Real Digital Risk Report 2023

August 2023

real INSURANCE®

Contents

About the report 03

Key findings 04

Australian digital risk concerns 10

Fear of online risks is high 11

Which risks concern us the most? 12

Are we comfortable sharing our details? 13

Are we asking for it? 14

Online privacy 15

Are we safe from computer viruses? 16

Social media is a risk 17

Australians at risk of scams 18

The scam marketplace 19

Scams impact more than just the bank 20

Online scam tactics 21

Do we know we've been scammed? 22

Where are we most exposed? 23

Tips to avoid digital risk 24

Spending on cybersecurity 25

Staying 'scam savvy' 26

Data security measures 27

Digital security measures 28

How are we protecting ourselves? 29

Australian families online 30

Most kids have internet access 31

How old are kids when they start using socials? 32

Family safety online 33

What concerns parents the most? 34

Experiences of children online 35

Keeping your family safe online 36

Safety is paramount 37

How far do parents go to protect their kids? 38

Emerging AI language tools 39

Aussies are starting to use AI language tools 40

There is concern around information being shared with AI language tools 41

real INSURANCE®

About the report

The *Real Digital Risk Report 2023* forms part of the Real Insurance Research Series and explores feelings around the risk associated with being active online, and how it is affecting Australians. The research also looks at concerns of parents around their family's safety online and the perceptions around the increasing use of language AI tools.

The report is compiled based on research commissioned by Real Insurance and conducted by CoreData between 29 March and 12 April 2023.

The research was conducted via a quantitative online survey, gathering 5,054 responses from Australians over 18 years old. The usage of the term Australians in this report refers to the respondents of the survey or the family members and acquaintances of respondents.

Important things to note about the charts in this report

- ✓ Footnotes directly underneath the charts may refer to one or more of the below dependent on the data presented. If more than one note is required, it would appear as a bulleted list.
    - Subset of the total sample size as certain questions would only be asked to specific respondents (e.g. n = 3,698, Have been targeted by online, email or phone scams).
    - Types of questions asked, for instance Multiple answers allowed appears when the question called for more than one answer from the respondent.
    - Data has been excluded from analysis (e.g. Outliers removed in analysis).
- ✓ Charts without a specific note represent questions that were asked to all respondents.
- ✓ Some charts and figures may not be equal to 100% due to rounding differences. This is also true for summed up figures.

Key findings

Key findings

Many Australians over 18 are reporting their fear of online risks as high

- Approximately 69% of Australians rate their fear of online risk as high.
- Less than half (46%) are very or extremely confident in their understanding of the risks associated with being online.
- The safety of their private information online is one of the primary concerns for 92% of Australians and 90% are concerned about scams.
- Australians believe they are most exposed to online risks through smartphones (73%), computers (69%) and smart home devices (19%).
- The online activities considered to pose the greatest risk to Australians are emails (49%), social networking (48%) and phones listening to them and collecting data without their knowledge or consent (43%).
- Just under half (48%) feel comfortable sharing their personal health information online.
- Less than a quarter (23%) have provided personal health information online to individuals or entities other than medical or insurance providers.
- Just under one-third (32%) estimate they have shared their personal information with more than 10 websites/online providers in the past year.
- Almost all (97%) agree that there should be tougher penalties for cybercriminals in Australia.
- Nearly 9 in 10 (89%) believe the Australian government should ban certain foreign companies if they pose potential cybersecurity risks.

Australians need to stay vigilant of online scams and viruses

- Just under 3 in 5 (59%) Australians have experienced a computer virus.
- Slightly more than 1 in 4 (26%) are certain that one of their devices has been listening to their conversations due to subsequent targeted advertising.
- Nearly 3 in 10 (28%) are certain they have been targeted by advertising or marketing campaigns using personal information they were unaware of sharing online for this purpose.
- Just under 2 in 5 (37%), either themselves or a family member, have been affected by a provider data breach within the past 2 years (to the best of their knowledge).
- Respondents reported that either they themselves or a family member had been a victim of the following privacy violations: Social media account hacking (24%), data hacking (23%) and having personal information or pictures shared without their consent (11%).
- Less than 1 in 5 (16%), either themselves or a family member, have experienced cyberbullying and less than 1 in 5 (15%) have experienced online harassment.

Key findings

Many Australians over 18 have been personally targeted by online, email or phone scams

- Just under half (47%) have personally been targeted by online, email or phone scams, while a similar percentage (49%) said their family, friends or colleagues have also been targeted.
- The average amount of money taken from Australians in online, email or phone scams is $4,307.
- Less than half (45%) of those targeted by online, email or phone scams and had money taken were unable to recover any of the money.
- Less than 1 in 5 (17%) Australians who have been targeted by online, email or phone scams experienced significant negative impacts on their mental or overall well-being as a result of the scams.
- 3 in 5 (60%) of those who had money taken from online, email or phone scams reported the scams to the authorities for investigation.

Australians need to be careful about email and phone scams

- More than 3 in 5 (63%) of Australians are confident in their knowledge of what to do if they have been scammed.
- The most common types of scams experienced by individuals targeted by online, email or phone scams are phishing or smishing (50%), online shopping payment scams (38%) and technical support scams (32%).
- The most common online activities that contributed to or delivered the scams for individuals targeted by online, email or phone scams were emails (47%), text messaging or phone calls (46%) and social networking (24%).
- Just over 1 in 3 (34%) of individuals targeted by online, email or phone scams reported that hyper-realistic-looking fake websites, emails and social media profiles played a role in the execution of the scam.

Key findings

Many Aussies over 18 are spending money and adopting techniques to increase their online security

- 2 in 5 (40%) Australians have invested in antivirus/antimalware software to enhance the security of their phones, laptops or home computers. A little over 1 in 5 (21%) have allocated funds for a firewall and just under 1 in 5 (18%) have spent money on a VPN (Virtual Private Network).
- Over 1 in 10 (12%) back up their data on a daily basis, while just under 1 in 5 (18%) back up their data weekly.
- More than 1 in 5 (22%) rarely or never change their passwords, while the same percentage (22%) change their passwords quarterly.
- The most common security measures adopted by Australians to stay 'scam savvy' include being mindful of the types of information they share online and who has access to it (56%), educating themselves about common types of digital scams and remaining vigilant for signs of fraud (55%) and regularly reviewing their online accounts and credit reports for any suspicious activity (52%).
- The key scam red flags highlighted by Australians are poor grammar and spelling (72%), offers that seem too good to be true (68%) and requests for personal information (66%).
- The most common data security measures adhered to by Australians include keeping their devices locked when not in use and refraining from sharing login credentials (59%), looking for "https" at the beginning of a URL to ensure encryption for information protection (45%) and avoiding public Wi-Fi (45%).
- The most common software and digital security measures followed by Australians include avoiding public Wi-Fi for sensitive transactions and utilising a virtual private network (VPN) when necessary (53%), keeping software, operating systems, firewalls and antivirus/antimalware software up to date with the latest security patches (53%) and clearing cookies on their computers (50%).
- Over 7 in 10 (71%) prioritise security by being cautious of suspicious emails, messages or phone calls and refraining from responding to unsolicited requests for personal information.
- When selecting reputable providers, the most commonly followed security measures are using trusted payment methods only (67%), refraining from opening emails and attachments from unfamiliar senders (65%) and exercising caution when downloading files or clicking on links, particularly from unknown sources (61%).

