



Digital Lives of Australians 2026

How Australians use, trust and
navigate the internet in 2026



Contents

Introduction	3
Value of the internet	5
AI uptake	8
AI regulation	13
Security barriers	16
Threat detection	25
Cyber risks	28
Digital skills	31
Digital ID	36
Insights and considerations	40
Research methodology	43

CEO foreword



Dr. Bruce Tonkin
auDA CEO

The internet underpins modern Australian life – powering businesses, connecting communities, and shaping how we work, learn and access essential services every day.

Now in its sixth year, **auDA's *Digital Lives of Australians 2026* research** demonstrates the **increasing importance of the internet** to the lives of Australians.

This year, 83% of consumers report they could not imagine life without the internet (82% in 2025), and 68% of workers say they could not do their job without it (64% in 2025). For small businesses, digital connectivity is equally foundational: 85% would struggle to operate without the internet, and 56% now have a dedicated website – up from 49% in 2025.

These insights highlight that the internet is undoubtedly essential infrastructure, much like water and electricity. However, with increased reliance on the internet also comes challenges.

Cyber security threats are becoming more frequent and more sophisticated, and many Australians fear financial consequences.

Almost 12% of consumers report losing money to online scams in 2025, while nearly half of small businesses say they feel ill equipped to defend themselves against cyber threats.

While confidence using the internet remains high, this report shows that confidence can mask capability gaps – particularly when it comes to cyber security protections and knowing where to go for trusted advice.

At the same time, Australians are navigating a significant change in how they engage online with the rise of generative and agentic artificial intelligence (AI). **AI use has surged over the past year**, with 61% of consumers (up from 56% in 2025) and 72% of small businesses (64% in 2025) now using it for at least one purpose. Many are already seeing the benefits of AI through time savings and improved problem solving. Yet concerns about accuracy, privacy, misuse and the future of work remain widespread, even among those actively using the technology.

This year's report also explores **Digital Identity (Digital ID), which aims to make verification more secure** and convenient for Australians, yet uptake remains low outside of government services. Many Australians are unsure whether they have a Digital ID, and concerns about data security continue to shape attitudes towards the technology.

When it comes to digital skills, consumer and small business capability varies greatly.

Cyber security and AI are identified as two priority digital skills by respondents. Yet self-reported competence with cyber security remains low, and the uneven uptake of AI risks creating a new digital skills gap.

While the challenges are not insignificant, they also present opportunities to build trust and capability in the online environment. Upskilling in cyber security and AI, and clear messaging on the benefits of Digital ID can help Australians participate online with greater confidence.

Our aim in carrying out the *Digital Lives of Australians* research is to help inform decision makers in government, industry, academia and the training sector and contribute to a stronger digital future for Australians.

This year, we have set out suggestions and practical considerations alongside the research findings. We hope this further supports meaningful discussions and informs new policies and initiatives to provide improved online security, capability, trust and confidence among all Australians.

About the research

This report presents findings from research conducted by SEC Newgate for the .au Domain Administration (auDA), involving Australian adults (consumers) and small business owners and managers (small businesses). It represents the sixth wave of the Digital Lives study, which began in 2021.

In 2026, the survey followed an initial qualitative phase comprising 10 in-depth interviews and eight focus groups. Fieldwork ran from 27 February to 5 March. Final samples were weighted to reflect population profiles: by age, sex, location, education, and workforce participation for consumers, and by industry sector and location for small businesses. The research methodology is set out in more detail on [page 43](#).

Notes for the reader:

Where available and relevant, results from previous Digital Lives surveys have been included for comparison purposes.

Where time series data is reported as “NA”, this indicates that specific question was not asked that year.

Some total or net results may not sum to 100% due to rounding.

Throughout the report these colours are used to indicate findings for consumers and small businesses.

Consumers

Small businesses

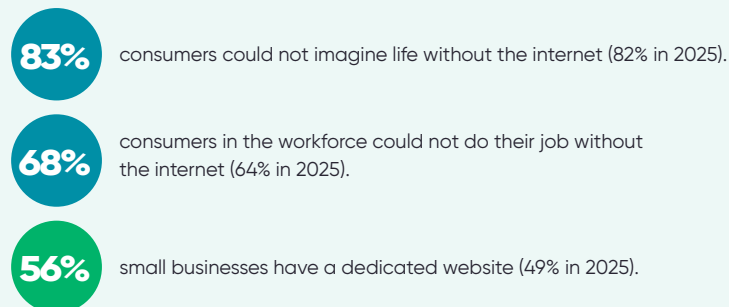


Value of the internet

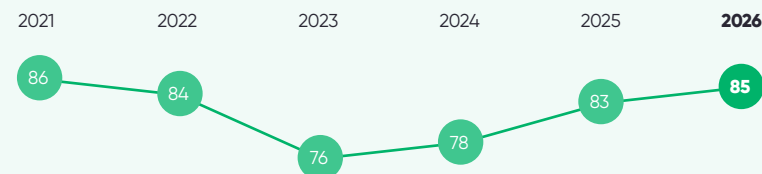
The internet continues to deliver a range of benefits as it becomes more entrenched in our everyday lives

Australians rely on the internet every day to connect with family, friends and community around the world, access information, services and entertainment; and to work. For small businesses, the internet is a critical tool for reaching customers and operating efficiently, both locally and globally.

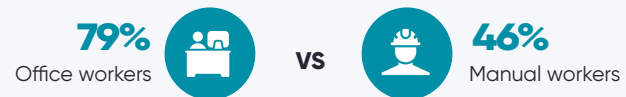
The internet is essential infrastructure in our daily lives and digital communications and continues to become more deeply embedded in economic and social life. With a growing share of workers and small businesses dependent on the internet to operate, it is the backbone of the Australian economy.



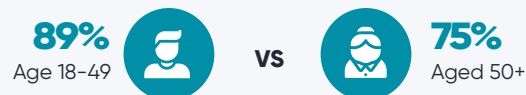
Would struggle to function without the internet (% Small businesses)



Depend on the internet for work (% Consumers)



Unable to imagine life without the internet (% Consumers)



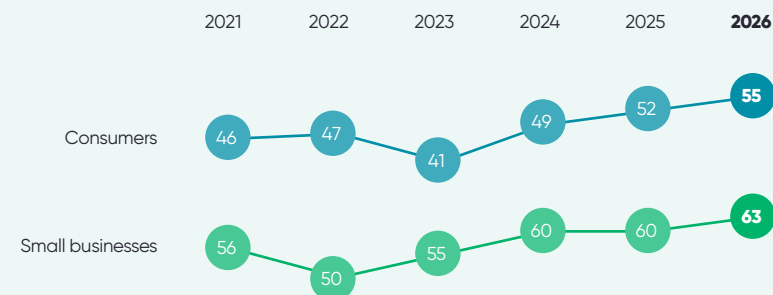
Confidence online is high, driven by everyday use

Australian consumers and small businesses are more confident online than they have ever been. The internet is so entrenched in daily lives that it is second nature for many.

Consumer confidence is largely habitual – shaped by routine use of everyday digital services such as online banking, email and messaging communications, and workplace processes.

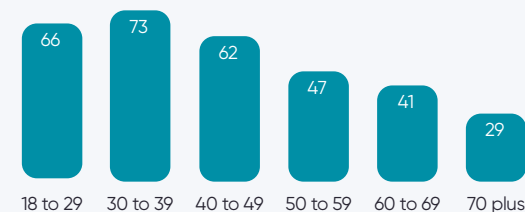
For small businesses, confidence is operational rather than technical – it comes from knowing how to run core business functions online.

Confidence using the internet (% Very confident)



Younger Australians are especially confident online. This may reflect their heavier participation in digital environments across social, work and service interactions.

Confidence using the internet: By age group - Consumers (% Very confident)



Digital lives in focus: Pari



**Female, 35–49,
Perth, WA**

Key points:

- Relies on the internet and digital technology to participate independently in daily life
- Lives with a disability
- Values digital tools for the access, information and autonomy they provide

Pari is blind and uses the internet and digital technology as a core part of everyday life, both personally and professionally. Digital tools like screen readers, AI powered image descriptions, smart devices and accessible apps enable her to navigate the world independently and access information that would otherwise be unavailable. These tools allow her to more easily complete everyday tasks such as shopping, banking and managing her home without relying on others.

Pari finds that well designed digital services create a strong sense of inclusion and trust. Pari consistently returns to brands and platforms that are accessible and easy to use, even when cheaper alternatives exist. In contrast, poor digital accessibility leads her to abandon services altogether or find workarounds.

"I could switch to another bank and probably be better off, but I don't because the accessibility of my current bank's app is great and it's so easy for me to use."



AI uptake

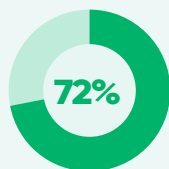
AI use has surged over the past year

An increasing number of Australians and small businesses are embracing AI and usage has moved beyond experimentation to being incorporated into many aspects of everyday life. In 2026, a significantly higher percentage of consumers and small businesses are using AI for work, studies and personal reasons.

Have used AI for any purpose:



Consumers
(56% in 2025)

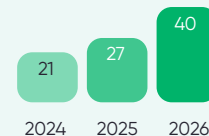
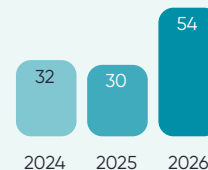


Small businesses
(64% in 2025)

Use AI regularly or occasionally for work (%)

● Consumers

● Small businesses

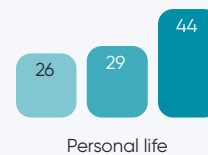


Use AI regularly or occasionally for personal life and studies (%)

● 2024

● 2025

● 2026



Digital lives in focus: Willie



**Male, 18–34,
Regional NSW**

Key points:

- Uses AI regularly in his personal life
- Views AI as a game-changer

Willie has a very active digital life. He uses online apps and platforms to interact with his friends and to build connections with and understanding of his Aboriginal community and issues affecting First Nations communities more broadly.

He has readily adopted AI and uses several AI tools and platforms, for various purposes. For example, he has used AI to generate holiday plans and gift ideas, to compare insurance plans, to create song lyrics and to help with university assignments. He sees AI as a valuable and fun part of his digital toolkit.

While AI use is normalised within his peer group, Willie acknowledges that others with less digital literacy skills may face barriers in using AI tools, primarily with overcoming the learning curve.

"There's so many things AI could be used for and we're really just scratching the surface at the moment with our new ideas."

