

METHODOLOGY DISCLOSURE STATEMENT

Client name	.au Domain Administration (auDA)
Project name	Digital Lives of Australians 2026 - How Australians use, trust and navigate the internet in 2026
Project reference	SNR 2511008 / AUDA009

Research dates:	Jan - March 2026
Target population:	Australian consumers (adults in the general population) and small businesses (owners, managers, or decision makers) with between 1 and 19 employees.
Research methodology:	Eight online focus groups with n=55 participants in total, four with consumers and four with small businesses. Participants were recruited to represent a mix of locations, gender, and age. In-depth interviews with five consumers and five small business participants followed, recruited to represent specific profiles and interviews focussed more specifically on their experiences. Participants for the qualitative research were incentivised with cash rewards for their time. This was followed by an online survey of a sample of n=2,080 consumers and n=408 small business owners or managers. The average survey completion time was 20 minutes. Survey participants were sourced via a commercial research panel and rewarded with points upon completion. All participation was on a voluntary, opt-in basis.
Weighting approach:	The sample was weighted to match ABS Census population data, using rim weighting. The consumer sample was weighted by age, gender, location, education and workforce participation. The small business sample was weighted by industry sector and location. For consumers, the effective sample size after weighting was approximately n=1,357 (a weighting efficiency of approx. 65%), equating to a margin of error of approximately +/-1.5% (at the 95% confidence interval) for estimates based on the total sample. For small businesses, the effective sample size after weighting was approximately n=303 (a weighting efficiency of approx. 75%), equating to a margin of error of approximately +/-2.9%.
Research questions:	The question line was created by SEC Newgate for the purpose of this research. All response options were visible to participants. A combination of single choice, multiple choice and open-ended (text response) questions were used. For multiple choice questions and statement grids, the order of response options was randomised to avoid potential order effect.

This research was conducted in accordance with the Australian Polling Council Quality Mark standards which can be viewed here: <https://www.australianpollingcouncil.com/>

Questions

Section 1: Value of the internet

NEW SCREEN FOR **SMALL BUSINESS**:

Please note: This survey focuses mainly on your business' use of the internet and online services but also includes some questions about your personal use as well.

The first few questions are about your business' use of the internet and online services. Please think about all the ways in which you use the internet and online services within the business.

NEW SCREEN FOR **CONSUMER**:

Q1AINTRO. Firstly, please think about all the ways you use the internet across all aspects of your life. This includes websites, apps, streaming services, and any device that connects to the internet.

1. Thinking broadly about the internet and online activities, overall, how confident would you say you are in using the internet?
1. Very confident 2. Somewhat confident 3. Neither confident nor unconfident 4. Somewhat unconfident 5. Very unconfident

CONSUMER ONLY

2. Which one of the following statements best describes how you personally feel about the internet?
1. The internet is invaluable, and I couldn't live without it 2. The internet adds a lot of value to my life, and I couldn't imagine life without it 3. The internet adds some value, but I could live without it 4. The internet doesn't add value to my life, I don't need it

CONSUMER ONLY.

2. Where do you work and how often?
1. In a dedicated place of business (e.g. office, factory, shop) - all the time 2. Work from home - all the time 3. Hybrid - a mix of working from home and working from a dedicated site 4. Somewhere else (please specify)
3. In a typical week, how many days do you work from home?

CONSUMER ONLY.

4. . Do you need the internet to do your job?
1. Yes, I could not do my job without it 2. No, I could do my job without the internet, but it helps make my job easier or better 3. No, I can do my job completely without the internet

SMALL BUSINESS ONLY

5. Which one of the following statements best describes how you feel about the internet and the role it plays in your business?
1. The internet is invaluable; the business couldn't function without it 2. The internet adds a lot of value; the business would struggle to function without it 3. The internet adds some value, but the business could function without it 4. The internet doesn't add any value; the business could function fully without it

6. **SMALL BUSINESS**: Does your business have a dedicated website?

1. Yes
2. No

7. Below are some **concerns** some people have when using the internet. Please indicate how much of a concern they are for [**CONSUMER** you. / **SMALL BUSINESS** your business.]

No concern at all

A minor concern

A major concern

1

2

3

1. Knowing who you can trust to keep your information secure
2. Ensuring the privacy of [your / your business'] online activities
3. Identifying fake content and misinformation online
4. **SMALL BUSINESS ONLY** Keeping business data secure
5. Avoiding online scams that could lead to financial losses and/or identity theft
6. Staying up-to-date with, and being able to use new digital technologies and platforms

Section 2: Cyber security

Next there are some questions about online security, including your privacy and data security when using the internet.

8. Which of the following best describes how concerned you are – if at all – about online security overall? By online security we are talking about the security of your [**CONSUMER**: personal] / [**SMALL BUSINESS**: business] data, online privacy, and the devices and networks that you use.