Key findings

Many parents are allowing kids under 18 to access many devices which have access to the internet

- The most common devices that kids use to access the internet at home are smartphones (58%), tablets (55%) and computers (49%).
- According to parents who have a child or children aged 18 years or younger, the most common age at which they allow their child or children to access the internet unsupervised is between 14 and 16 years (30%), followed by 11 to 13 years (25%).
- The most common response from parents regarding the amount of time they allow their child or children aged 18 or younger to spend online each day for non-school activities is a maximum of 2 hours (24%). Additionally, 14% reported that their child has an unrestricted amount of time for non-school-related online activities each day.
- For parents, the most common age at which they allow their child or children to have their own social media account is between 14 and 16 years (42%), followed by 11 to 13 years (22%) and 17 to 18 years (19%).

Parents are concerned about their children being online

- Nearly 7 in 10 (68%) parents with a child or children under 18 are most concerned about their child or children being exposed to cyberbullying or harassment through technology. This is followed by concerns about online predators and cyberstalking (61%) and exposure to porn or sexually inappropriate content (59%).
- Almost 1 in 5 (17%) parents have experienced a situation where one of their children met someone in real life whom they only knew online.
- 1 in 4 (25%) parents report that their children have online friends or acquaintances whose identity they have no knowledge of.
- Just over 1 in 3 (34%) parents have encountered a situation where one of their children was exposed to inappropriate content. Additionally, just over 1 in 4 (26%) have had a child experience abusive behaviour online and just under 1 in 4 (24%) have had a child make an unauthorised online purchase.

Key findings

Parents are trying to keep their children safe online. Are some going too far?

- Nearly 3 in 5 (59%) parents with a child or children under 18 engage in conversations with their children about the importance of online safety and using technology sensibly to mitigate potential negative effects.
- Almost all (96%) parents agree that parents should prioritise online safety over protests about privacy from their children. Furthermore, over 9 in 10 (95%) agree that parents require better support to effectively manage the online risks that children face today.
- More than 1 in 3 (34%) parents, whose children have their own social media accounts, have accessed their children's accounts using their passwords to check their activity.
- Just over half (51%) of parents, whose children have their own social media accounts, have either created or considered creating a "fake" social media account to monitor their children's activities without their knowledge.
- Less than half (47%) of parents obtain explicit consent from their children before posting specific photos of them online. Additionally, just under 7 in 10 (69%) parents agree that parents should refrain from posting pictures of their children without their permission.

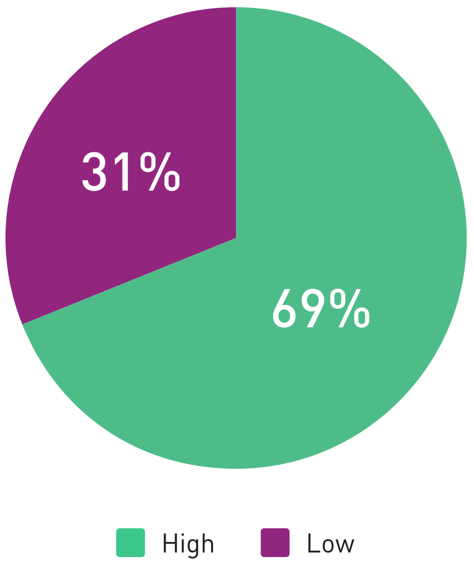
Australians over 18 are starting to use AI language tools

- Just under 3 in 5 (59%) Australians have heard about, tried and used the latest AI language tools like ChatGPT.
- Among those currently using AI language tools, a little over 2 in 5 (41%) use them regularly, while more than 1 in 4 use them all the time (28%) or sometimes (26%).
- More than half (55%) of current AI language tool users trust their accuracy.
- The main reasons for individuals currently using, having tried or planning to try AI language tools are fun and entertainment (38%), work or study tasks (34%) and writing and editing tasks (33%).
- Almost 7 in 10 (69%) of those currently using, having tried or are planning to try AI language tools express concerns about the privacy and security of the information they might share with these platforms or tools.

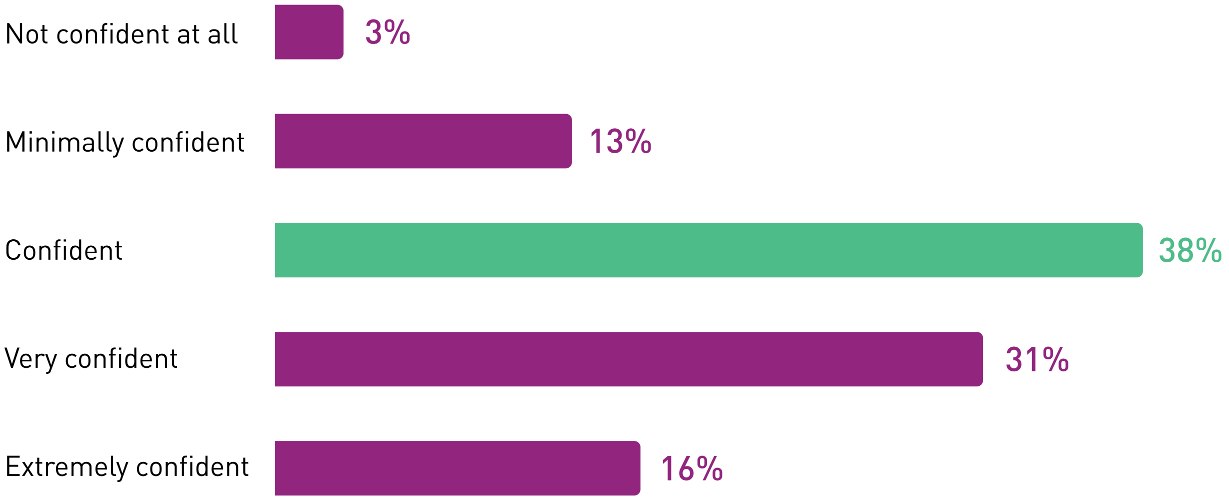
Australian digital risk concerns

Fear of online risks is high

How would you best rate your fear of online risks these days?