AI usage varies; automation and productivity gains still lag

How AI is being used (% AI users)

● Consumers ● Small businesses



Analyse or summarise
content

89% **86%**



Create or refine
content

69% **75%**



Automate tasks or
processes

20% **29%**

AI is being used mostly to analyse or summarise content, for example, to answer questions and explain unfamiliar topics (35% of consumers and 33% of small businesses). It is also widely used to create or refine content, for example, to draft emails or reports (23% of consumers and 27% of small businesses).

By contrast, a relatively small percentage of consumers and small businesses are currently using agentic AI to automate tasks or processes, for example, large email mail-outs (9% of consumers and 16% of small businesses), and administrative processes such as payroll (6% and 9%).

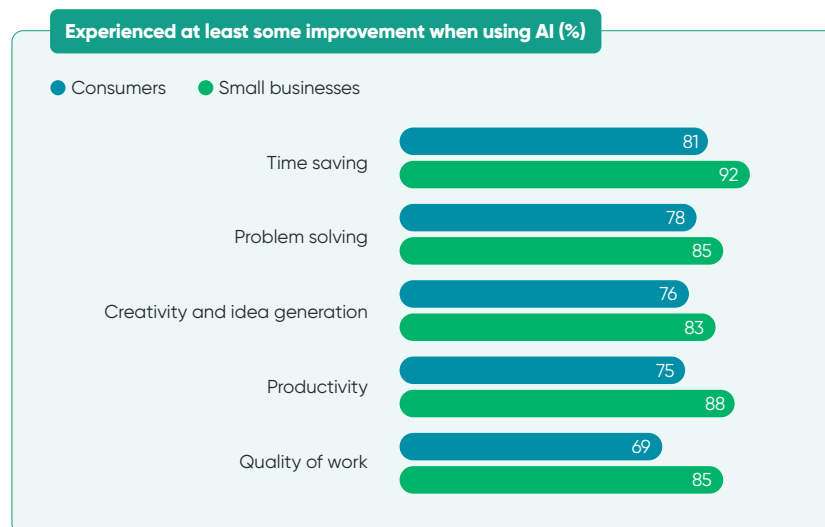
What this means

- AI adoption is maturing, but many are still using it in assistive, task-specific ways rather than redesigning workflows to automate repeatable processes.
- In practice, the biggest productivity gains may remain unrealised for now, reflecting barriers such as limited confidence, unclear use cases, and the added complexity of integrating AI into existing systems and routines.
- Bridging this gap will likely require more practical guidance on where automation adds value and how to implement it securely and effectively.

Increased AI use is uncovering time-saving and other key benefits

The incentives to use AI are strong, with most AI users reporting at least some improvement in relation to time saving, problem solving, creativity, or productivity.

In delivering these benefits, AI is an increasingly valuable digital assistant, especially for small businesses.



In qualitative discussions, AI users reported they often feel the need to verify outputs, which tempers productivity gains. While consumers recognise the tools themselves are improving, they also note that improvements are due to continuous use, 'learning by doing', and trial and error.



"You have to have your wits about you and do your fact checking when using AI tools."

Male, 50-69, Metro VIC



"AI helps me put my thoughts into words. It gradually learns your style. Something that used to take me an hour, now takes 5 minutes."

Small business, Regional NSW, Medical centre

AI users expect greater benefits as their confidence and capability grows

Among small businesses...

54%

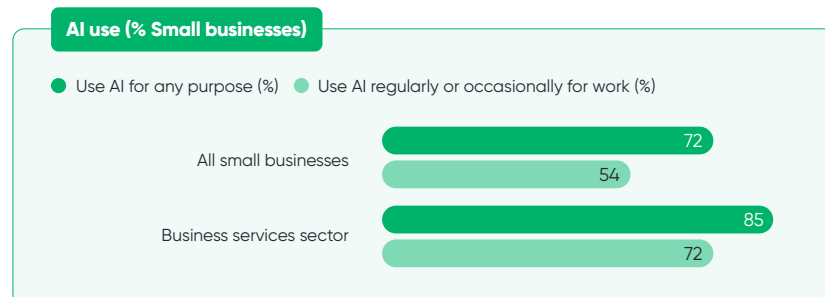
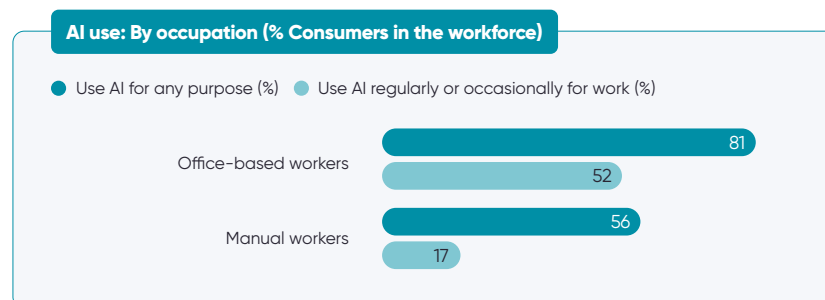
believe being able to use AI will increase efficiency

51%

think AI will help their business stay competitive

Office-based workers are leading AI uptake

Australians working in office-based jobs and small businesses in the 'business services' field (such as accounting, consulting, admin support and IT services) are significantly more likely than others to be using AI and to have moved beyond experimentation to use it on a regular basis.



AI uptake is uneven, leaving some cohorts behind

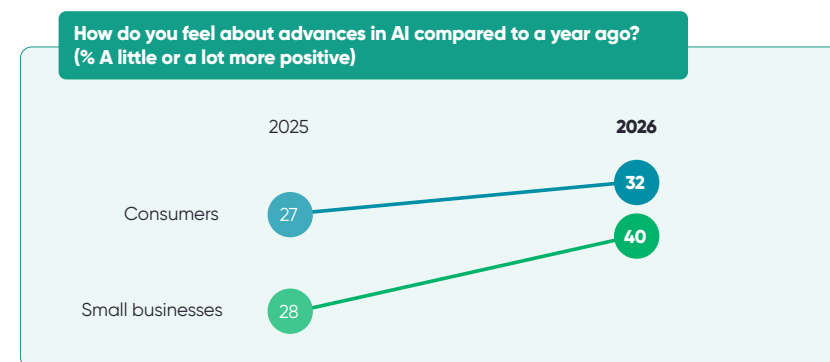
Some groups are significantly less likely to use AI, including Australians living with a disability (39%) and those aged 50 plus (40%). They are also less confident in their ability to use AI and less interested in learning more about how AI could benefit them.

Among small businesses, more established businesses (operating for six years or more) have lower levels of AI engagement compared to more newly established businesses.

These findings suggest certain groups within the Australian community are at risk of being left behind as AI becomes more embedded not just at work but across all aspects of everyday life.

AI optimism is increasing with frequency of use

Views on AI are more positive than in 2025, reflecting the accelerated uptake over the past year. With more consumers and small businesses adopting AI and realising the benefits it can deliver, there is a growing sense of optimism about the technology, particularly among small businesses.

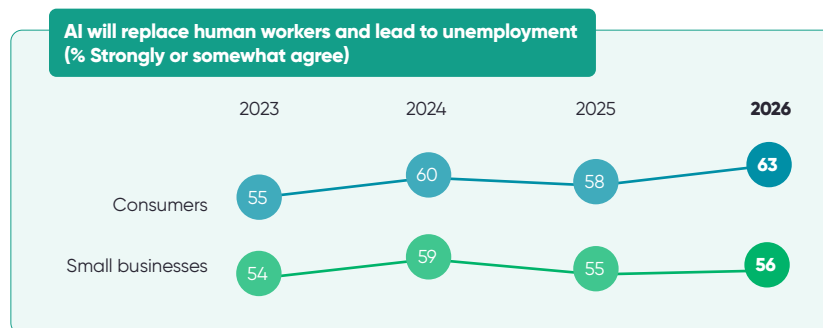


Those that use AI more frequently have significantly higher levels of optimism.

- **53%** of consumers who use AI at least occasionally say they are more positive about it, compared with just 12% of non-users or infrequent users.
- **63%** of occasional or regular small business users feel more positive about AI now, compared with just 13% of non-users or infrequent users

Fears of AI related job loss are growing

Despite positivity increasing, a common narrative around AI is the suggestion it will replace human workers, with a majority of Australians continuing to agree (either strongly or somewhat) that AI will replace human workers and lead to unemployment.



Beliefs about AI displacing workers remain broadly consistent regardless of whether people or small businesses are already using AI:

- **60%** of consumers who have adopted AI at work (vs 63% of those not using AI at work)
- **56%** of small businesses that use AI occasionally (vs 56% of those using it regularly)

Not all workers are worried about losing their jobs to AI. Some say that having learnt how to incorporate AI into their workflows, they can see how AI enhances their job but feel there will continue to be a human element required.

What this means

- The growing benefits and rapid integration of AI into everyday life present a challenge to address persistent fears of job loss amid deep uncertainty about what AI enabled work looks like.
- It also highlights the importance of increasing awareness about what support exists for both consumers and small business, such as training, transition pathways and safeguards.
- Read more about AI upskilling on [pages 31–35](#).

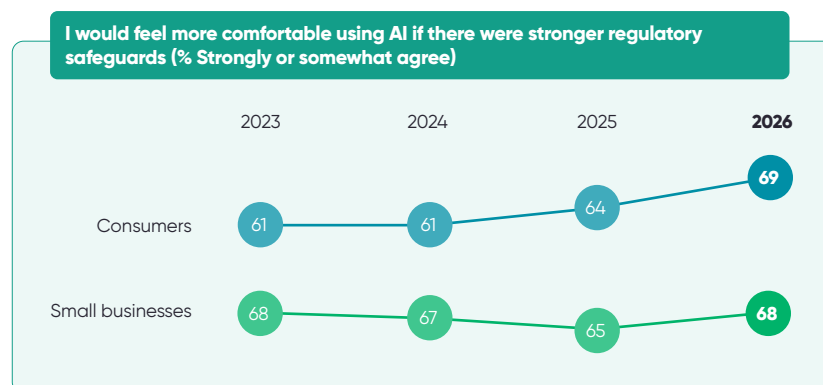


AI regulation

There is a strong desire for AI regulation

While the benefits of AI are widely recognised, for many consumers and small businesses, concerns about trust, data privacy, misuse and job displacement remain.

An increasing majority of consumers and a consistent majority of small businesses express support for regulatory safeguards to mitigate these concerns and reinforce confidence when using AI.



Qualitative discussions reveal support for AI regulation is driven by different motivations between consumers and small businesses, though both are relatively aligned on the safeguards considered most important.

