security, over half of people (55 per cent) admitted to regularly or occasionally using the same password across multiple accounts or using variations of the same password across accounts and services (59 per cent). Behaviours relating to data exposure in social media emerged as another key potential area of vulnerability, likely because the platforms themselves are perceived as personal, 'low stakes', and because there are few external cues or prompts that immediately tie these environments back to cyber security. When asked what a cybercriminal could potentially find after spending five minutes on their social media accounts, nearly two thirds of adult Australians (64 per cent) said that personal details could be readily identified, including:

- their birthdate (32 per cent)
- family members' names (29 per cent)
- email address (28 per cent)
- partner's name (26 per cent)
- their school or workplace (26 per cent).

The barriers and motivators to address

Across the community, although there were clear emotive and behavioural barriers, positively, there were also a number of clear potential motivators that are present which can be used to influence behaviours.

In qualitative discussions with Australian adults, a clear theme was that the immediate experience of being or feeling 'safe' versus 'vulnerable' to cybercrime was often difficult to distinguish in the moment. In short, this meant people tended to anchor more readily to the visible effort, and perceived inconvenience of putting protective cyber security steps into practice. In many cases, this was paired with the lack of a strong feedback loop (there can be an absence of visible or immediate signals to confirm, one way or another, if putting cyber security behaviours into practice is actually beneficial or worth the effort).

> ***"It's time consuming, like when it should be a more than 15 characters password… I won't remember it, that's a hurdle."***

The impact is that some in the community struggled to see a purpose in 'doing more' to be cyber secure. As at August 2025, almost 1 in 4 Australians (22 per cent) said it was unlikely they would be targeted in a cyber-attack, with this mindset even more pronounced among young people aged 18-24, where over a third (36 per cent) discounted the overall level of threat.

> ***"I guess in my head … [being targeted by a cybercrime] it's not very likely …because I don't have any personal experience of it happening. If you're just doing basic things, you're not at risk."***

Ultimately, the most important barriers in practice were that:

- risks were often discounted by immediate context
- motivation could be impaired by inevitability and lack of a perceived 'pay-off', often leading some to question if 'doing more' would make a meaningful difference
- the perceived effort in either learning about and regularly maintaining cyber security practices could feel behaviourally difficult and burdensome.

As noted, the dominant community norm was often to see cyber secure behaviour as more important and essential in high-risk settings, but perhaps optional or discretionary in other circumstances.

Overall, these barriers are not insurmountable, and research evidence pointed to a clear set of potential motivators. As a rule, it was clear that the community are likely to be more receptive and oriented to take action when:

- communications or messaging makes the consequences of inaction feel more tangible
- lower efficacy is addressed head on, by demonstrating that cybercrime is not inevitable, and that individual actions and choices are still powerful in reducing risk
- the overall behavioural 'ask' is made to feel simple, non-technical and actionable (i.e. by being clear that a relatively small, repeatable set of actions can be effective in changing the chances of information, identity or finances being compromised).

The key implications for communications and behaviour change

The audience-led insights from research suggest a set of key principles to support Australians to improve their cyber security behaviours, taking into account that many adults:

- often display uneven protective behaviours
- may not be highly engaged, or proactively looking for more information
- are often highly reliant on external prompts and situational cues to shape their choices or behaviours
- are often impeded by the belief that cyber secure behaviours are burdensome, complex and difficult to maintain.

As such, the challenge is not simply to improve overall awareness of the issue ('knowing what to do'), but also to address the underlying behavioural dynamics that shape how people act in practice.

1. **Re-establishing purpose and agency**
   To counter a topic that is often perceived as technical and daunting, reinforcing that relatively 'small' individual actions will make a meaningful difference can help to motivate people, even in a complex threat environment.

2. **Driving consistency across contexts, by demonstrating consequence**
   There is a strong tendency to treat some online environments as lower risk and therefore less deserving of protection. A key principle is therefore to educate people about how 'low risk' decisions can translate to exposure in 'higher value' parts of their lives, and without catastrophising, being clear about the realistic consequences they might face.