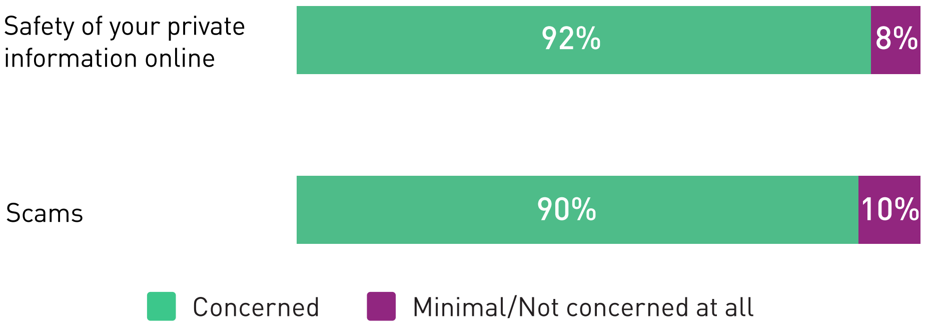
How confident are you in your understanding of the risks involved with being online these days (e.g. exposure to cybercrime, scams, privacy issues and abusive behaviour)?



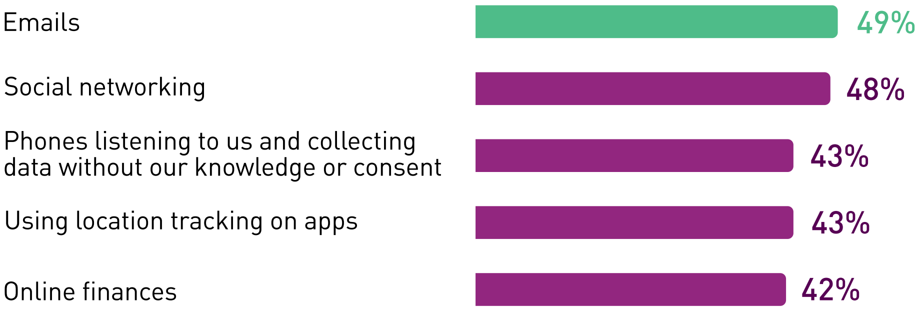
Approximately 69% of Australians over 18 rate their fear of online risk as high. Less than half (46%) are very or extremely confident in their understanding of the risks associated with being online.

Which risks concern us the most?

What kind of online risks do you tend to be most concerned about?

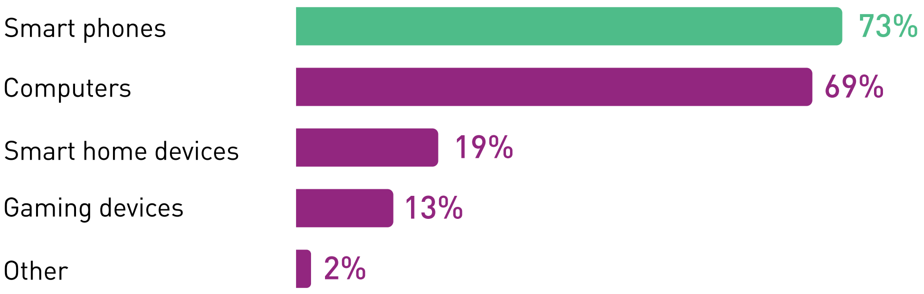


What online activities do you (and your family) feel pose the greatest online risks?



Multiple answers allowed, top 5 answers

Where do you (and your family) feel the most exposed to online risks?



Multiple answers allowed

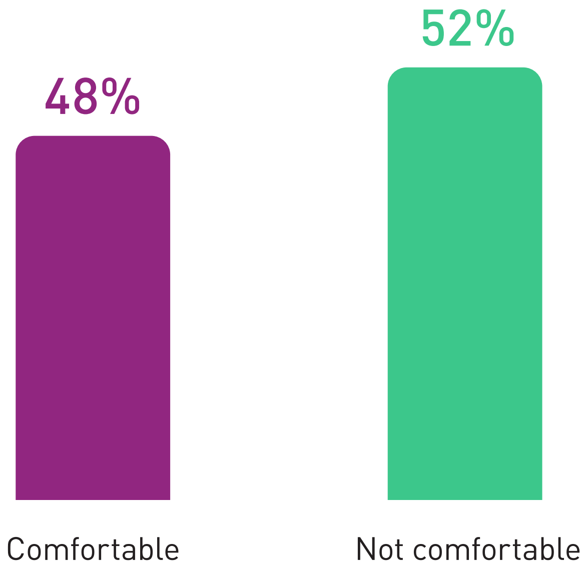
The safety of their private information online is one of the primary concerns for 92% of Australians and 90% are concerned about scams.

Australians believe they are most exposed to online risks through smartphones (73%), computers (69%) and smart home devices (19%).

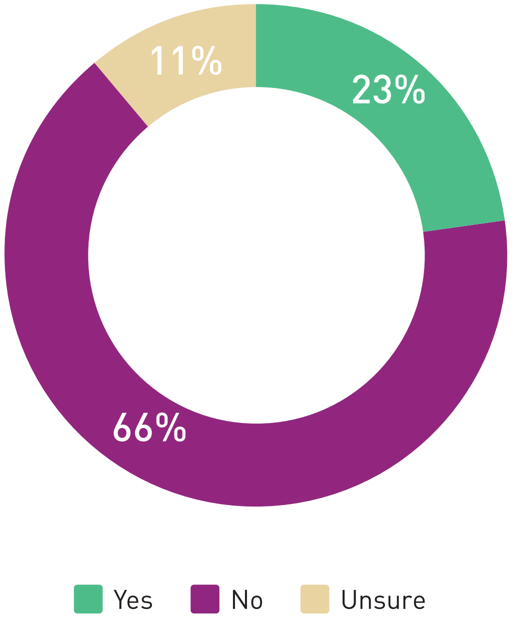
The online activities considered to pose the greatest risk to Australians are emails (49%), social networking (48%) and phones listening to them and collecting data without their knowledge or consent (43%).

Are we comfortable sharing our details?

How comfortable do you feel sharing your personal health information online?