1. Not at all concerned
2. Not very concerned
3. Somewhat concerned
4. Quite concerned
5. Very concerned

9. How **confident** are you in each of the following?
Select one answer for each.

Very confident

Somewhat
confident

Neither confident
nor unconfident

Somewhat
unconfident

Very unconfident

1

2

3

4

5

1. Keeping your [**CONSUMER**: personal] / [**SMALL BUSINESS**: business] information secure online
2. **SMALL BUSINESS ONLY** Storing your staff and clients' personal data securely online
3. Spotting an online scam
4. Knowing where to report a data security breach
5. **SMALL BUSINESS ONLY** Knowing what to do if any of your business accounts are hacked or your business has an online security breach
6. Creating strong passwords/passphrases for websites or apps
7. Spotting misinformation or 'fake news'
8. Safely backing up [**CONSUMER**: your] [**SMALL BUSINESS**: your business'] data and files
9. Finding reputable information on how to be secure online
10. Using multifactor authentication (e.g. SMS codes, or mobile phone authentication apps)
11. Recognising a phishing scam email

10. Thinking now about online security. Which of the following, if any, [**CONSUMER: do you personally** / **SMALL BUSINESS: does your business**] do currently? Please select all that apply.

1. Use a password manager that you pay a fee to use
2. Use a free password manager
3. Avoid saving passwords in an internet browser (e.g. Chrome, Safari, Edge)
4. Use multifactor authentication where available (e.g. an SMS with a 6-digit number)
5. Apply password protection/encryption to digital documents
6. **SMALL BUSINESS ONLY** [IF HAVE A WEBSITE] Regularly check your website security with an online tool
7. Maintain up-to-date antivirus software on [**your computer** / **your business' computers**]
8. **CONSUMER ONLY** Adjust settings on social media platforms to restrict who has access to your content
9. **SMALL BUSINESS ONLY** Restrict access to who can login and post on your business' social media accounts
10. **CONSUMER ONLY** Use pseudonyms or avatars instead of your real name or photograph when creating an online profile
11. Have a hardware firewall installed for your [**CONSUMER: home**] [SMALL BUSINESS: business'] computer network
12. **SMALL BUSINESS ONLY** Employ someone internally with responsibility for cyber security
13. **SMALL BUSINESS ONLY** Use an external IT and/or cyber security consultant
14. **SMALL BUSINESS ONLY** The business has a documented cyber security policy
15. **SMALL BUSINESS ONLY** Regularly talk about cyber security with others in the business
16. **SMALL BUSINESS ONLY** Provide staff with cyber security training
17. **SMALL BUSINESS ONLY** Provide staff with regular cyber security training (i.e. monthly, quarterly etc.)
18. **SMALL BUSINESS ONLY** Audit cyber security practices and procedures on a regular basis (i.e. annually)
19. **SMALL BUSINESS ONLY** The business has an incident response plan in place
20. **SMALL BUSINESS ONLY** The business has a documented AI-related security policy
21. Don't do any of these things <ANCHOR> <EXCLUSIVE>
22. Unsure <ANCHOR> <EXCLUSIVE>

11. [Q11 NOT = UNSURE] You indicated [**you're not** / **your business isn't**] currently doing the things listed below.

[Q11 = UNSURE] You indicated you're unsure if **you are** / **your business is** currently doing any of the things listed below.

Please select the cyber security measures that you would be interested in implementing.

Relevant unselected codes from Q11 shown.

12. You've said you are interested in implementing the following security measure / measures:
[Codes selected at Q12]

What is holding you back from implementing this?

1. I'm not sure how to do this
2. I don't have the time to implement this
3. It would be too expensive
4. I don't think [I need / the business needs] this
5. None of the above <EXCLUSIVE><ANCHOR>

13. If you needed to find out more about online security, or you needed to upgrade **[CONSUMER: your / SMALL BUSINESS: your business]** online security practices, who would you go to for help? Select all that apply.

1. Family
2. Friends
3. Work colleagues
4. Workplace IT support
5. Google (or another search engine)
6. ChatGPT (or another AI tool)
7. Online resources (e.g. YouTube videos)
8. Government websites (e.g. cyber.gov.au or esafety.gov.au)
9. A website or email registrar (e.g. GoDaddy)
10. Online forums / discussion boards
11. **[SMALL BUSINESS ONLY]** IT or cyber security consultant
12. Someone else (please specify) <SPECIFY>
13. No one **<EXCLUSIVE"> <ANCHOR>**
14. Not sure **<EXCLUSIVE"> <ANCHOR>**

14. Following are some things other people have said about online security. Please indicate how much you **agree or disagree** with each statement.