Support for AI regulation amongst consumers is driven by privacy concerns, fear of false or inaccurate content, and unease about data being used without consent.

Among small businesses, strong support for AI regulation is driven by privacy concerns, desire to reduce legal and reputational risk, clarifying liability, and reducing the likelihood of getting tricked or scammed. Stronger regulation may encourage AI uptake by small businesses that currently restrict or limit AI use due to these concerns.

Consumer protections considered most important safeguards

The highest priorities for AI regulation across both cohorts are to embed consumer protections (privacy, data security and protection against AI-supported scams), followed by clear accountability and disclosure and monitoring processes.



"Regulation is needed especially if you are making decisions based on advice given by AI. That opens up employers to possible issues."

Sole trader, Brisbane, QLD, Photography



"Regulation is a good thing because you want to know what companies are doing with your data, where it's going, and what's happening with it behind the scenes."

Micro business, Regional VIC, Finance

Concerns around AI regulation

While regulation of AI is broadly supported, concerns were raised in qualitative discussion about the extent of regulatory controls, and effectiveness of enforcement.

Key concerns include:

- Doubt about the extent to which AI platforms owned and hosted overseas would comply with Australian regulations
- A belief that AI platforms would find workarounds to bypass regulatory constraints
- Worry that over-regulation could stifle innovation to increase the technical capability of AI platforms
- The pace of change is too fast for regulation to keep up
- Feeling that 'bad actors' would disregard regulatory safeguards and that risks could never be fully eliminated



"It might be difficult to enforce because it's moving at such a rapid pace, legislation might lag behind."

Male, 35–49, Melbourne, VIC



"You don't want to put restrictions on people too early before we learn the good things we can do."

Small business, Regional QLD, Entertainment

What this means

- AI regulatory safeguards are sought by Australian consumers and small businesses to address concerns and support the continued adoption of the technology.
- Prior to implementation of regulation, in-depth consultation should be undertaken to determine the most effective approach to regulation to meet the needs of Australians while encouraging innovation and take up.
- Regulation of AI that is both robust and fit for purpose, with credible, enforceable protections in place will support public trust in AI.

Digital lives in focus: Rohan



Male, Small business owner, Sydney, NSW, Computer training provider

Key points:

- Uses AI at work
- Is experimenting and learning
- Believes AI regulation can be beneficial but is cautious

Rohan owns a training business and uses generative AI for content creation (e.g. training manuals) and translation. He finds it useful and regards AI as a way for his business to stand out from its competition. He sees AI tools as providing him with extensive opportunities to create and improve his service offering.

While Rohan feels positive about AI, he considers there is a long road ahead to understanding it. He is exploring different AI platforms and watching tutorials to build his familiarity with the tools available.

He also believes regulation of AI would ensure ethical practices, such as mandatory watermarks on AI-generated content. However, he is cautious that regulation shouldn't go too far so as to impede its efficacy.

"There has to be ethical standards on usage, there are ads on platforms without any watermarks disclosing AI use. But I've also heard about people using AI and then facing copyright issues. There is not an infinite amount of options, so things will get reused."

Security barriers

A majority of Australian consumers and small businesses are highly concerned about online security

Overall concern about cyber security (% Quite or very concerned)

54%

Consumers

55%

Small businesses

A majority of Australian consumers and small businesses are highly concerned about online security. While concerns around individual details or photos being leaked or falling for a financial scam are widespread, those who are middle-aged (35-69) appear to be more concerned overall (91% at least somewhat concerned, significantly higher than other age groups). Qualitatively, this appears to be due to this age group simultaneously having concerns about their own cyber security, their children's privacy online and their elderly parents falling victim to scams.

Concerns about online security (% Consumers)

	18-34	35-49	50-69	70 plus
At least somewhat concerned	86%	92%	91%	87%
Quite or very concerned	51%	54%	56%	59%



"I have anxiety around cyber security because I understand how important it is, but don't feel I have the skill needed to look after myself online."

Female, 50-69, Regional VIC



"I know cyber security serves a pretty important role in my life and privacy, but I have zero clue on how it operates and what is required of me."

Male, 35-49, Regional NSW

Low confidence in online security measures continues to hold back behaviour

Despite increasing online confidence in general, confidence in relation to online security has not increased in the past few years and remains relatively low.

Only 42% of consumers feel very confident using multifactor authentication (MFA) (despite 70% reporting using it). Fewer still are confident in their ability to create strong passwords, back up data, find trustworthy information about online security, and crucially, knowing where to report a data breach.

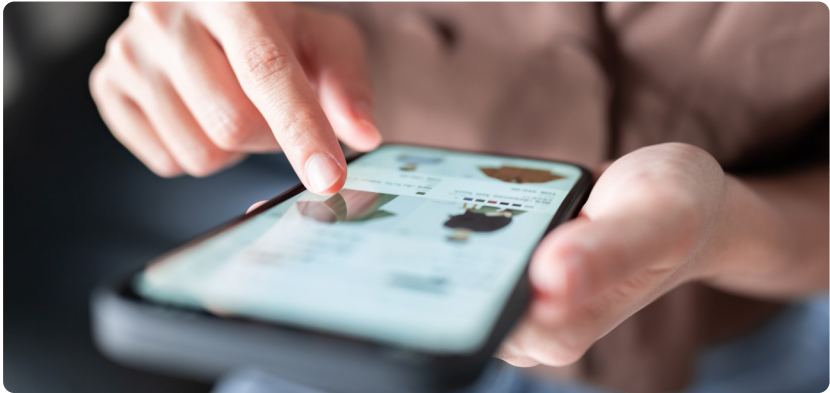


Security features built in to digital technology likely influence behaviour

MFA is the most widely adopted security measure because it is often mandated. Other security behaviours that rely on users taking proactive action continue to see much lower uptake.

Cyber security behaviours in last 12 months (% Consumers)

	2025	2026
Used MFA	73%	70%
Used more complex passwords	42%	43%
Avoided connecting to public Wi-Fi (e.g. at shopping centres or airports)	39%	39%
Avoided saving credit card details in your device or web browser	37%	36%
Changed passwords regularly	32%	36%
Avoided using the same password for multiple sites or accounts	34%	35%

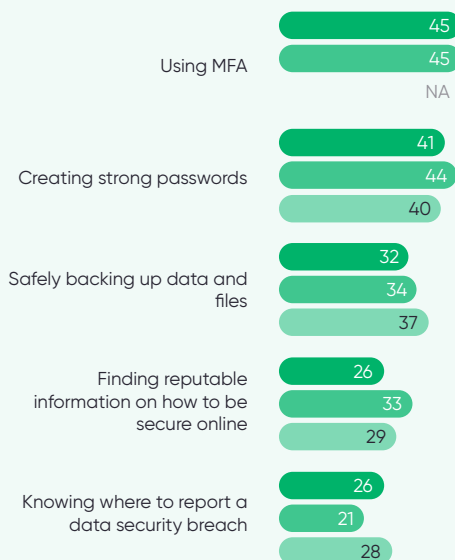


Small business cyber security confidence is limited

Among small businesses, confidence is highest for creating strong passwords and using MFA, but drops sharply when it comes to knowing where to go for information on how to stay secure online and where to report incidents, suggesting under preparedness for response.

Cyber security confidence – (% small businesses - Very confident)

● 2024 ● 2025 ● 2026



"It would be handy to know who to contact if there was an incident, who would be able to give you accurate advice."

Sole trader, Brisbane, QLD, Photography



"We need somewhere you can get unbiased or free information – to tell you 'these are the weak points, here are things to consider' – just more direction."

Micro business, Regional VIC, Financial services

Investment in cyber security is rising, but unevenly

A substantial proportion of small businesses (37%) do not know how much they spend on cyber security, indicating it is not always a visible or strategic budget line.

Among those who are aware how much the business spends, results show an increase in median annual spend to \$500 in 2026, up from \$300 in 2025. However, spend on cyber security continues to vary by business size.

Median spend per year on cyber security (Small businesses)



\$200

Sole trader
(2025 = \$120)



\$1000

Micro
(2025 = \$400)



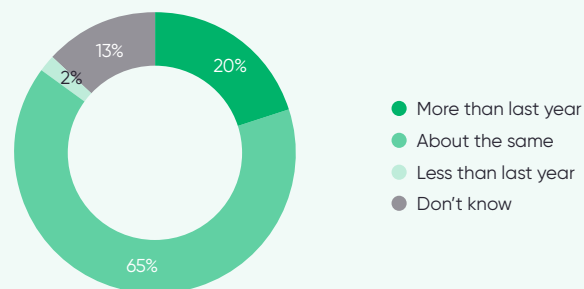
\$5000

Small
(2025 = \$3,000)

Future cyber security spend not expected to change

Despite the uplift this year, a large majority of small businesses (65%) expect to maintain current spend when looking ahead. Just one in five (20%) say they expect to increase their spend in future.

Expected future cyber security spend (% Small businesses)



For many small businesses, cyber security is limited to basic preventative measures

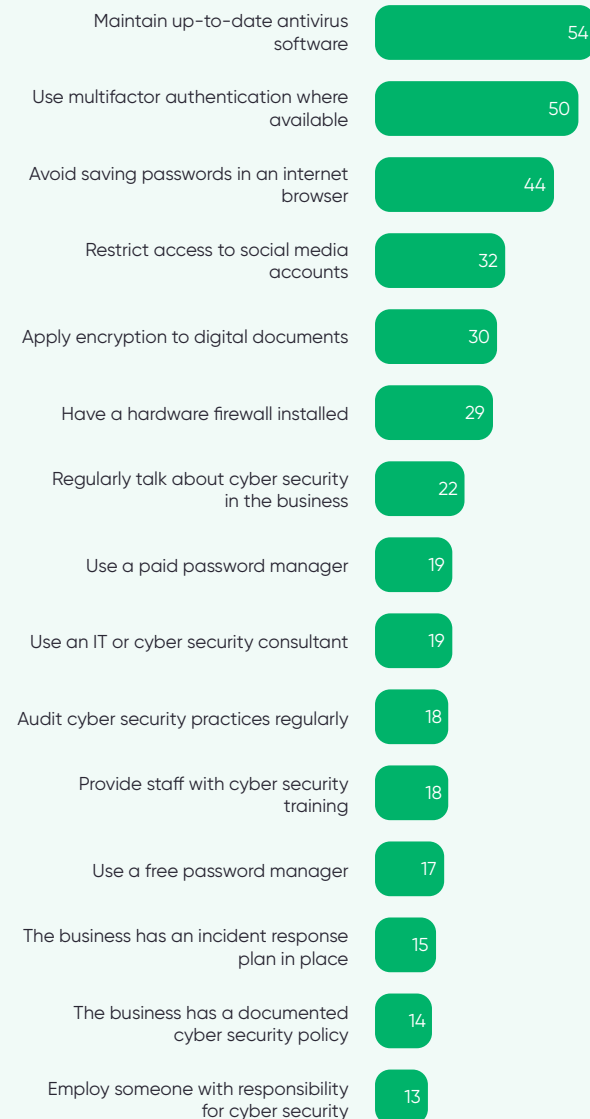
The most common online security behaviours are antivirus software, MFA and password management. More advanced behaviours such as dedicated cyber security resources, incident response planning and staff training are less common, particularly among smaller businesses.