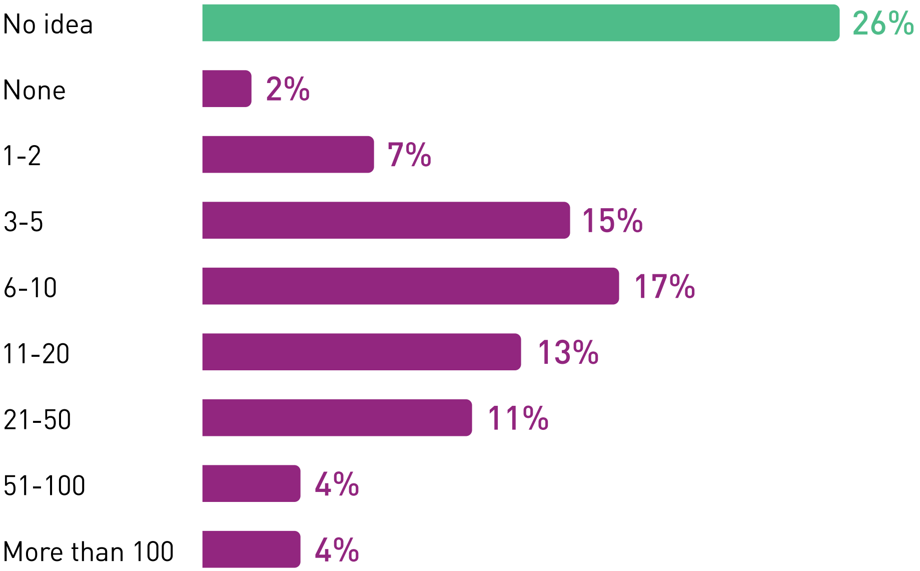
Have you ever provided personal health information online to someone other than medical or insurance providers?



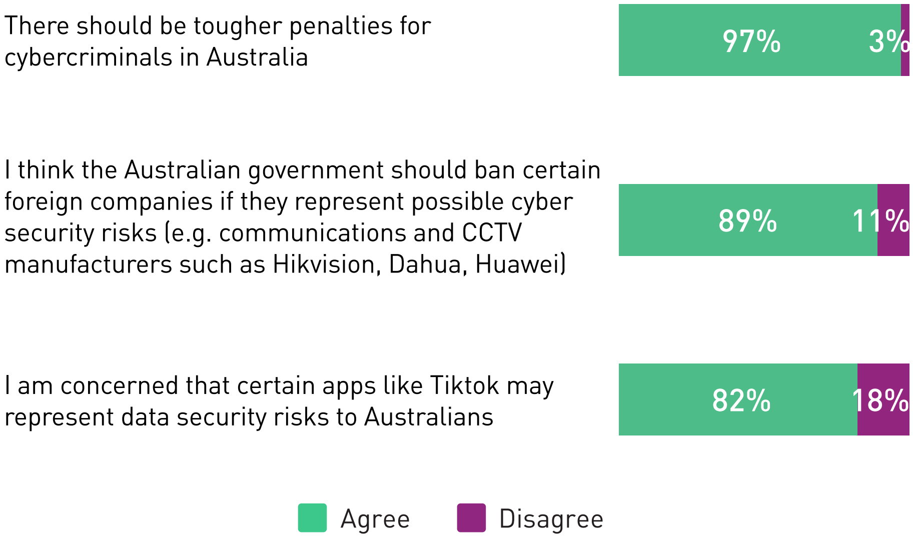
Just under half (48%) of Australians feel comfortable sharing their personal health information online. Less than 1 in 4 (23%) have provided personal health information online to individuals or entities other than medical or insurance providers.

Are we asking for it?

How many websites/online providers would you estimate you have provided personal information to in the last year?



How much do you agree with the following statements about cyber security?



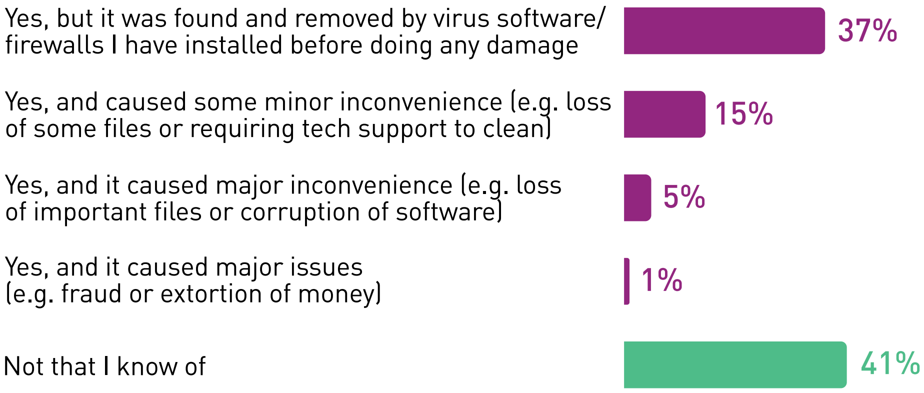
Almost a third (32%) of Australians estimate they have shared their personal information with more than 10 websites/online providers in the past year.

Almost all (97%) agree that there should be tougher penalties for cybercriminals in Australia. Nearly 9 in 10 (89%) believe the Australian government should ban certain foreign companies if they pose potential cybersecurity risks.

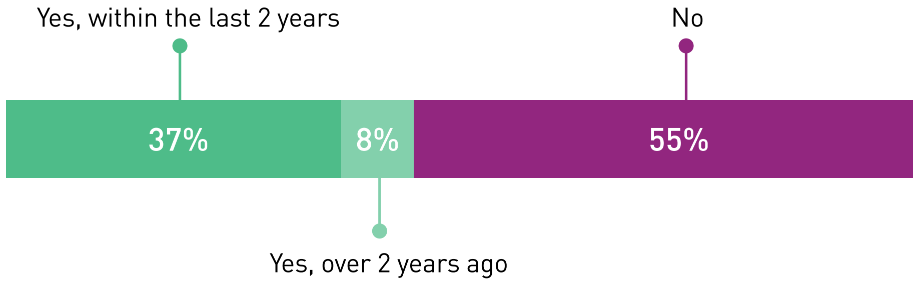
Online privacy

Are we safe from computer viruses?

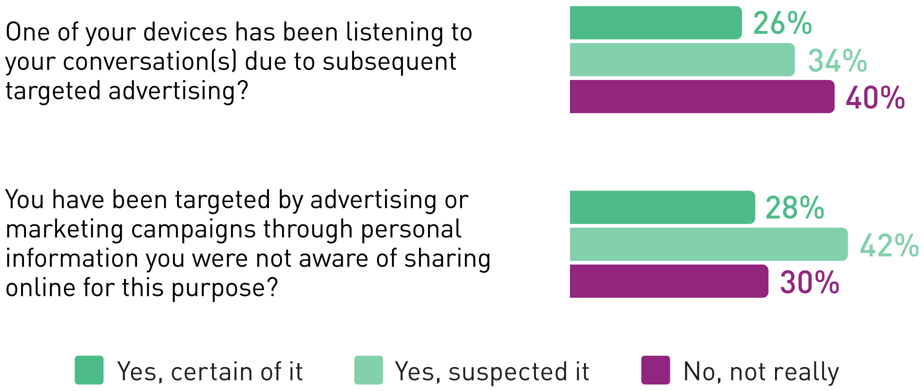
Have you ever had a computer virus?