Please select one answer for each statement

Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree
1	2	3	4	5
1. Cyber criminals are becoming smarter and more sophisticated, so it is important to stay up to date with the latest online security trends 2. [CONSUMER] I feel confident I have safeguards in place to keep my personal data secure online 3. [SMALL BUSINESS] I feel confident the business has safeguards in place to keep its data secure online 4. I am not worried about cybercrime as I don't feel I have much to lose 5. [CONSUMER] I am more worried about cyber security at home than I am at work as I don't have the resources at home to guard against it 6. 10. Companies should be doing more to protect the personal information of their customers from cyberattacks 7. Companies should be subject to penalties if they fail to protect their customers' personal information from cyberattacks 8. I am comfortable sharing my personal information with apps and websites in order to receive information or content that is tailored to my individual goals or situation 9. I trust providers of apps and websites to keep my personal information secure 10. [SMALL BUSINESS] My business wouldn't be a target for cyber criminals because it's too small 11. [SMALL BUSINESS] If larger, well-resourced companies can't protect against cyber attacks, then I can't protect my small business				

SMALL BUSINESS ONLY

15. Approximately how much does the business spend each year on **cyber security**?
Please type in the amount to the nearest dollar (no decimals or cents).

1. **RECORD \$ AMOUNT (RANGE \$0 - \$999,999)**
2. Don't know

SMALL BUSINESS ONLY

16. How much does the business intend to spend on cyber security in 2025?

1. Less than last year
2. About the same

3. More than last year
4. Don't know

CONSUMER ONLY

17. Are there any online activities that you actively **avoid** due to fear or concerns you have about online security, including potential personal data leaks and scams?
Select all that apply.

1. Internet or mobile banking
2. Using social media, including posting your own content on social media
3. Communicating with others using instant messaging apps (e.g. WhatsApp, Messenger)
4. Buying groceries online
5. Buying products (other than groceries) or services online
6. Using an internet enabled wearable device (e.g. Apple Watch, Fitbit)
7. Selling products online (e.g. via eBay, Gumtree, Facebook Marketplace)
8. Accessing government services online (e.g. MyGov, Medicare)
9. Using a virtual assistant (e.g. Amazon's Alexa, Apple's Siri or Google Assistant)
10. Using generative AI tools (e.g. ChatGPT)
11. Interacting with other players while gaming online
12. Managing health and/or general wellbeing through apps or online services
13. None of these / Don't avoid any online activities because of online security concerns **<ANCHOR>**
<EXCLUSIVE>

SMALL BUSINESS ONLY

18. Are there any online activities that your business actively **avoids** due to fears or concerns about online security?
Select all that apply.

1. Promoting the business via paid online advertising on third party websites (not including social media)
2. Using social media platforms to advertise or promote the business
3. Promoting your business using search engine optimisation (SEO)
4. Selling products via an online marketplace (e.g. eBay)
5. Taking bookings via an online booking system on your own or a third-party website
6. Using online platforms for business functions (e.g. payroll, accounts, HR, CRM)
7. Using online collaboration solutions for staff to communicate (e.g. Microsoft Teams)
8. Recording / monitoring staff attendance
9. Using online platforms for inventory and stock control
10. Collecting feedback from customers or clients
11. Using generative AI tools (e.g. ChatGPT)
12. Using AI chatbots to interact with customers
13. Online banking
14. Allowing staff to work remotely
15. Something else (please specify) **<SPECIFY>**
16. None of these / Don't avoid any online activities because of online security concerns **<ANCHOR>**
<EXCLUSIVE>

19. Which of the following do you think would be most helpful to strengthen your online security?
Please select up to five (5) things that you would find most helpful.

1. Update settings to restrict certain content
2. Enable automatic updates on your devices
3. Enable ransomware protection on your devices
4. Avoid saving passwords in your device or web browser
5. Avoid saving credit card details in your device or web browser
6. Change passwords more regularly
7. Use more complex passwords
8. Avoid using the same password for multiple sites or accounts
9. Avoid connecting to public Wi-Fi (e.g. at shopping centres or airports)
10. Delete or deactivate online accounts you no longer use
11. Use an adblocker to block tracking pixels
12. Increase privacy settings on social media accounts
13. **[SMALL BUSINESS ONLY]** Educate staff about online security risks so they know what to avoid
14. **[SMALL BUSINESS WITH DEDICATED WEBSITE]** Ensuring access to your website content management system is restricted
15. **[SMALL BUSINESS ONLY]** Remove third-party integrations and permissions that are no longer in use
16. **[SMALL BUSINESS WITH DEDICATED WEBSITE]** Apply updates and security patches to your website CMS, including plugins, as soon as they become available
17. Don't know <ANCHOR> <EXCLUSIVE>

20. Have you done any of the following in the past 12 months?
Please select all that apply.

1. Updated settings to restrict certain content
2. Enabled automatic updates on your devices
3. Enabled ransomware protection on your devices
4. Avoided saving passwords in your device or web browser
5. Avoided saving credit card details in your device or web browser
6. Changed passwords regularly
7. Used more complex passwords
8. Avoided using the same password for multiple sites or accounts
9. Avoided connecting to public Wi-Fi (e.g. at shopping centres or airports)
10. Deleted or deactivated online accounts you no longer use
11. Used an adblocker to block tracking pixels
12. Increased privacy settings on social media accounts
13. **[SMALL BUSINESS ONLY]** Educated staff about online security risks so they know what to avoid
14. **[SMALL BUSINESS WITH DEDICATED WEBSITE]** Ensured access to your website content management system is restricted
15. **[SMALL BUSINESS ONLY]** Removed third-party integrations and permissions that are no longer in use
16. **[SMALL BUSINESS WITH DEDICATED WEBSITE]** Applied updates and security patches to your website CMS, including plugins, as soon as they become available
17. None of these <ANCHOR> <EXCLUSIVE>