3. **Simplifying the behavioural ask to disrupt the idea that cyber security is complex and burdensome**
   Many Australians assume or believe that everything they would need to do to be cybersecure is too hard to do consistently, which can erode their sense of purpose. However, it was clear that where people are exposed to behavioural modelling (such as showing how achievable but high impact 'protective' actions can be built into everyday routines), this can help to re-inspire confidence and motivation.

4. **Leveraging moments of risk and relevance**
   Many Australians are not proactively looking for more information about cyber security, meaning that general risk-based or prevention messages are not always highly memorable at the point that decisions are made. Certain higher risk decisions tend to occur spontaneously, often without people seeing the real risk equation or trade-off that might sit behind a particular choice or behaviour. A key principle is that attention and salience can be gained by linking cyber security messages within potentially 'riskier' situations, contexts, moments and triggers where people tend to prioritise speed, convenience and/or use behavioural shortcuts.

5. **Using audience language / framing to reframe complexity**
   Framing the issue around staying safe or secure online aligns to how most Australians see the topic (cyber security is often not seen as the only thing that they need to think about when online). As a rule, anything that uses technical or narrow language, or imagery that is risk-based but which confirms inevitability (for example, depicting the sophistication of 'hackers') can make the issue feel distant, too complex or alienating.

Specific findings: 'at risk' and vulnerable audiences

The prevalence and drivers of cyber vulnerability are not necessarily distributed evenly across the community. The research therefore included specific approaches to include a number of 'at risk' or potentially more vulnerable audiences, to understand any key differences in sentiment, beliefs or behaviours.

At a population level, it was noticeable that the key norms and beliefs that impaired confidence, reduced perceived personal relevance, and limited consistent protective behaviours were broadly held in common across most parts of the community. Where some differences in outlook or behaviour were present, these were typically driven by contextual, structural or situational factors (in short, these differences are less about the inherent characteristics of any cohort/group, and more about the particular circumstances or structural drivers that sit around their lives):

- **Culturally and linguistically diverse communities (CALD)**: People from CALD backgrounds were not uniquely at risk, but for some, vulnerability tended to be heightened by language barriers, newer engagement with Australian systems, and a need to interact with products or services that are potentially newer or unfamiliar.

- **Older Australians**: many were likely to feel intimidated by the online environment, which could reduce confidence and discourage engagement, although this group also tended to be more highly self-aware, showing openness to learning and self-protection, and often higher degrees of caution when unsure.

- **First Nations Australians**: there was no consistent evidence of fundamentally different attitudes to cyber security, but structural factors such as poor access to services and remoteness can see a necessity for frequent and widespread sharing of devices across family and community, therefore creating greater risks. For example, First Nations Australians in very remote areas are often sharing devices out of necessity, rather than as an optional or discretionary behaviour.

- **Lower income audiences (household incomes of less than $50,000)**: cost barriers appeared less prominent than in the past (likely due to many in this audience benefiting from strengthened cyber protections available at no additional cost, often within platforms, products or services). Although not unique to this group, a strong sense of having less to lose or being a 'small target' played a role in eroding motivation to be more cyber secure.

- **People living with disability** were more likely to express somewhat more fatalistic attitudes about the inevitability of cyber attacks, lower levels of proactive behaviour, but also stronger assumptions or beliefs that devices or platforms would provide protection.

Appendix

Research approach, methodology and interpretation

Data collection used a mixed-methods approach combining qualitative and quantitative methodologies to provide a comprehensive understanding of community attitudes, behaviours and vulnerabilities in relation to cyber security.

Qualitative research involves structured discussions with small groups of people. The nature of this type of research is that it is designed for 'discovery': it is a powerful technique to elicit and discern key themes, beliefs, barriers and motivations that are likely to be present across populations of interest. Illustrative, de-identified quotes from participants have been included in this report (while they are verbatims from a single individual, they represent beliefs, behaviours, mindsets, attitudes or sentiment that were commonly held or observed across the Australian adult community).