"In financial advice the biggest risk is transferring money, but we don't have cyber security training on this. In my previous bigger business, we did have this training."

Micro business, Brisbane, QLD, Financial services

Cyber security behaviours undertaken (% Small businesses)



Time, cost and lack of knowledge hold many small businesses back from implementing stronger online security measures

Many small businesses acknowledge gaps between concerns about cyber security and workforce capability. Cyber security practices tend to be reactive, ad hoc and dependent on external support.

They recognise the importance of strong cyber security practices but report uncertainty around best-practice implementation, and investment in cyber security varies widely.

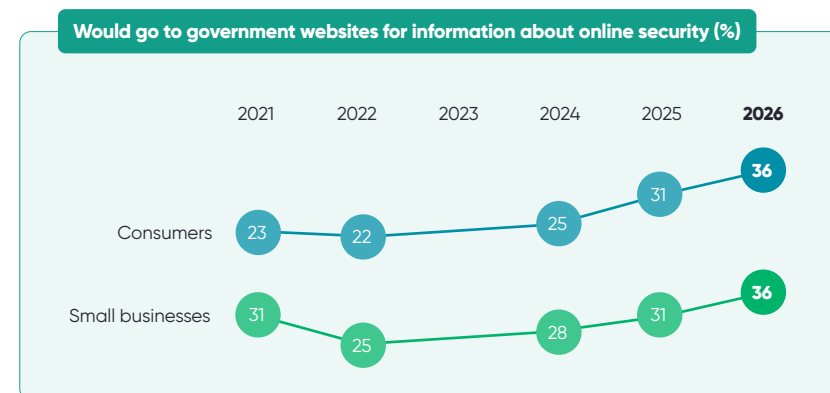
Those that have employed a dedicated or external IT consultant tend to have more measures in place.

Survey findings this year highlight the cost and time barriers that prevent small businesses from implementing cyber security measures.

- **51%** of small businesses that did not provide staff with regular cyber security training but were interested in doing so said cost was a barrier, and **39%** didn't have the time to organise this.
- **47%** of small businesses that do not maintain up-to-date antivirus software on their computers but were interested in doing so said cost was a barrier, and **22%** didn't have the time to organise this.

Government website usage on the rise

More Australian consumers and small businesses this year say they would use government websites (such as [cyber.gov.au](https://www.cyber.gov.au)) for information and guidance on improving online security. Preference for these sources has grown steadily in the past few years, however intended use still remains relatively low.



Small businesses emphasise the need for low cost (or ideally free), trusted sources for information and guidance on cyber security. However, survey results show continued low awareness of free, Australian government cyber security resources.

Most small businesses hold sensitive data but few feel equipped to protect it

Most Australian small businesses (92%) hold some form of personal or sensitive data, either for staff, customers, suppliers or the business itself, highlighting the universal importance of maintaining good online security practices.

Types of data held by the businesses (% Small businesses)



Regardless of size, a majority of small businesses have a need to ensure good data protection. Fewer sole traders report holding personal identity documents, but most hold some form of sensitive data.

Types of data held – by business size (% Small businesses)

	Sole traders	Micro businesses	Small businesses
Personal identification documents	21%	41%	51%
Any personal or sensitive data	88%	95%	98%



Majority of small businesses are not confident protecting their data

Despite nearly all small businesses holding personal or sensitive business data, few are confident they can protect this data against increasingly sophisticated cyber threats.

Confidence keeping business data secure online (% Very confident)



Small businesses that hold personal or sensitive data are more likely to have proactive cyber security practices in place. Notably, those that hold personal identification documents for employees, clients or suppliers are more likely to:

- Talk about cyber security with others in the business (43% vs 22% of all small businesses)
- Provide staff with cyber security training (36% vs 18% of all small businesses)
- Have a documented cyber security policy (29% vs 15% of all small businesses)
- Have an incident response plan (29% vs 16% of all small businesses)



"It frightens me that my clients' personal information is on our computers. I think about cyber security all the time, especially seeing regular spam emails."

Micro business, Sydney, NSW, Personal care services

Digital lives in focus: Linh



Female, Micro business, Retail, Regional VIC

Key points:

- Improved security measures following significant cyber incidents

Linh is the co-owner of an independent retail business. A few years ago, her business was the victim of a serious cyber incident after her mobile phone number was illegally ported, allowing criminals to access her email and bank accounts and drain the business' funds. This happened twice within the same year.

The attack had an immediate impact on her operations, leaving her unable to pay suppliers and manage cash flow. Linh was able to recover the stolen funds, but the experience was highly disruptive to the business and damaging to her confidence.

Following the incidents, Linh strengthened the business' cyber security by engaging a local technology provider, introducing MFA across key accounts, improving email security and installing antivirus software.

"The support we got from our IT consultant was invaluable. It gave us a sense of security to learn those things we didn't know, and feel as if we weren't on our own."

Small business size is fueling false perceptions and cyber security risk

Almost half of small businesses feel helpless against cyber security threats on the basis their limited resources pale in comparison to larger corporate organisations that have fallen victim to cyber criminals.

Meanwhile 2-in-5 believe they do not need to worry about cyber criminals, believing they won't be targeted by cyber criminals due to their small size.



'If larger, well-resourced companies can't protect against cyber attacks, then I can't protect my small business'



'My business wouldn't be a target for cyber criminals because it's too small'

Looking at the overlap between these attitudes, 52% of those who think their business is too small to be a target also feel they are powerless to stop cyber attacks due to their small size.

These mindsets increase risk by encouraging complacency. For example, small businesses that believe they are too small to attract the attention of cyber criminals are far less likely to use MFA where it is available (38%), compared with those that do not hold this view (57%).

When the topic was raised in qualitative discussion, many noted they were unaware that attacks against small business by cybercriminals are often fully automated, with thousands of businesses being attacked at the same time, regardless of business size.



"What chance do we have when big companies are getting hacked? They have high grade protection and still were attacked by hackers."

Small business, Melbourne, VIC, Cleaning business



"I am not too concerned about cyber security, we are a small business and I don't see scammers and hackers going into small businesses."

Small business, Sydney, NSW, Computer training provider

What this means

- There are clear gaps in small businesses' approach to online security. Many underestimate their risk of being targeted by cyber criminals, while also believing a cyber incident is inevitable. This combination of misplaced confidence and resignation is contributing to underinvestment in basic security practices.
- In reality, every business operating online is at risk of cybercrime, regardless of size, as cyber criminals rely on highly automated systems that scan the internet for vulnerabilities and can attack many businesses simultaneously. Rather than targeting businesses by size, cyber criminals use sophisticated tools to identify those lacking basic security protections, and then exploit these weaknesses, often at scale and through offshore operations.
- This year's Digital Lives research shows that 13 per cent of small businesses have experienced a cyber attack, while 12 per cent have had data compromised in a breach. These findings align with the [Australian Signals Directorate's 2024–25 Annual Cyber Threat Report](#), which indicates financial losses from cybercrime continue to rise year-on-year for small businesses.
- Greater education for small business on the realities of cybercrime and simple steps small businesses can take, including [the Five P's of website security](#), would be beneficial and support an economy-wide uplift in cyber security practices.
- The Federal Government's investment in resources such as [cyber.gov.au](#) provide a free and reliable source of cyber security information and advice for Australian consumers and small businesses. While use of these resources has grown steadily, it remains low, highlighting the need for continued investment to build awareness.

Digital lives in focus: Terry



Male, Small business owner, NSW, Construction and building maintenance

Key points:

- Experienced significant business interruption due to cyber incident
- Cyber security investment is influenced by business size (revenue and headcount)

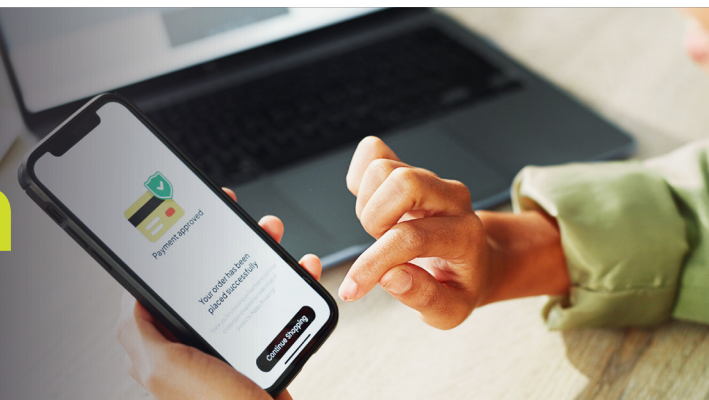
Terry runs two businesses – a smaller one (5–19 employees) and a larger one (30 employees, including offshore staff).

As a result of previously having his IT system hacked, the larger of his two businesses lost a month's worth of data. Since then, it has moved to cloud-based systems and implemented formal cyber security policies, taken out cyber insurance and introduced monitoring software and cyber security training for staff throughout the year.

His smaller business does not have formal policies, insurance or training. With only a few staff accessing key platforms, Terry feels risk is low and that more formal protections are not needed. While he acknowledges external risks exist, he feels being smaller might make it less of a target, and that the higher revenue and employee count at his larger business justifies the increased spend on cyber security measures.

"We're vulnerable in the sense hackers might see this as an easy way to get some money quick. But because we're so small, I wonder whether smallness is actually a bit of an advantage."