CONSUMER ONLY

21. In the past year, have you experienced any of the following?

1	2	99
Yes	No	Don't know
1. A password of yours had been compromised in a data leak 2. Your personal data had been compromised in a data leak 3. Visited or purchased items from a fake online store, e.g. goods never delivered or clearly fake 4. Been a victim of a financial scam where you lost money 5. Been a victim of a romance scam		

22. **[IF RECEIVED NOTIFICATION OF DATA BREACH]** What did you do after this happened?
 Please select all that apply.

1. Change password for the site or account affected
2. Change passwords for other sites or accounts
3. Cancel or deactivate the affected account
4. Switch to another provider
5. Check details to decide what action I needed to take
6. Contact the company to find out more
7. Contact the company to complain
8. Upgrade virus protection or security software on my devices
9. Contact the police
10. Report to cyber.gov.au
11. Comply with any requests of the scammer or hacker
12. Contact my bank
13. Something else (please specify)
14. Nothing **<ANCHOR> <EXCLUSIVE>**

23. What are the main reasons for implementing measures to protect your **[CONSUMER] own cyber security?** / **[SMALL BUSINESS] business's cyber security?**

Please select up to 5

1. **[CONSUMER]** Keeping **your own** personal data secure online
2. **[CONSUMER]** Keeping your **family secure** online
3. **Reducing the risk** of online scams and other types of cybercrime such as identity theft
4. Avoiding the **stress and hassle** that might come with being a victim of cybercrime
5. Avoiding the **embarrassment** if your private information was leaked
6. **Keeping up** with the scammers and hackers
7. Avoiding **financial loss**
8. **[SMALL BUSINESS ONLY]** Keeping **the business's own** data secure online
9. **[SMALL BUSINESS ONLY]** Keeping **staff** data secure online
10. **[SMALL BUSINESS ONLY]** Keeping **clients'** data secure online
11. **[SMALL BUSINESS ONLY]** Protecting your reputation and trust among your clients
12. **[SMALL BUSINESS ONLY]** Ensuring the business can **keep operating** through an incident
13. **[SMALL BUSINESS ONLY]** Having a **competitive advantage**
14. **[SMALL BUSINESS ONLY]** Meeting **compliance criteria** for laws and regulations, such as the *Australian Cyber Security Act 2024*
15. **Peace of mind**
16. **[SMALL BUSINESS ONLY]** Reducing the likelihood of a **significant data breach** or cyber attack
17. Other (please specify) **<ANCHOR>**

SMALL BUSINESS ONLY

24. Which of the following types of data does your business hold for each of the following groups?

Please select all that apply

1. Identification documents (to verify employee or customer identity)
2. Documents with confidential or sensitive information
3. Personal references
4. Banking or credit card details (for employees, customers, or suppliers)
5. Invoice and transaction records
6. Payslips
7. Contracts or agreements
8. Emails and online messages / conversations (e.g. Teams, Slack)
9. Other (please specify) **<ANCHOR>**

10. None of these <ANCHOR> <EXCLUSIVE>

SMALL BUSINESS ONLY

25. Does your business currently have any of the following types of data infrastructure, processes and policies in place?		
1	2	99
Yes	No	Not sure
1. Physical infrastructure such as physical server on business premises, Network Attached Storage (NAS) or a Storage Area Network (SAN) 2. A cloud-based storage service 3. Requirements for data encryption, password protection and device security and network protection 4. Access controls that restrict data access to specific levels of employees or specific individuals 5. Data retention practices, e.g. policies for disposing of data once no longer needed or within a specified timeframe, and policies for back-up of data 6. Data handling practices, e.g. policies for safe transfer of data within and outside the business 7. Data security training for employees 8. Regular review of policies and processes to stay up to date with latest threats 9. Data breach response plan 10. Privacy training for staff		

ONLY ASK IF SMB HAS DATA RETENTION PRACTICES IN PLACE

26. How often does the business back-up data?
1. Every day 2. At least once a week 3. Every couple of weeks 4. Once a month 5. Every few months 6. Once a year 7. Less often

27. How often does the business delete any personal or sensitive data that it holds that it no longer requires?
1. 1-2 years 2. 3-7 years 3. + 7 years 4. Periodically, but not according to a set time period 5. Never

SMALL BUSINESS ONLY

28. In the past year, has your business experienced any of the following?		
1	2	99
Yes	No	Don't know
1. Your business experienced a cyberattack (such as a malware attack) 2. Your business's data was compromised in a data breach 3. Had business accounts hacked, resulting in financial loss (even if the money was returned)		