The initial developmental qualitative phase (December 2024-January 2025) comprised over 100 hours of engagement with members of the Australian community, including 67 participants across 12 online focus group sessions. Sessions were structured to capture a diversity of experiences across metropolitan, regional and remote locations, and were further segmented by life stage (e.g. 18–35 years, 36–64 years, 65 years and over). A small number of depth interviews (private, one on one interviews) were conducted with representatives from multicultural and community organisations, including service providers and community liaison roles, to provide expert perspectives on the needs and vulnerabilities of new and emerging CALD communities. Focus groups were used to ensure inclusion of the following audiences of interest:

- General population (i.e. from households where the main language spoken at home is English)
- CALD communities (including both English-speaking and in-language participants)
- First Nations Australians
- People living with disability
- Older Australians (65+)
- Lower-income households.

Quantitative research: Quantitative data is statistical and survey-based. For this project, initial quantitative research was used to measure and assess key issues and themes that emerged out of qualitative discussions, and to index the population in terms of actual behaviours and potential vulnerability. A second phase of quantitative data collection was also used to gain more granular insight into cyber security behaviours and prevalence, including impacts on people who had experienced incidents or exposure to cybercrime.

The initial national quantitative survey of 2,042 Australians aged 18 years and over was designed to validate and quantify observed patterns in attitudes, behaviours and vulnerability from qualitative fieldwork, and to segment or index the community in terms of their risk profiles. A sample of this size has a maximum margin of error of +/-2.17%. The survey was conducted online in December 2024 using a nationally representative sample, with quotas applied across key demographic variables including age, gender and location (state/territory and metropolitan versus regional areas). Additional representation was ensured for priority groups, including CALD audiences, First Nations Australians, older Australians and lower-income households. Data was post-weighted to reflect the Australian population, based on ABS Census data from 2021. Weights were applied by:

- Age within gender
- State and Territory
- Metro versus regional areas
- Aboriginal and Torres Strait Islander (First Nations status)
- Culturally and linguistically diverse people.

A second wave of quantitative data collection involved a survey of 2,074 Australians aged 18 and over, conducted online in August 2025, which sought to answer additional questions about prevalence, attitudes and behaviours in detail. A sample of this size has a maximum margin of error of +/-2.15%. Nationally representative quotas were put in place for age, gender, and location (state and territory, and metro/regional). As per earlier data collection, it was weighted to reflect the Australian population, based on ABS Census data.

In interpreting references to quantitative data throughout the report (e.g. "x per cent"), readers should note that some percentages may not sum to 100 per cent. This may reflect rounding (all percentages are reported to the nearest whole number), or question sets where multiple responses were collected.

Quality, ethics and participant welfare: All research components were conducted in line with relevant ethical and Australian market research industry standards. Verian maintains ISO 20252:2019 accreditation, which involves regular internal and external auditing and adherence to quality standards. Verian is a corporate member of the Australian Data and Insights Association (ADIA) and The Research Society, and adheres to privacy principles and all industry codes of professional practice of those bodies. Verian's senior practitioners are members of the Research Society, ESOMAR, the Australian Evaluation Society, and other key professional bodies.