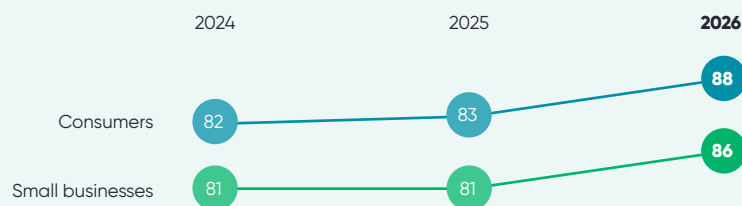
Threat detection



Scams are becoming harder to detect

Concern among Australian consumers and small businesses about online scams continues to intensify. This year sees an increase in the proportion of Australian consumers and small businesses who believe the complexity of scams is increasing, and that they need to be increasingly vigilant to such threats.

Cyber criminals are becoming smarter and more sophisticated, so it is important to stay up to date with the latest online security trends (% Strongly or somewhat agree)



"Cyber threats are constantly evolving, the bad actors are very good at evolving and scamming people and it's hard to stay ahead."

Male, Sydney, NSW

This uptick coincides with the rapid acceleration in the capability of models used by AI platforms. There is a strong sense that it is becoming harder to detect what is real online and what is not, due to the ability to create images or content using AI.

In qualitative discussions, research participants recounted occasions on which they, or a friend or family member, were initially deceived by fake content online. While the examples given were often light-hearted (such as humorous videos of someone famous dancing) there was a sense that this type of content could evolve and be used for more sinister purposes, as the quality of the underlying technology continues to improve.

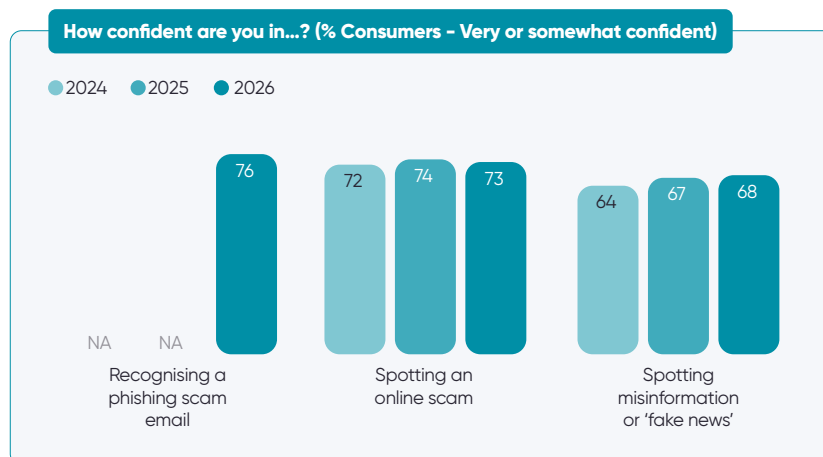


"We used AI at work to create an avatar and videos of a colleague with their permission. We uploaded a script and photo and it looked just like them. I couldn't tell the difference. From an identity perspective someone could impersonate them, use that to get on Teams or contact their bank."

Male, 35-49, Brisbane, QLD

Confidence is high but detection is imperfect

Despite heightened concern about cyber threats, survey results show a clear majority of consumers and small businesses continue to feel confident in their ability to spot fake content and online scams.

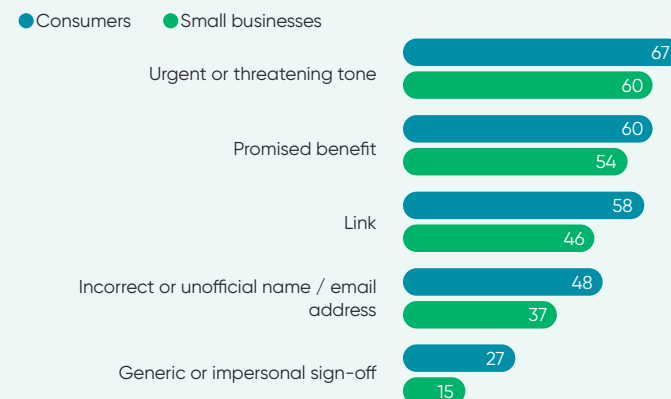


In this year's survey, we tested consumers' confidence to spot fake content and online scams by showing participants a genuine email and an example of a scam email and asking them to select elements that indicated whether the emails were genuine or suspicious.

The most obvious sign that an email is a scam is an urgent tone, for example encouraging the recipient to click on a link and take action immediately or implying an immediate risk if a particular action is not taken. Additionally, the inclusion of a promised benefit, to be received after providing personal information or financial information, is considered another clear sign of a potential scam email.

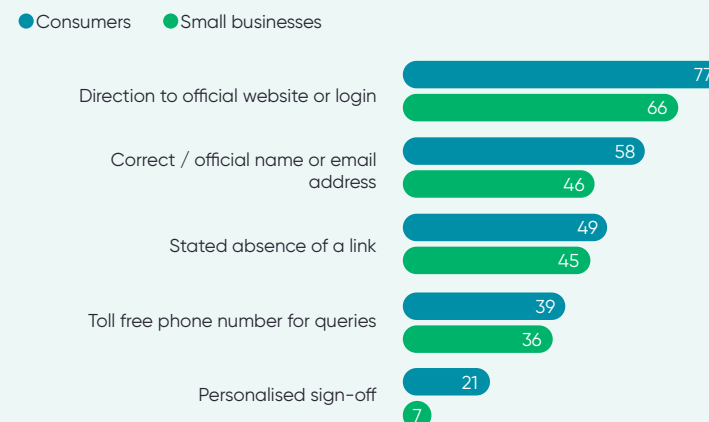
A majority of consumers could correctly identify these elements; however recognition of all suspicious elements was lower among small businesses. Confidence in ability to recognise phishing emails is high across all age groups, however those aged 70 plus are less confident about spotting online scams more generally. In the test exercise, they were less likely to identify the inclusion of a link, and incorrect email address as suspicious.

Elements considered suspicious that may indicate a scam or phishing attempt (% Selected)



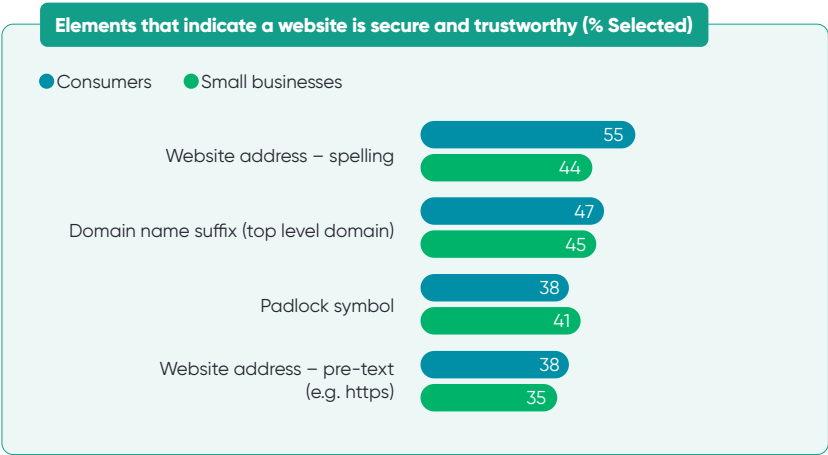
Consumers were also better at identifying elements that indicate an email is legitimate. The clearest sign of a legitimate email is the absence of a link, with instructions instead to login to accounts via the website or app to access the full message or take the required action.

Elements that indicate a legitimate email (% Selected)



Website address and domain names are key trust signals

When assessing whether a website is trustworthy or not, people most commonly rely on cues such as correct spelling of website addresses and the website suffix (e.g. .au or .com, which are known as top level domains) but many don't know what to look for. This indicates the importance of educating people on elements that indicate a website is safe to use.



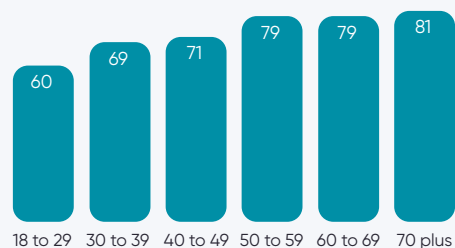
Cyber risks

Fear of financial loss underpins cyber security concerns and prompts action

Among consumers who have implemented cyber security measures, the strongest motivation for doing so was to avoid financial loss. 73% of consumers indicated this was a factor in wanting to strengthen their cyber security, ahead of keeping personal data secure (67%), peace of mind (60%), reducing the risk of cybercrime such as identity theft (59%) and avoiding the hassle of dealing with a cybercrime event (50%)

Fear of financial loss is most acute among older age groups. While younger age groups are comparably less concerned about financial loss, it is the number one motivator among all age groups.

Reasons for implementing cyber security measures – Avoiding financial loss: By Age Group (% Consumers who implemented measures)



Qualitative discussions reveal that concern about cyber security threats is highly emotive and grounded in fear of loss or harm. Identity theft, account takeover and family safety (especially children) also dominate concerns for consumers.

Additional concerns for small businesses include business disruption, reputational damage and responsibility for client data. Participants frequently cite high profile data breaches as catalysts for anxiety, often accompanied by uncertainty about appropriate responses.



"We had an email sent from a supplier who had been hacked. We ended up transferring \$80k as it looked like a standard email. It was reported but nothing could be done. Human error. We're very cautious now."

Micro business, Melbourne, VIC, Retail



"My biggest concern is waking up one day to an email that says 'your account has been linked to new credit cards'."

Female, 18-34, Regional VIC



"My information is insignificant compared to clients'. The consequence of our clients' sensitive information being accessed to us as a business is massive."

Micro business, Regional NSW, Digital services

Almost one-in-five Australians report financial loss due to scams

Consumer fears of financial loss related to cyber security are not unfounded. Almost one-in-five Australian consumers report having lost money due to online scams last year. The true number may be higher, given the potential reluctance to admit these experiences, even in an anonymous survey.

Cyber crimes experienced in the past year (% Consumers)

12%

Lost money to a financial scam

10%

Purchased items from a fake online store

4%

Were victims of a romance scam

19%

Lost money due to any online scam

Experiencing scam losses can improve security behaviour but may reduce online engagement

Fear of financial loss can act as a powerful trigger to improve online security awareness and behaviour. However, heightened concern following an online scam can also lead to changes that undermine the value of the internet to those affected.

People who experienced financial loss due to an online scam are significantly more likely to:

- Feel very or quite concerned about online security overall (64% vs 52%)
- Know where to report a data breach (55% vs 49%)
- Delete or deactivate accounts no longer in use (33% vs 24%)
- Enable ransomware protection on devices (14% vs 9%)
- Use a paid password manager (16% vs 8%)
- Avoid online activities, most notably buying products online (19% vs 11%), online banking (16% vs 11%), and accessing government services online (11% vs 5%).