4. Your business received a ransomware demand
5. Your business received an email that you believed was a phishing scam

[If Yes to Q29]

29. How did this incident / these incidents affect your business and/or you personally?

OPEN ENDED

30. What did you do after you became aware of this incident / these incidents?

Please select all that apply

1. Inform the business's IT team
2. Hire an external cyber consultant for assistance
3. Inform the business's cyber insurance provider
4. Inform the individuals impacted by the incident to outline next steps for data recovery
5. Change password for the site or account affected by the data leak
6. Change passwords for other sites or accounts
7. Cancel or deactivate the affected account
8. Upgrade virus protection or security software on my devices
9. Contact the police
10. Report to cyber.gov.au
11. Comply with the requests of the hacker
12. Contact the business' bank
13. Contact service provider (e.g. the telecommunications company if the breach was on your phone)
14. Something else (please specify) <ANCHOR>
15. Nothing / Would not do anything <ANCHOR> <EXCLUSIVE>

31. If another small business was in a similar situation, what do you think would be the most important thing they could do to strengthen their cyber security and cyber threat response?

OPEN ENDED

32. Which of the following - if anything - do you look for to determine whether a website is secure and trustworthy?

1. The padlock symbol in the browser bar
2. The pre-text in the web address, i.e. http or https
3. The spelling of the website address
4. The domain name suffix / namespace (e.g. .com or .com.au)
5. The businesses contact details indicate it operates in Australia
6. Referrals from family or friends
7. A well-designed website
8. A professional looking website
9. Notifications from software protection (e.g. Norton)
10. Something else **(please specify)**
11. Nothing in particular <ANCHOR> <EXCLUSIVE>

ASK ONLY FOR SMBS WITH WEBSITE

33. Which of the following - if any - does your business do to keep its website secure?

1. Set up auto-renew settings for your website's domain to ensure the domain doesn't expire

2. Ensure any domain renewal reminder notifications are sent to more than one employee
3. Require multi-factor authentication (MFA) for any customer logins
4. Set password strength requirements for any customer logins
5. Use a more secure hypertext transfer protocol (HTTPS) in place of standard HTTP for your website's address
6. Limit website administration access to those that need it
7. Only provide specific website administration privileges for individual roles and responsibilities
8. Use a website hosting service that provides high-quality security features, e.g. malware detection, regular or automated data backups, and firewalls
9. I outsource website security to a professional, who knows more about it than I do
10. Something else **(please specify)** <ANCHOR>
11. Nothing in particular <ANCHOR> <EXCLUSIVE>

Section 3: Digital Identification

The next set of questions ask about digital identification.

34. How much do you feel you know about Australian **digital identity** (often referred to as Digital ID)? *Don't worry about looking it up if you're not sure - we'll give you some info in the next question.*
 1. **Nothing at all**
 2. **Not much** - I would need someone to explain this to me
 3. **A little** - I have some understanding but would struggle to explain it to others
 4. **A fair bit** - I could explain it at a basic level only
 5. **A lot** - I am confident I could explain it in detail to others

NEW SCREEN

Digital ID in Australia refers to a secure and streamlined system that allows individuals and businesses to verify their identity online when accessing government and private sector services.

You can set up a Digital ID via a small number of providers, accredited by the Australian Government and use your Digital ID to prove who you are without having to provide physical documents. Examples include myID, (previously known as myGovID).

Digital ID aims to enhance convenience, and security by reducing the need to share personally identifiable information. Note that a digital driver's licence is not a Digital ID.

35. Do you currently have a Digital ID set up?

1. Yes
2. No
3. Not sure

IF HAVE DIGITAL ID

36. Which of the following Digital IDs do you have?

1. My ID (formally myGovID)
2. Digital iD™ by Australia Post
3. NSW Digital ID
4. IDVerse by OCR Labs
5. ConnectID®
6. None of the above <ANCHOR>

ASK SMB ONLY

37. Does the business ever need to verify identity of any of the following groups?

1. Customers

2. Suppliers
3. Employees
4. Visitors
5. Someone else (please specify) **<SPECIFY>**
6. None of these **<EXCLUSIVE> <ANCHOR>**

ASK IF NEED TO VERIFY IDENTITY. REPEAT FOR EACH CODE SELECTED.