Have you or anyone in your family ever been caught in a provider data breach that you know of (i.e. personal data held by your provider compromised in a cybercriminal attack)?



Have you ever felt like...



Almost 3 in 5 (59%) Australians have experienced a computer virus.

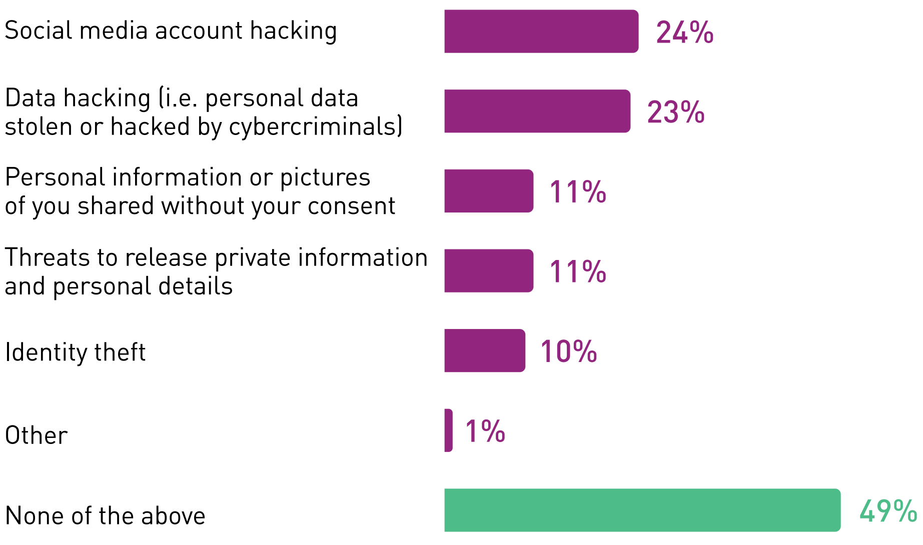
Over 1 in 4 (26%) are certain that one of their devices has been listening to their conversations due to subsequent targeted advertising.

Close to 3 in 10 (28%) are certain they have been targeted by advertising or marketing campaigns using personal information they were unaware of sharing online for this purpose.

Nearly 2 in 5 (37%), either themselves or a family member, have been affected by a provider data breach within the past 2 years (to the best of their knowledge).

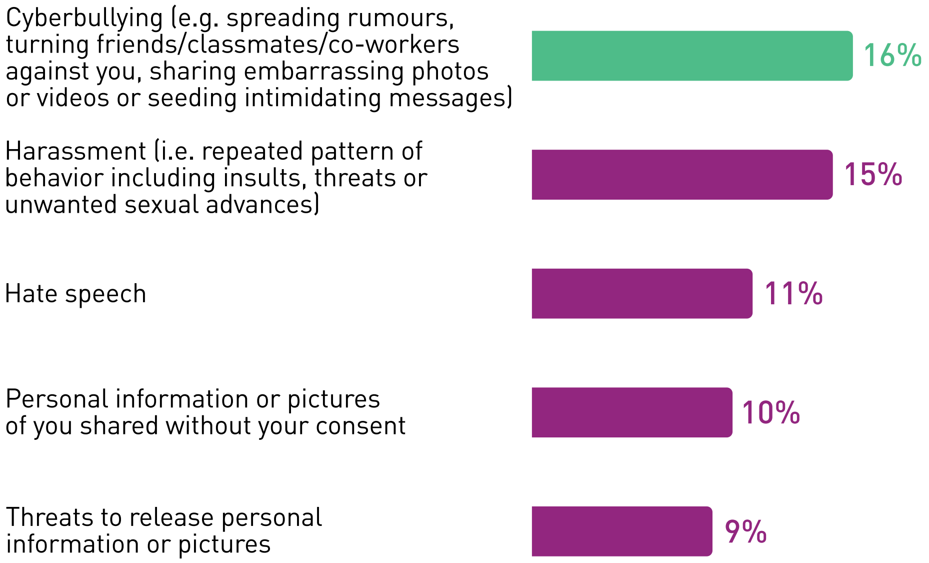
Social media is a risk

Have you or anyone in your family ever been the victim of any of the following online privacy violations?



Multiple answers allowed

Have you or anyone in your family ever experienced any of the following types of abuse online?



Multiple answers allowed

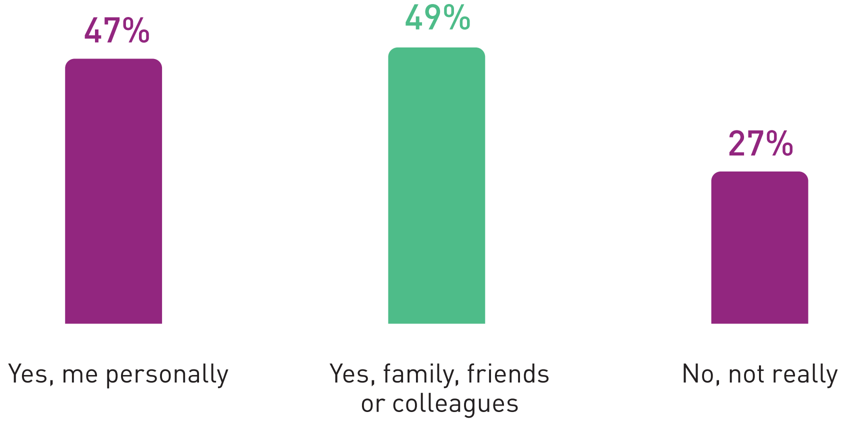
Respondents reported that either they themselves or a family member had been a victim of the following privacy violations: Social media account hacking (24%), data hacking (23%) and having personal information or pictures shared without their consent (11%).

Less than 1 in 5 (16%), either themselves or a family member, have experienced cyberbullying and less than 1 in 5 (15%) have experienced online harassment.

Australians at risk of scams

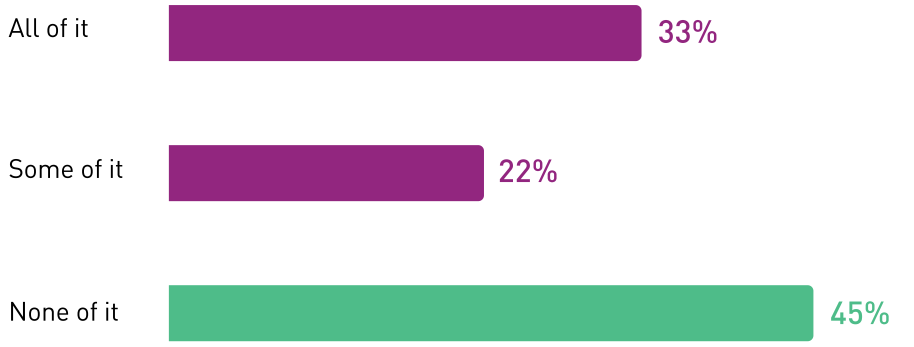
The scam marketplace

Have you or people you know ever been targeted by online, email or phone scams?