Response to online security incidents is limited

The actions taken following an online security breach vary according to the nature and severity of the incident. Most focus on immediate, practical responses such as changing passwords or cancelling affected accounts. More serious incidents, particularly those involving financial loss, prompt stronger escalation (for example, contacting banks and reporting to authorities).

Yet many Australians are not taking appropriate follow-up action when cybercrime occurs.



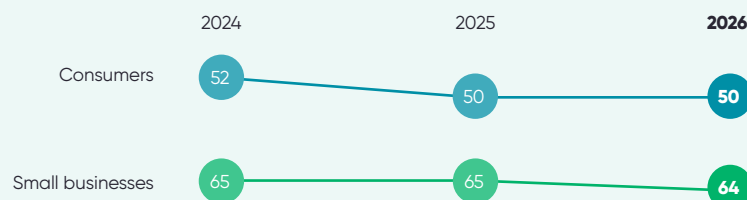
of those who received a notification that their password was contained in a data leak changed the impacted password

Among those who experienced financial loss due to an online scam, 56% contacted their bank. However:

- Only 16% contacted the police
- Only 18% reported the incident to cyber.gov.au
- Only 18% upgraded security settings on their device.

These figures indicate a lack of awareness of what actions to take and who to report to in the event of a cybercrime. Indeed, confidence in knowing where to report a data security breach remains limited among both consumers and small businesses.

How confident are you that you know where to report a data security breach (% Very or somewhat confident)



Digital lives in focus: Lucy



**Female, 50-69,
Brisbane, QLD**

Key points:

- Had personal data leaked in data breaches
- Unsure how to properly protect herself online

Lucy uses the internet for various tasks such as online banking, social media, and booking appointments. While she appreciates the convenience of these online activities, she sometimes feels frustrated and overwhelmed by increased cyber security requirements and having to remember multiple, complex passwords.

Lucy experienced her personal data being exposed in data breaches, however, wasn't sure what immediate actions to take after receiving notification of this, or what changes she should make long term. She has since decided to limit and 'simplify' her digital life, by choosing to make physical purchases where possible, and limiting providing her credit card details to websites.

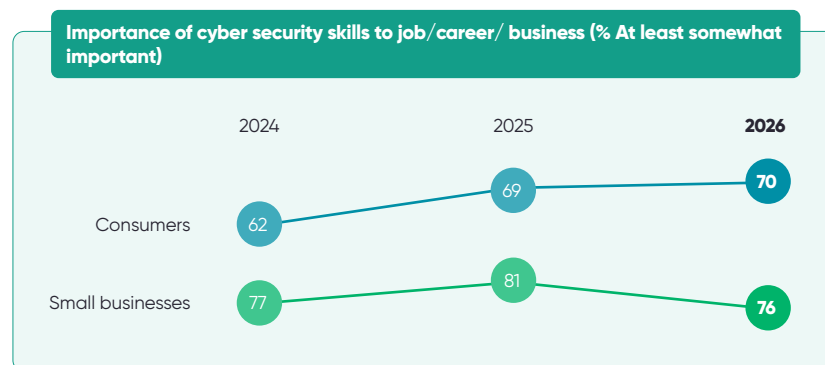
In addition to her own experiences, Lucy's father lost his life savings through an email scam. She wishes there were more organisations or resources to assess potential scams, particularly those for older people.

"I didn't really know what to do apart from changing passwords and keeping watch on those accounts."

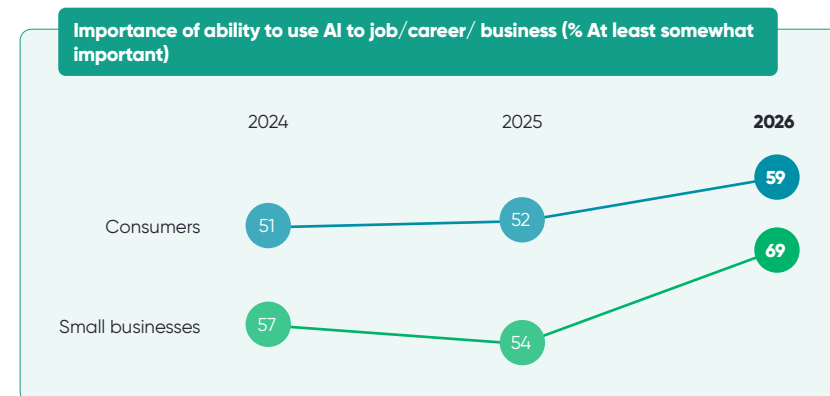
Digital skills

Cyber security and AI stand out as the two priority areas for digital skills development

Strengthening cyber security knowledge and skills is not only important for staying secure online – it is also seen as increasingly important for the workplace and careers, whether in a technical role or not.



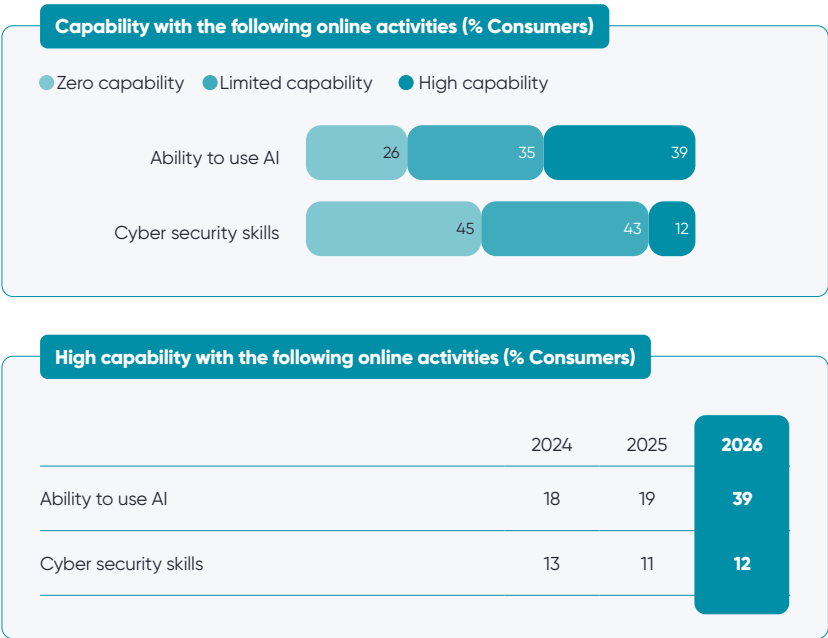
Australians of working age and small businesses both increasingly consider ability to use AI as an essential skill.



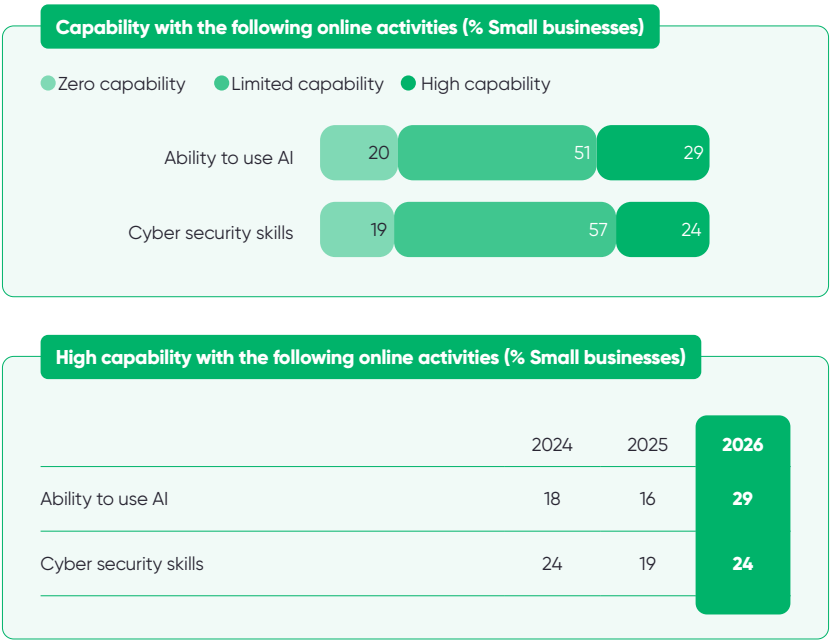
Given their importance, self-reported capability with using AI and cyber security skills highlight a skills gap

39% of consumers report high capability using AI, a significant uplift from 2025 (19%) reflecting the rapid increase in AI adoption over the past year. The remaining majority have only limited or no capability and admit needing guidance.

Meanwhile, only a minority continue to report high capability with cyber security skills (12% vs 11% in 2025). This suggests the increasing sophistication and complexity of cyber security threats makes it hard (or feel too hard) for consumers to strengthen their capability.



Similar patterns are evident among small businesses, with a significant increase in the proportion reporting high capability using AI (29% up from 16% in 2025), and a marginal increase in cyber security skills (24% vs 19%).



AI capability is growing despite static confidence

Despite increased capability, confidence using AI remains moderate, with just 46% of consumers and 61% of small businesses saying they feel very or somewhat confident using AI.

In qualitative discussion, participants noted their confidence online is undermined by a range of concerns, including:

- How confidential and sensitive data is handled by the business and third-party platforms
- The accuracy and reliability of AI generated outputs, and who is accountable when those outputs are wrong.

Confidence using AI (% Consumers)

● Somewhat confident ● Very confident

Consumer

31 14

Confidence using AI (% Small businesses)

● Somewhat confident ● Very confident

Small Businesses

42 20



"Whilst there is a lot of good information, it does also have inaccurate information. Believing it all the time has risks."

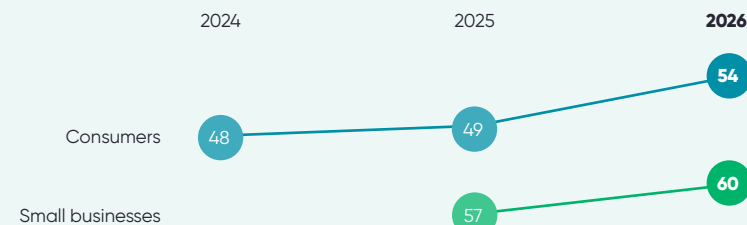
Male, 18-34, Sydney, NSW

Australians increasingly see the ability to use AI as a crucial workplace skill, and there is a strong appetite to improve capability.

Ability to use AI will increase my employment prospects – Working age consumers (% Strongly or somewhat agree)



I would like to learn more about AI and how it could benefit me in my life / my business (% Strongly or somewhat agree)



Digital skills are mostly built organically but there is desire for structured training

When asked about their digital capability, consumers and small businesses often describe having developed their skills over time through everyday use, rather than from structured learning or education. There is however persistent demand for practical, accessible skill building, especially to develop cyber security skills.