38. Does the business currently accept Digital ID for verifying the identity of [CODE SELECTED] ?		
A. Yes	B. No	C. Not sure
1. [SELECTED CODE]		

ASK IF DO NOT OR UNSURE IF THEY ACCEPT DIGITAL ID FOR ANY. REPEAT FOR EACH CODE NOT SELECTED

39. Would you be interested in being able to accept Digital ID for any of the following reasons in the future?	
CAROUSEL FORMAT	
A. Yes	B. No
1. [NOT SELECTED]	

ASK ALL

40. How much do you agree or disagree with the following statements about Digital ID?					
RANDOMISE STATEMENTS					
Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree	Don't know
1	2	3	4	5	99
1. Digital ID systems should be voluntary, not compulsory 2. I would feel that my privacy is more secure using a Digital ID instead of providing copies of personal documents 3. Using a Digital ID would be a more convenient way of accessing government services, such as Centrelink, Medicare, NDIS. 4. Using a Digital ID would be more convenient when submitting applications or opening accounts 5. Digital ID can make your life easier by reducing the need to provide hard-copies or scans of personal documents 6. I worry that my personal information could be hacked or stolen through Digital ID 7. I worry that my personal information could be used for other unintended purposes through Digital ID 8. Digital ID providers must be regulated and held accountable for any privacy breaches that occur 9. I am confident that my personal information is secure in Digital ID as it has in-built security features 10. I would feel more secure sharing personal documents rather than having a Digital ID 11. I'd be more likely to use Digital ID if I could use the one Digital ID with all service providers 12. [SMALL BUSINESS ONLY] I'd be more likely to accept digital ID as a form of identity verification if it was an easier and more affordable process					

ASK IF DO NOT HAVE DIGITAL ID OR UNSURE

41. How interested are you in setting up a Digital ID [CONSUMER] to use when verifying your personal identity? / [SMALL BUSINESS] to use when verifying your personal identity for business purposes (e.g. accessing ATO online)?	
1. Not at all interested 2. Not very interested 3. Somewhat interested 4. Quite interested	

5. Very interested

Section 4: Digital skills

Now some questions about your interest in, and ability with, a range of digital skills.

ASK ONLY IF NOT RETIRED

42. How **important** are each of these online activities to your [**CONSUMER**: job / career, **SMALL BUSINESS**: business] whether now or in the future?

RANDOMISE

Not at all important	Not very important	Somewhat important	Very important	Essential
1	2	3	4	5
1. Coding and programming (e.g. Python, Java) 2. Data analytics (e.g. R, SQL) 3. Online collaboration tools (e.g. SharePoint, Trello) 4. Website development and maintenance 5. Digital marketing 6. Maintaining a social media presence 7. Ability to use Artificial Intelligence (AI) (e.g. ChatGPT, Copilot) 8. Data visualisation 9. Using Customer Relationship Management (CRM) software (e.g. Salesforce, HubSpot) 10. Cyber security skills (e.g. data security, secure app development, cloud and network security, cyber threat intelligence, incident response, risk management, security compliance)				

ASK ALL

43. How would you rate your [**CONSUMER**: ability, **SMALL BUSINESS**: business' capability] with each of these online activities?
Please select one answer for each activity.

RANDOMISE ACTIVITIES

[I have no idea how to do this / Zero capability with this]	[I would need some guidance to do this / Limited capability with this]	[I could do this without any guidance / High capability with this]
1	2	3
1. Coding and programming (e.g. Python, Java) 2. Data analytics (e.g. R, SQL) 3. Online collaboration tools (e.g. SharePoint, Trello) 4. Website development and maintenance 5. Digital marketing 6. Maintaining a social media presence 7. Ability to use Artificial Intelligence (AI) (e.g. ChatGPT, Copilot) 8. Data visualisation 9. Customer Relationship Management (CRM) software (e.g. Salesforce, HubSpot) 10. Cyber security skills (e.g. data security, secure app development, cloud and network security, cyber threat intelligence, incident response, risk management, security compliance)		

ASK CONSUMER: ASK ONLY IF NOT RETIRED

44. How interested would you be to develop skills in and/or work in the following types of roles?

RANDOMISE

Not at all interested	Not very interested	Somewhat interested	Quite interested	Very interested
1	2	3	4	5
1. Web and app development 2. Data science 3. User experience (UX) design 4. IT support 5. Software engineering 6. Network and systems administration 7. Cyber security analysis 8. AI prompt engineering				

ASK IF INTERESTED IN AT LEAST 1 OF Q45

45. What support would you find most helpful in developing any of these skills?
1. Training within your workplace 2. Online training course or webinar 3. Free community workshop (in person) 4. Online video guides or tutorials (self-guided) 5. Regular newsletter or email with how-to guides, tips and tricks, etc. 6. Online forum where you can interact with other users 7. Something else (please specify) <SPECIFY> <ANCHOR>

ASK CONSUMER: ASK ONLY IF NOT RETIRED

46. Here are some things people have said about working in technology and IT roles. How much do you personally agree or disagree with each statement?				
Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree
1	2	3	4	5
1. I don't have the required technical skills 2. I don't fit the norm of a typical 'IT worker' 3. There are a lack of role models or mentors who I can look to for guidance and support 4. The IT / technology sector is too male-dominated 5. Technology moves too quickly and it is too difficult to keep pace with changes 6. There should be more women working in online and IT-related roles because diverse perspectives are crucial for innovation and problem solving 7. Societal norms and expectations in Australia prevent women from entering the technology sector 8. [ASK WOMEN ONLY] I would be more inclined to consider working in technology or IT if there were initiatives designed to support entering the sector such as mentorships and internships 9. [ASK WOMEN ONLY] I would be more inclined to consider working in technology or IT if companies demonstrated inclusivity such as greater female representation at management level and diverse interview panels				

Section 5: Artificial Intelligence (AI)

Now some questions about artificial intelligence (AI).