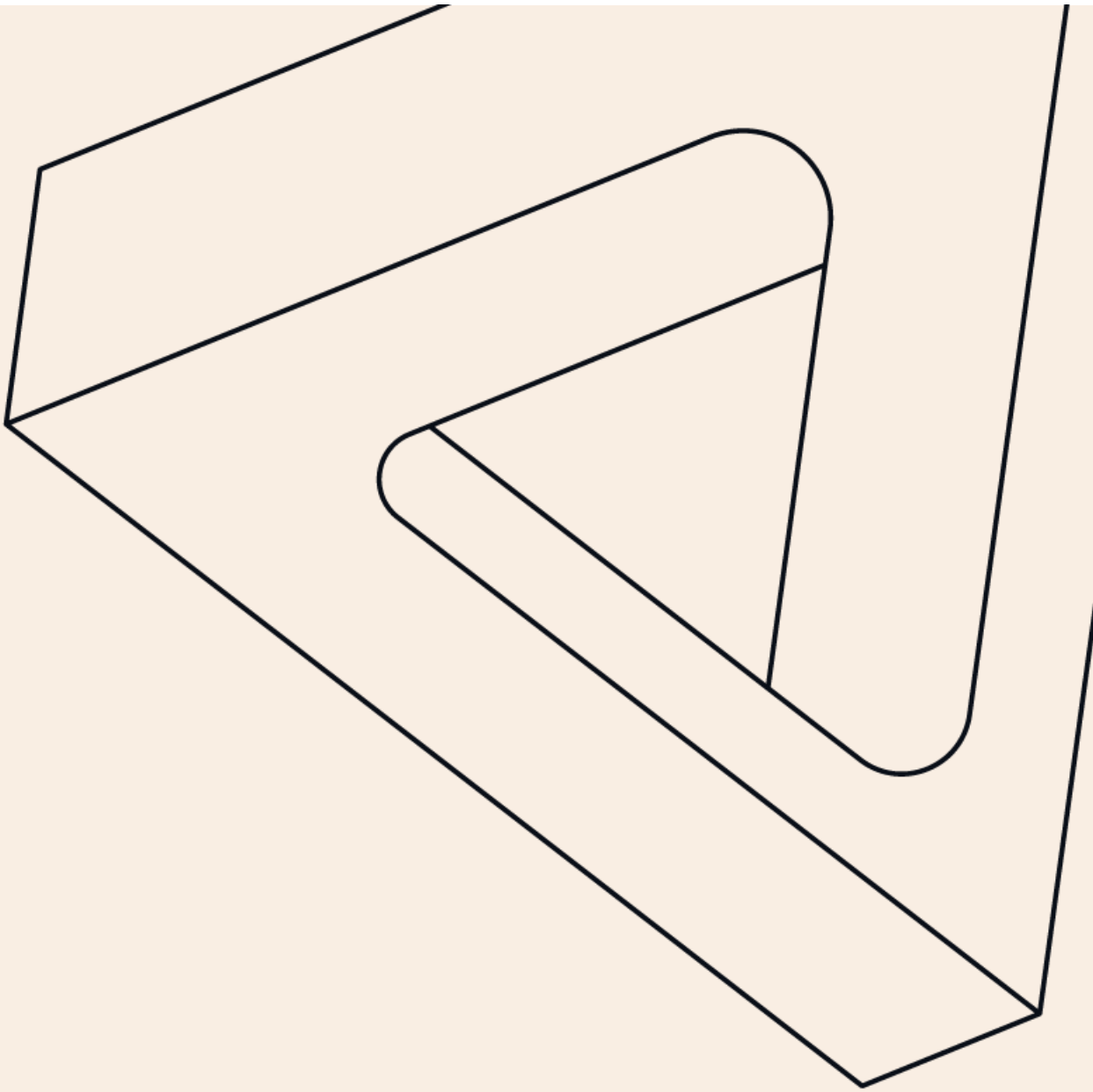
Following the completion of fieldwork, all data and responses were analysed to determine the main themes and issues. Verian's senior researchers drew on the findings, data and evidence from both qualitative and quantitative components to consider their implications in terms of study objectives.

Ethics, consent and participant welfare: Verian conducts research to fully adhere to industry standards and national guidelines on human research[1]. All research components were designed and implemented in such a way as to minimise the risk that participation in research would involve harm (psychologically or otherwise). Informed consent from participants was achieved at all stages. Participants/respondents were treated with dignity, respect and politeness at all times.

[1] https://www.nhmrc.gov.au/about-us/publications/national-statement-ethical-conduct-human-research-2025

verian

Powering decisions
that shape the world.



veriangroup.com/en-au