Multiple answers allowed

Did you/they get the money back?



n = 1,115, Have been targeted by online, email or phone scams AND money was taken from scam

How much money was taken (if any)?

$4,307

- *n = 1,095, Have been targeted by online, email or phone scams*
- *Outliers and $0 responses removed from analysis*

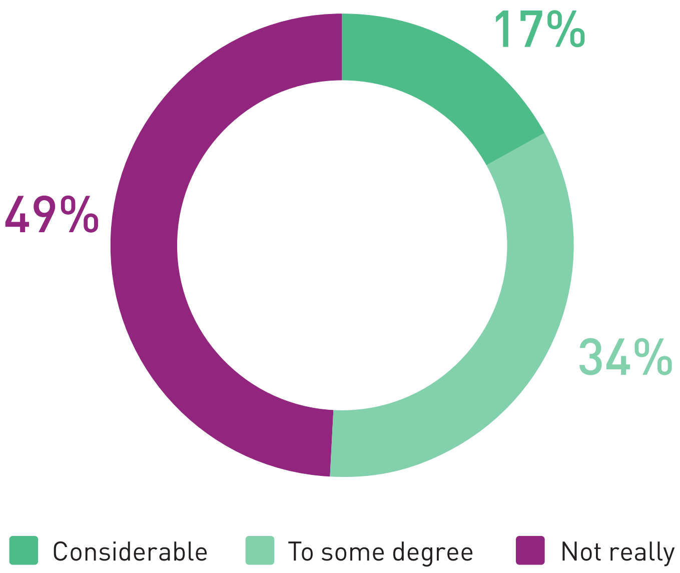
Almost half (47%) have personally been targeted by online, email or phone scams, while a similar percentage (49%) said their family, friends or colleagues have also been targeted.

The average amount of money taken from Australians in online, email or phone scams is $4,307.

Less than half (45%) of those targeted by online, email or phone scams and had money taken were unable to recover any of the money.

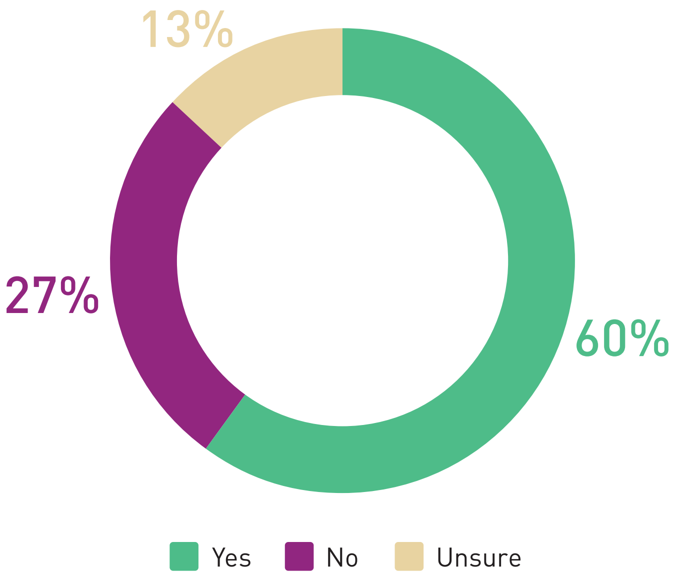
Scams impact more than just the bank

Did you/they experience any negative mental or wellbeing impacts from being targeted by the scam?



n = 3,698, Have been targeted by online, email or phone scams

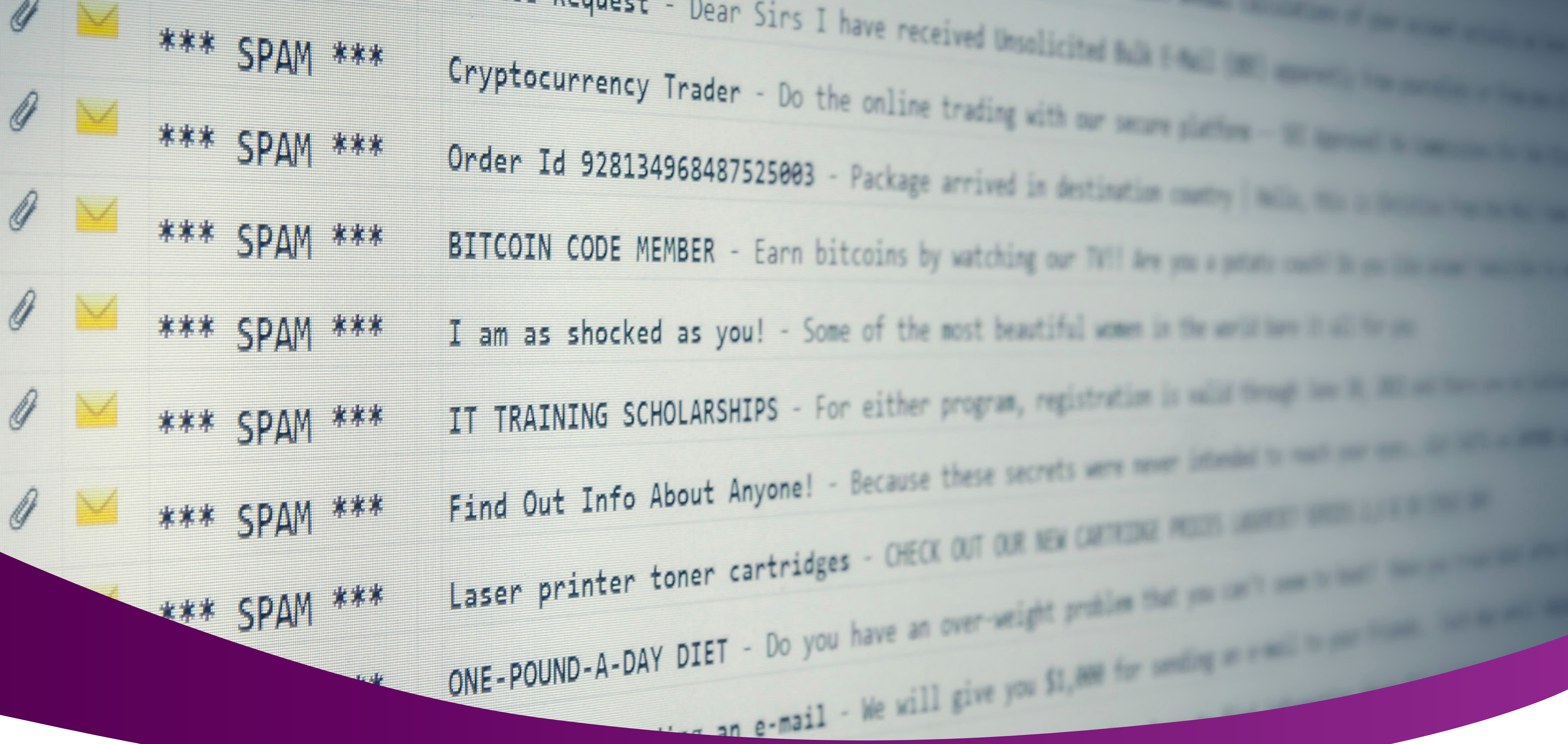
Did you/they report it to authorities to investigate (e.g. police, eSafety or ReportCyber)?