47. Overall, how confident would you say you are using AI?
1. Very confident 2. Somewhat confident 3. Neither confident nor unconfident 4. Somewhat unconfident 5. Very unconfident

48. How much do you agree or disagree with the following statements about artificial intelligence (AI)?

Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree	Don't know
1	2	3	4	5	99
1. AI will deliver positive social outcomes 2. AI will deliver positive economic outcomes 3. AI will replace human workers and lead to unemployment 4. I would feel more comfortable about AI if there were stronger regulatory safeguards around it 5. When I need < CONSUMER service> < SMALL BUSINESS > service or support with a business-related issue>, I would be just as happy to interact with an AI chatbot as I would to interact with a human 6. CONSUMER ONLY. ASK IF NOT RETIRED: Being able to use AI tools will increase my employment prospects 7. SMALL BUSINESS: Being able to use AI tools will increase my business' efficiency 8. I would like to learn more about AI and how it could benefit < CONSUMER: me in my life / SMALL BUSINESS: my business> 9. I trust the information provided by AI platforms is accurate and reliable 10. I would be able to identify text or images that have been created by AI SMALL BUSINESS: I just don't have the time or expertise to use AI within my small business, even though it could fall behind as a result of this 11. SMALL BUSINESS: Using AI will help my business to stay competitive					

49. Have you ever used artificial intelligence (AI) for any of the following purposes?
Please select all that you have done, even if only once.

1. Summarise reports and research papers into executive summaries 2. Condense long emails, meeting notes, and documents into key points 3. Analyse data or analytics and explain insights in plain language 4. Generate logos, brand assets, and marketing visuals 5. Create images, posters, and presentation graphics 6. Edit or enhance images and media (e.g. photos, headshots) 7. Draft emails, reports, briefs, and presentations 8. Translate or simplify complex or technical language 9. Support email management, e.g. large mail-outs 10. Automate administration processes, e.g. payroll 11. Answer questions and explain unfamiliar topics quickly 12. Compare options (e.g. products, travel, vehicles) to support decisions 13. Act as a research assistant to gather and check information 14. Generate ideas for events, workshops, lessons, or activities 15. Something else (please specify) < ANCHOR < SPECIFY > 16. None of these / Haven't used AI for any purpose < ANCHOR < EXCLUSIVE >					
---	--	--	--	--	--

CONSUMER ONLY

50. How much are you using artificial intelligence (AI), if at all?

In your personal life	SHOW IF EMPLOYED In your workplace	SHOW IF STUDENT In your studies
1	2	3
1. Use it regularly 2. Use it occasionally 3. Used it once or tried using it 4. Thinking about using it		

5. **[SHOW ONLY IF EMPLOYED UNDER 'IN YOUR WORKPLACE']** The use of AI is not allowed at my workplace
6. **[SHOW ONLY TO STUDENTS UNDER 'IN YOUR STUDIES']** The use of AI is not allowed for my studies
7. Never / not thinking about using it

SMALL BUSINESS ONLY

51. To what extent is your business using artificial intelligence (AI), if at all?

1. Use it regularly
2. Use it occasionally
3. Used it once or tried using it
4. Thinking about using it
5. Not using it and not thinking about using it
6. Do not allow our employees to use it

ASK ALL WHO USE AI REGULARLY OR OCCASIONALLY

52. To what extent has your use of AI led to improvement in...?

No improvement	Not much improvement	Some improvement	Moderate improvement	Big improvement
1	2	3	4	5
1. Productivity 2. Time saving 3. Quality of your work 4. Creativity and idea generation 5. Problem solving				

53. Overall, how do you feel about advances in artificial intelligence (AI) compared to a year ago? Would you say you are...?

1. A lot more negative
2. A little more negative
3. About the same
4. A little more positive
5. A lot more positive

54. What type of regulatory safeguards, if any, do you feel are most important when it comes to the use of AI?

Please select up to five (5) that you feel are most important.

1. Rules against collecting or using personal or sensitive data to train AI models without consent
2. Data security requirements that AI platforms must adhere to
3. Mandatory digital watermarking of AI-generated content
4. Mandatory disclosure if AI is used for commercial purposes
5. Clear accountability guidelines for ensuring AI generated content is accurate
6. Clear accountability guidelines for ensuring AI generated content is legal
7. Rules against using AI in ways that may cause harm to individuals

8. Ability for users to report false or offensive AI-generated information to AI platforms and/or regulatory bodies
9. Other type of regulation (please specify) **<SPECIFY>** **<ANCHOR>**
10. None of the above **<ANCHOR>** **<EXCLUSIVE>**

ASK ALL

55. How familiar are you with these different types of AI?

Generative AI	Agentic AI
1. I have a good understanding of what this is	
2. I have heard of it, but not too sure what this is	
3. I have not heard of this type of AI	

56. Here is some more information about generative and agentic AI.

Generative AI: Software that **creates**. This kind of AI creates new content based on prompts, for example "Write a follow-up email" or "Summarise this report". It excels at producing text, images, or code quickly. This acts more like a **creative engine**.