Interest in developing cyber security analysis skills increased significantly this year, while interest in other digital skills remains relatively constant.

Growing cyber security concerns are driving a desire to upskill

The increase in interest in developing cyber security skills reflects growing anxiety about online safety and a recognition that threats are becoming harder to identify and keep up with. Participants describe feeling under-skilled, even when they have not yet been personally affected. This is driven by constant exposure to scams and the evolving tactics and skill of cyber criminals.

Many simply want to know what actions to take to better protect their online privacy and security, stay on top of scams, and where to find trusted, up-to-date information.

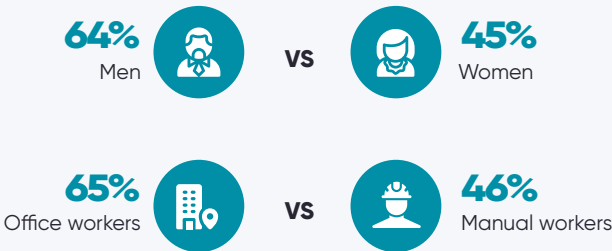
Some have access to training/information sessions through workplaces, banks, community groups or government sessions, and find these reassuring and useful.

Interest in developing the following skills or working in the following roles (% Working Age Consumers - Quite or very interested)

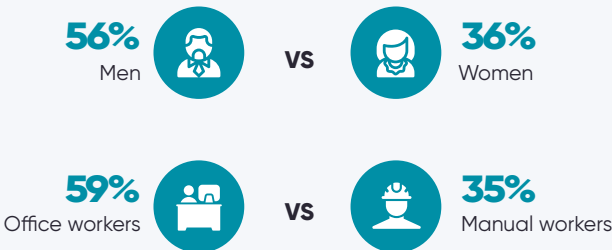
	2025	2026
Cyber security analysis	48%	54%
IT support	48%	51%
Web and app development	50%	50%
Network and systems administration	47%	50%
Data science	47%	48%
AI prompt engineering	44%	46%
Software engineering	44%	45%
User experience design	50%	44%

Interest in improving digital skills is significantly higher among men, younger consumers (aged 18-34), people who work in office-based jobs, and people from culturally and linguistically diverse backgrounds. This is equally true when focusing on cyber security and AI skills.

Interest in developing cyber security analysis skills

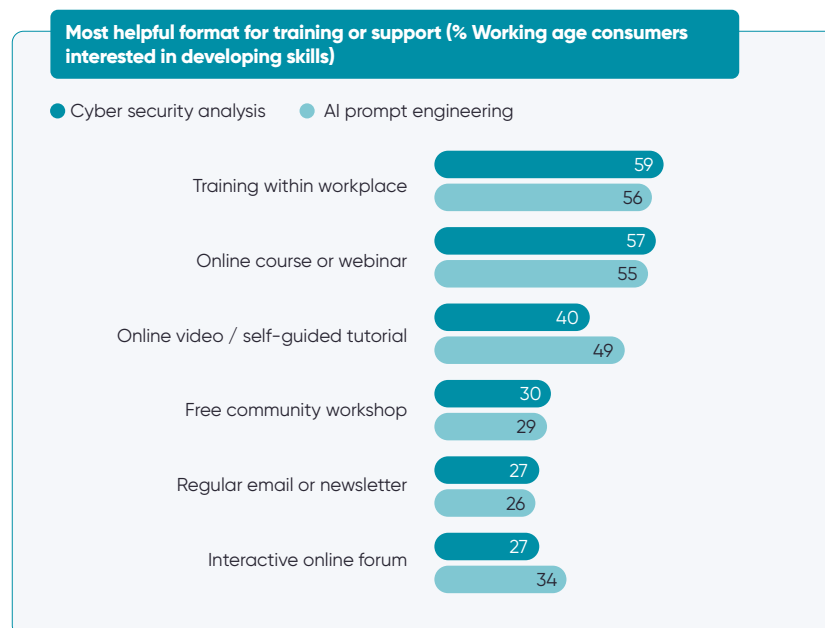


Interest in developing AI prompt engineering skills



Employee-led digital skills training and online formats are preferred

Findings reveal a strong expectation that employers will provide training on cyber security and AI skills in the workplace. Participants show a strong preference for online training – either structured online courses or shorter videos that allow self-guided learning. These training and support preferences were consistent across all types of digital skills surveyed.



During qualitative discussions, small businesses expressed a desire for more accessible cyber security education and resources specifically for small businesses, noting a lack of clear guidance on best practices and the risks associated with emerging technologies such as AI.

Digital lives in focus: Connor



Male, Small business, Regional TAS, Insurance

Key points:

- Sees AI as a valuable productivity tool for small businesses
- Believes the biggest cyber security risk is human error
- Provides ongoing AI and cyber security training for staff

Connor's business works with sensitive client information and he has taken a deliberate, structured approach to introducing AI, alongside long-standing investments in cyber security.

The business has developed a formal AI policy outlining approved tools, acceptable uses and restrictions. It also provides ongoing AI training and embeds AI into everyday practice through regular discussions, shared examples and reinforced policy settings.

Alongside AI adoption, cyber security is treated as a core business priority. Training begins during staff onboarding and is reinforced through regular reminders, supervision and monitoring.

Connor believes a proactive rather than reactive approach to AI and cyber security is crucial for sustainability and risk mitigation, viewing the measures implemented and staff training as invaluable.

"The excitement for staff is they can see the benefit of using technology, and that is efficiency. And efficiency means the capability to do more in a day."



Digital ID

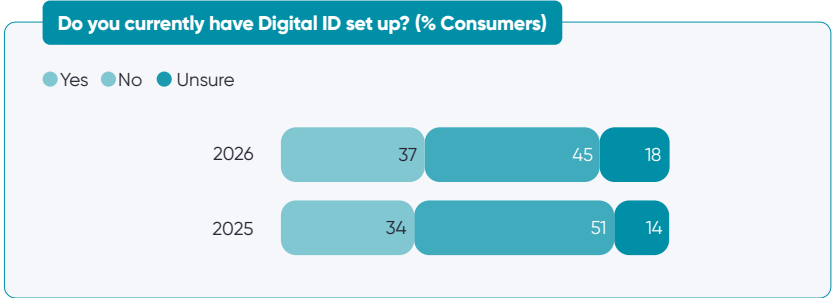
Digital ID continues to be met with confusion

Digital ID is a technology that enables identity verification online without the identity holder having to further share sensitive documents such as a drivers' licence or passport with third parties. Digital IDs are issued by providers accredited by the Australian Government. Examples of Digital IDs include myID (the Digital ID platform operated by the Australian Government), IDVerse (document authentication and biometric verification platform) and ConnectID (Australian digital identity verification platform).

According to Australian government data, more than 15 million people (54% of the population) have registered with myID.

Though our survey results show that most Australians know about Digital ID (69% of consumers, 81% of small businesses), only 37% of consumers report having a Digital ID, much lower than the proportion indicated by government data. A further one in five (18%) are unsure if they have one.

These results reflect similar findings to last year's survey, highlighting ongoing confusion about what Digital ID is, and if people who use myID are aware they have a Digital ID.



Qualitative findings reflect these results, with awareness and understanding of Digital ID typically being high-level only. Digital ID is predominantly associated with myID, however there is also confusion as many also think Digital ID relates to digital driving licences or other digital forms of identity documents.

The benefits of Digital ID are compelling, but limited opportunities for use prevents benefits from being realised

A majority of Australians see the potential convenience of Digital ID when accessing government services (67%) or when submitting applications or opening accounts (66%).



of Australians who do not already use Digital ID are interested in setting it up

The main perceived benefits for consumers interested in Digital ID are reduced paperwork, no need to share documents and improved security of personal data.

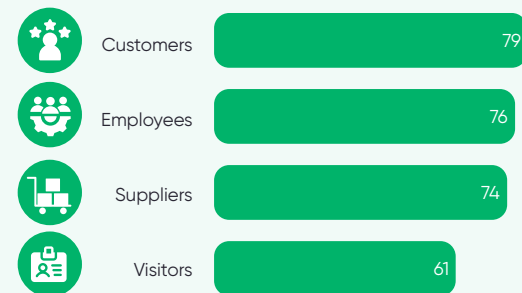
Of those who have Digital ID, most only use it for the service they set it up for (e.g. tax return), citing lack of need to use it elsewhere. A few want to use it elsewhere but it is not accepted. Some people only remembered they had a Digital ID once an explanation was provided, attributing this to lack of use.

For small businesses, interest in being able to accept Digital ID when they need to verify identification stems from a belief it would reduce administration burden, improve security and streamline onboarding or transactions.

Many small businesses are eager to increase their use of Digital ID to streamline identity verification processes

46% of small businesses currently need to verify the identity of groups that interact with the business (such as employees, customers, suppliers and visitors). Among those who do not currently accept, or are unsure if they accept, Digital ID, interest in the technology is high.

Interest in accepting Digital ID for the following groups (% Small businesses not currently or unsure if accepting Digital ID for each group)



Persistent concerns about Digital ID represent barriers to uptake

The perceived benefits of Digital ID are felt to be limited unless it can be used more broadly with a range of service providers and replace the need for multiple logins or documents.

Currently, people feel there are insufficient ways to use Digital ID for it to be worth setting up. Survey results show a high proportion (62%) of consumers would be more likely to use Digital ID if it could be used with all service providers.



"I don't know what I will get from the time spent setting it up. If there were more benefits then I would be more inclined."

Female, 18-34, Regional VIC



"If it streamlined other logins I'd be more inclined to set up a Digital ID. There's really no incentive at the moment."