n = 1,115, Have been targeted by online, email or phone scams AND money was taken from scam

Less than 1 in 5 (17%) Australians who have been targeted by online, email or phone scams experienced considerable negative impacts on their mental or overall well-being as a result of the scams.

3 in 5 (60%) of those who had money taken from online, email or phone scams reported the scams to the authorities for investigation.


Request - Dear Sirs I have received Unsolicited Bulk E-Mail (UBE) apparently from

*** SPAM *** Cryptocurrency Trader - Do the online trading with our secure platform

*** SPAM *** Order Id 92813496848752503 - Package arrived in destination country | Hello,

*** SPAM *** BITCOIN CODE MEMBER - Earn bitcoins by watching our TV!! Are you a potato couch?

*** SPAM *** I am as shocked as you! - Some of the most beautiful women in the world bare it all for you

*** SPAM *** IT TRAINING SCHOLARSHIPS - For either program, registration is valid through

*** SPAM *** Find Out Info About Anyone! - Because these secrets were never intended to reach your

*** SPAM *** Laser printer toner cartridges - CHECK OUT OUR NEW CARTRIDGE PRICES

*** SPAM *** ONE-POUND-A-DAY DIET - Do you have an over-weight problem that you can't seem to beat?

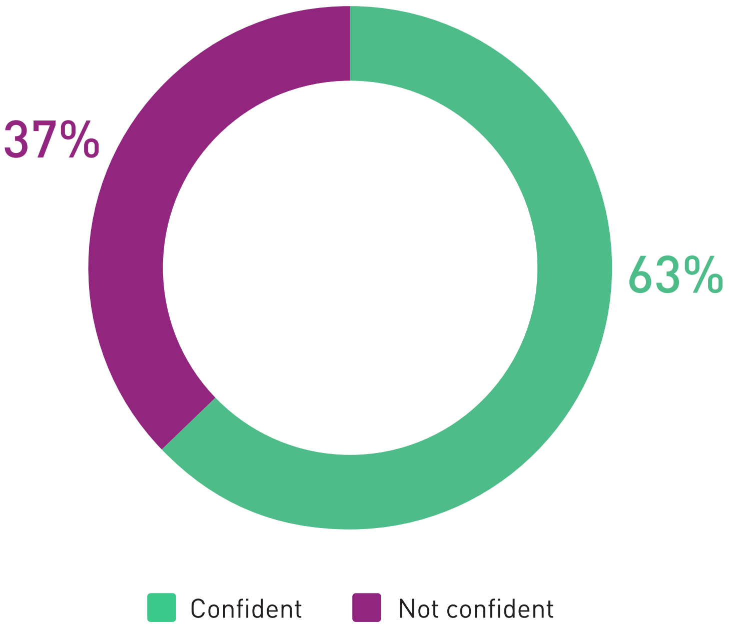
an e-mail - We will give you $1,000 for sending an e-mail

Online scam tactics

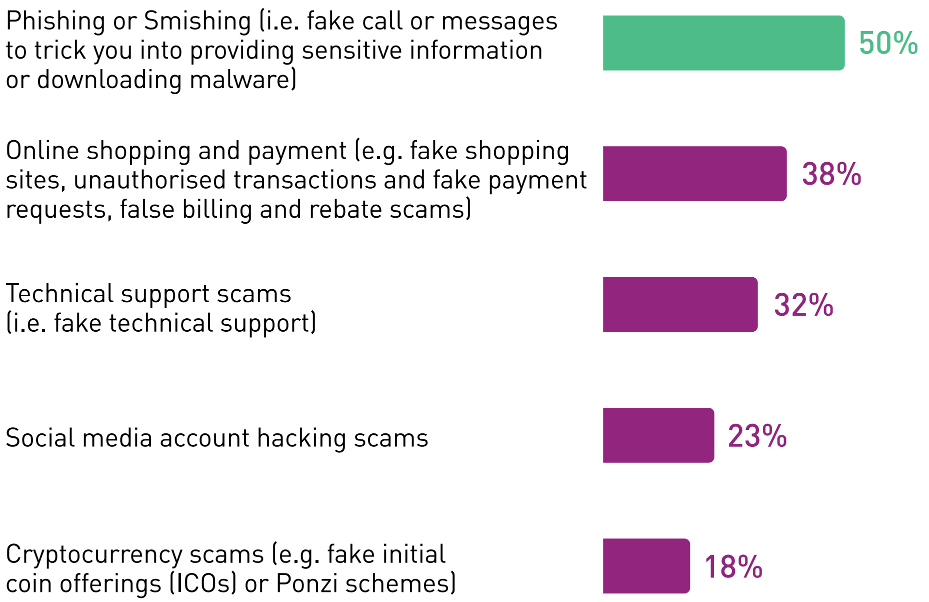
real INSURANCE®

Do we know we've been scammed?

How confident are you that you know what to do if you have been scammed?



What type of scam(s) were involved?



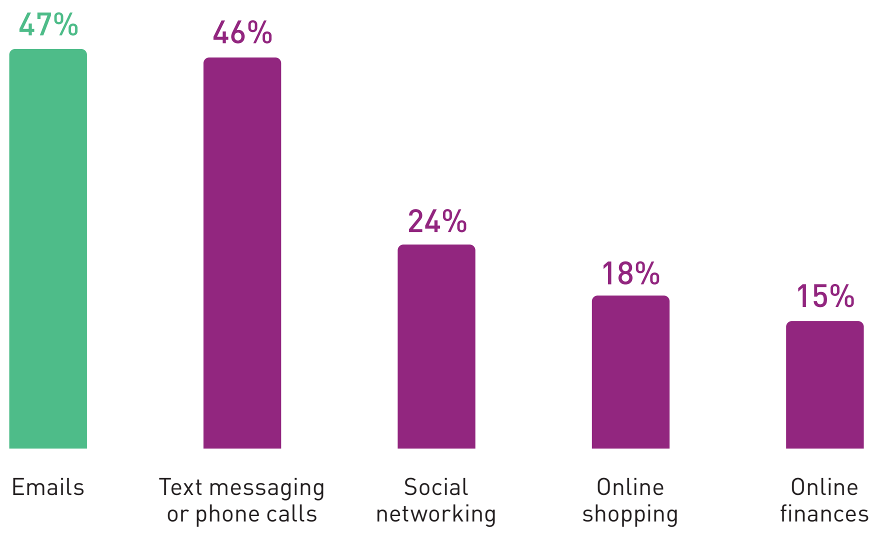
- *n = 3,698, Have been targeted by online, email or phone scams*
- *Multiple answers allowed, top 5 answers*

More than 3 in 5 (63%) Australians are confident in their knowledge of what to do if they have been scammed.