Agentic AI: Software that **automates**. This kind of AI takes a goal and completes it through multiple steps. It may analyse, decide, fetch data, communicate with other programs or servers, update documents, and notify stakeholders, for example "Research our top five competitors, prepare a comparison sheet, and email a one-page summary to the team." This acts more like an **assistant**.

Now that you know a bit more about generative and agentic AI, how interested are you in using each of these tools?

Not at all interested	Fairly uninterested	Neither interested nor uninterested	Fairly interested	Very interested
1	2	3	4	5
1. Generative AI				
2. Agentic AI				

ASK ALL WHO USE AI RARELY OR NEVER, EXCLUDING THOSE WHO SAY THEY CAN'T USE IT DUE TO WORK/STUDY RESTRICTIONS

57. **CONSUMERS:** You mentioned that you are not using AI very often in your personal life / at work / for your studies. What is the reason for this?
- SMALL BUSINESS:** You mentioned that your business is currently not using AI very often. What is the reason for this?

58. Here are some things people have said about why they are not using AI. Please select any reasons you agree with.

1. I don't believe I have the skills to use it correctly
2. I have used it before but didn't like using it
3. I don't have a reason to use it
4. I don't believe it would be useful or helpful
5. I'm not interested in using it
6. I don't like that it might be taking other people's jobs / replacing people
7. I don't trust AI generated content
8. I feel uncomfortable about the lack of regulatory safeguards
9. I am worried about inputting my personal information into AI for privacy reasons
10. It takes too long to get the output I want from AI
11. Another reason **<SPECIFY>** **<ANCHOR>**

12. None of these <ANCHOR> <EXCLUSIVE>

ASK CONSUMERS AND SMALL BUSINESSES WHO CAN USE AI AT WORK (OR ARE UNSURE IF THEY USE IT)

59. Has your [CONSUMER] employer / [SMALL BUSINESS] business undertaken any of the following initiatives regarding use of AI?

1. Yes	2. No	3. Don't know
--------	-------	---------------

1. Introduced a formal AI policy, with clear usage guidelines that must be followed
2. Introduced informal guidelines for AI usage
3. Provided resources such as prompt templates to help AI users
4. Arranged AI training for employees (either a program or informal on-job training)
5. Introduced integrated AI services (such as Copilot) that offer more secure use
6. Introduced restrictions on which AI platforms can and cannot be used in the workplace
7. Provided access to premium AI subscriptions/services
8. Something else (please specify) <ANCHOR> <SPECIFY>
9. None of these <ANCHOR> <EXCLUSIVE>

60. Would you find it useful if [CONSUMER] your employer / [SMALL BUSINESS] your business introduced any of the following initiatives for AI usage [CONSUMER] at work / [SMALL BUSINESS] for your business?

Please select all that apply.

1. [SHOW ANY CODES =2 OR 3 AT Q60]
2. Something else (please specify) <ANCHOR> <SPECIFY>
3. None of these <ANCHOR> <EXCLUSIVE>

ASK n=100 EACH OF CONSUMER AND SMALL BUSINESS SAMPLE. ROTATE ORDER OF Q62 and Q63 FOR 50%

61. Below is an example of an email that someone might receive. Please have a look at this email and place:

- **green highlight** against anything that would reassure you that this email was legitimate
- **red highlight** against anything that you would see as suspicious and potentially a sign of a scam or phishing attempt.

From: ATO Refunds <support@ato-refundportal.com>

Subject: URGENT: You are owed a tax refund – action required within 24 hrs

Dear Taxpayer,

Our system has recalculated your taxable income and determined you are owed a refund of \$1,287.52.

To release your refund, please verify your details immediately:

Click here to claim your refund

<https://ato-refund-confirmation.com/login>

Failure to act will delay your payment and may lead to penalties.

Sincerely,

ATO Processing Centre

62. Below is another example of an email that someone might receive. As before, please have a look at this email and place:

- **green highlight** against anything that would reassure you that this email was legitimate
- **red highlight** against anything that you would see as suspicious and potentially a sign of a scam or phishing attempt.

From: Australian Taxation Office <no-reply@ato.gov.au>

Subject: Reminder: Check your myGov inbox for new ATO correspondence

Hi Olivia,

You have a new message from the ATO in your myGov inbox.

For your security, we do not include links in our emails.

Please sign in to myGov by typing my.gov.au into your browser.

If you weren't expecting a message or want to confirm, please phone us on 1800 008 540.

Kind regards,

Australian Taxation Office