Male, 18-34, Adelaide, SA

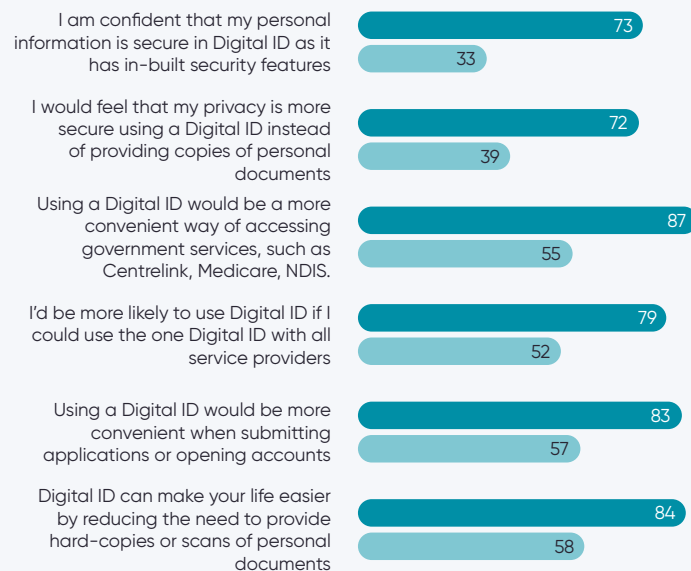
Concerns over data security underpin Digital ID apprehension

Strong protections are expected, and people want clear safeguards, transparency and reassurance about who can access their data and for what purpose. Support for Digital ID increases when systems are perceived as secure, voluntary and delivering clear value, reinforcing that trust, not technical literacy, is the main barrier to broader uptake.

Notably, there are clear differences in perceptions towards Digital ID amongst those who do and do not currently have one. Those who use Digital ID are more likely to see it as convenient, secure and privacy enhancing, while those without it are more likely to worry about data misuse or theft.

Feelings towards Digital ID – Consumers (% Strongly or somewhat agree)

● Have Digital ID ● Do not have Digital ID



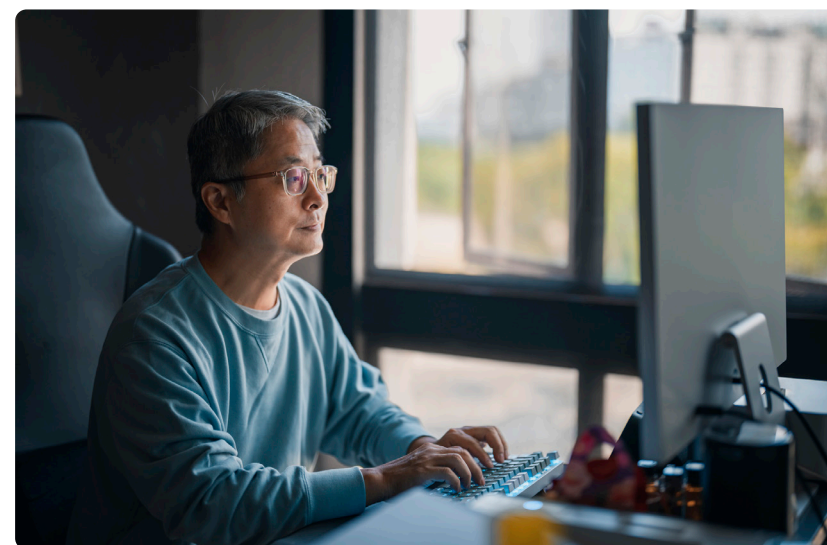
"Digital ID sounds good but I wonder where my uploaded documents go, hopefully they're safe."

Male, 35–49, Brisbane, QLD



"Having everything in one spot is too vulnerable. They say there's all these bulletproof systems, encryption, but I don't believe any of that. Nothing's safe."

Female, 50–69, Regional VIC



The role of regulation is critical in addressing confusion, building trust and unlocking the full value of Digital ID

There is widespread expectation among both users and non-users that the Digital ID system will be subject to strict regulatory compliance and enforcement.

	Have Digital ID	Do not have Digital ID
Digital ID providers must be regulated and held accountable for any privacy breaches that occur	88%	77%

Concerns among non-users of Digital ID remain and reassurance is crucial to alleviate concerns and encourage uptake.

	Have Digital ID	Do not have Digital ID
I worry that my personal information could be hacked or stolen through Digital ID	57%	65%
I worry that my personal information could be used for other unintended purposes through Digital ID	59%	64%

Beyond regulation, clear communication on what Digital ID is, and wider acceptance of it, will support trust and uptake. Participants expect Digital ID to be recognised consistently across government services and by third parties such as banks and superannuation funds. Current confusion about the benefits of Digital ID, which providers are legitimate, and where it can be used, reduced confidence and engagement.

What this means

- People express concern about Digital ID providers holding all their data in one place and feel government systems aren't secure enough for this.
- Explaining why holding data centrally through Digital ID is more secure than through multiple organisations or entities that have lower safety protections is key.
- Policy settings that promote broader acceptance across government and the private sector will help Australians overcome the "limited use" perception.
- Overall, there is also universal belief that Digital ID must remain voluntary and that other methods of identity verification must be retained for those who choose not to opt in to the Digital ID system.



Insights and considerations

Drawing on this year's research findings and trends observed over the six-year study, auDA has identified the following insights for future consideration. These are designed to support policymakers, industry, academia and the training sector to consider opportunities to enhance the digital experiences of Australians.

1

Increase awareness that small businesses are targets of cybercrime

2

Raise awareness of and normalise cyber security incident-response behaviours

3

Build understanding that simple practices can significantly reduce cyber risk

4

Tackle persistent job loss anxiety and build job-specific capability to support AI adoption

5

Actively support cohorts at risk of being left behind by AI

6

Raise awareness and unlock Digital ID value for small businesses

7

Increase practical cyber security and AI training opportunities

8

Build trust in Digital ID through increased use cases and reassurance

1

Increase awareness that small businesses are targets of cybercrime

Key insight

Many small businesses believe they are 'too small' to be targeted, and they are significantly less likely to put in place security protections.



Consideration

Target communications to explicitly challenge the 'too small to target' myth and promote baseline protections as non negotiable.

2

Raise awareness of and normalise cyber security incident-response behaviours

Key insight

Only half of consumers and two thirds of small businesses know where to report a data breach, and post incident action is limited among those affected.



Consideration

Continue to provide clear, simple incident response pathways and reporting guidance.

3

Build understanding that simple practices can significantly reduce cyber risk

Key insight

Almost half of small businesses feel helpless against cyber security threats on the basis their limited resources pale in comparison to larger corporate organisations that have fallen victim to cyber criminals.



Consideration

Continue investment awareness and education in cyber security practices with a focus on trusted, reliable, free resources such as cyber.gov.au and the Five P's of website security.

4

Tackle persistent job loss anxiety and build job-specific capability to support AI adoption

Key insight

AI is being used more, especially as it becomes integrated into commonly used applications such as search engines, but confidence remains moderate. AI adopters remain just as likely to believe AI will replace human workers.



Consideration

Embed AI training into workplace learning and business support programs, focused on practical, role based use cases. Emphasise the benefits of AI augmentation while reinforcing the need for 'human in the loop' processes (e.g. verifying outputs, protecting sensitive information, and understanding risks).

5

Actively support cohorts at risk of being left behind by AI

Key insight

Older Australians, people living with disability, and established small businesses show lower AI uptake, confidence and interest.



Consideration

Design targeted AI inclusion initiatives that address trust, relevance and perceived risk – not just access.

6

Raise awareness and unlock Digital ID value for small businesses

Key insight

The majority of small business owners are interested in the benefits of Digital ID and half have a current need to verify the identity of different groups that interact with the business.



Consideration

Increase awareness of Digital ID among small businesses to support uptake and help more businesses realise the benefits.

7

Increase practical cyber security and AI training opportunities

Key insight

Cyber security and AI are the most significant skills gaps for workers and small businesses. Australians' overall confidence online remains high, but confidence managing cyber security risks lags – many want to improve their cyber security but don't know how. As AI uptake accelerates, there is growing interest in training that helps people use AI effectively and responsibly.



Consideration

Accessible, trustworthy and practical training resources on cyber security and AI will support digital upskilling. Workplace training, online courses or webinars, and online video or self-guided tutorials are most in demand. Developing and delivering these resources would help build real-world capability for Australian workers and small businesses.

8

Build trust in Digital ID through increased use cases and reassurance

Key insight

Non users' concerns centre on data misuse, security and lack of clarity; education and increased availability increases comfort.



Consideration

Strengthen and clearly communicate Digital ID governance, enforcement and data security safeguards to build trust in the system.

Research methodology



Focus groups

The first stage of the research comprised eight online focus groups with n=55 participants in total, four groups were with consumers and four with small businesses. Participants were recruited to represent a mix of locations, gender, age, and life stage across Australia. The focus groups explored their experiences, attitudes and behaviours related to digital technologies and online activities.



In-depth interviews

10 qualitative in-depth interviews with 5 consumer and 5 small business participants were conducted. Participants were recruited to represent specific profiles (e.g. small businesses who have experienced a cyber attack, consumers working in a role with responsibility for cyber security and/or AI) and interviews focussed more specifically on their experiences.



Online survey

The survey was completed by 2,080 Australian adults (aged 18+) and 408 small business owners or managers. Participants were sourced from PureProfile, an opt-in market research panel.

Quota targets were set to ensure coverage of major demographic and business profile segments. Both samples were weighted to reflect their respective population profiles.

The consumer sample weighting included age, sex, geographic location, highest level of education, and workforce participation. The small business sample weighting included industry sector and geographic location.

Survey sample breakdown

		Consumers	Small businesses
Total		2,080	408
Gender	Male	1,027	--
	Female	1,053	
Region	5 Major Capital Cities (Sydney, Melbourne, Brisbane, Adelaide, Perth)	1,370	273
	Rest of Australia	710	135
Age	18-29	266	--
	30-39	503	--
	40-49	342	--
	50-59	250	--
	60-69	316	--
	70+	403	--
Personal characteristics	Employed / working		--
	Sole trader	1,322	203
	Micro business		151
Business size	Small business		54



Research questions

Many of the survey questions were retained from previous Digital Lives surveys to enable time series comparisons, which have been included in the report where appropriate. New questions were included in this year's research to further explore and measure attitudes, experiences and behaviours relating to artificial intelligence and cyber security.



Artificial intelligence (AI)

Artificial intelligence (AI) was used in the development of this report. A secure, enterprise version of Microsoft Copilot was used to analyse de-identified survey data, focus group discussions and interview transcripts to identify high level themes.

All report content was drafted by SEC Newgate's research team and reviewed and edited by auDA. Copilot was also used selectively to refine draft text for clarity and succinctness.

auda.org.au

To read auDA's suite of *Digital Lives of Australians* reports,
visit auda.org.au/DL

.au Domain Administration Ltd
ABN 38 079 009 340



Copyright © All copyright subsisting in the material contained in this publication is owned by .au Domain Administration Ltd unless otherwise stated. Except as provided by the Australian Copyright Act 1968 (Cth), no part of this publication may be reproduced without the prior written consent of the copyright owner.

All rights reserved.