The most common types of scams experienced by individuals targeted by online, email or phone scams are phishing or smishing (50%), online shopping payment scams (38%) and technical support scams (32%).

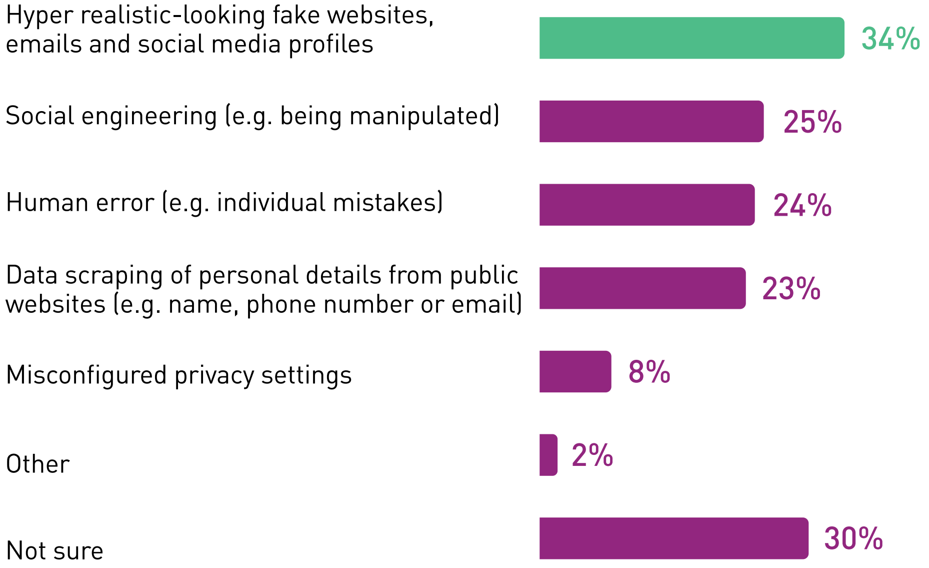
Where are we most exposed?

What online activities were involved in leading to or delivering the scam(s)?



- *n = 3,698, Have been targeted by online, email or phone scams*
- *Multiple answers allowed, top 5 answers*

Did any of the following contribute to how the scam was conducted?



- *n = 3,698, Have been targeted by online, email or phone scams*
- *Multiple answers allowed*

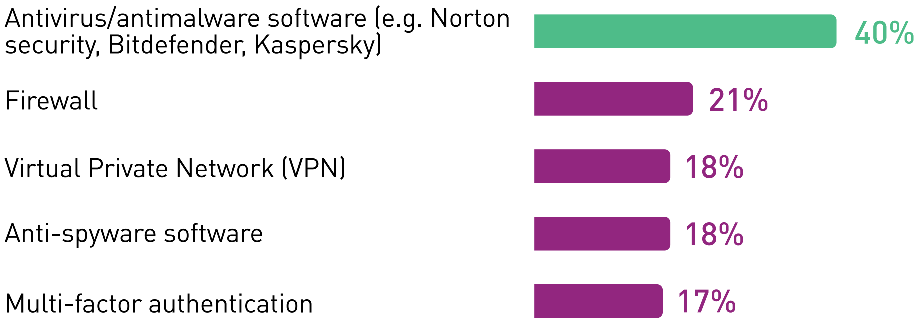
The most common online activities that contributed to or delivered the scams for individuals targeted by online, email or phone scams were emails (47%), text messaging or phone calls (46%) and social networking (24%).

Just over 1 in 3 (34%) of individuals targeted by online, email or phone scams reported that hyper-realistic-looking fake websites, emails and social media profiles played a role in the execution of the scam.

Tips to avoid digital risk

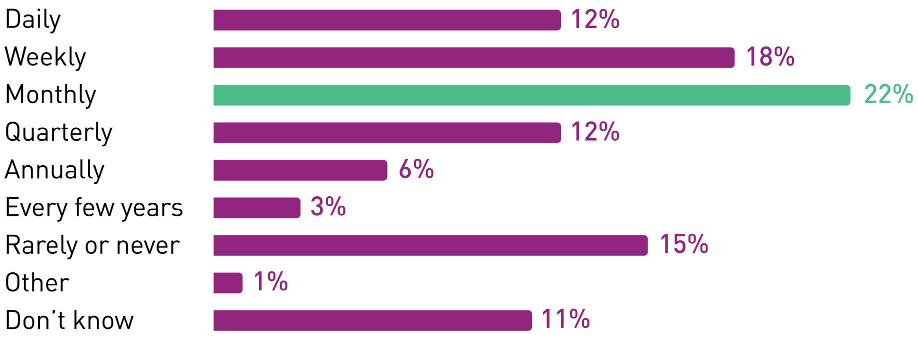
Spending on cybersecurity

Have you spent any money on the following to add security against cybercrime to the phones, laptops or home computers in your household?

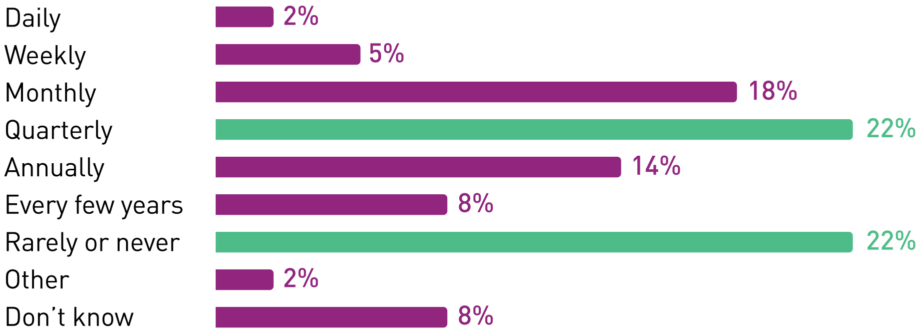


Multiple answers allowed, top 5 positive responses/answers

What best describes how often you typically backup your data?



What best describes how often you typically change your passwords?



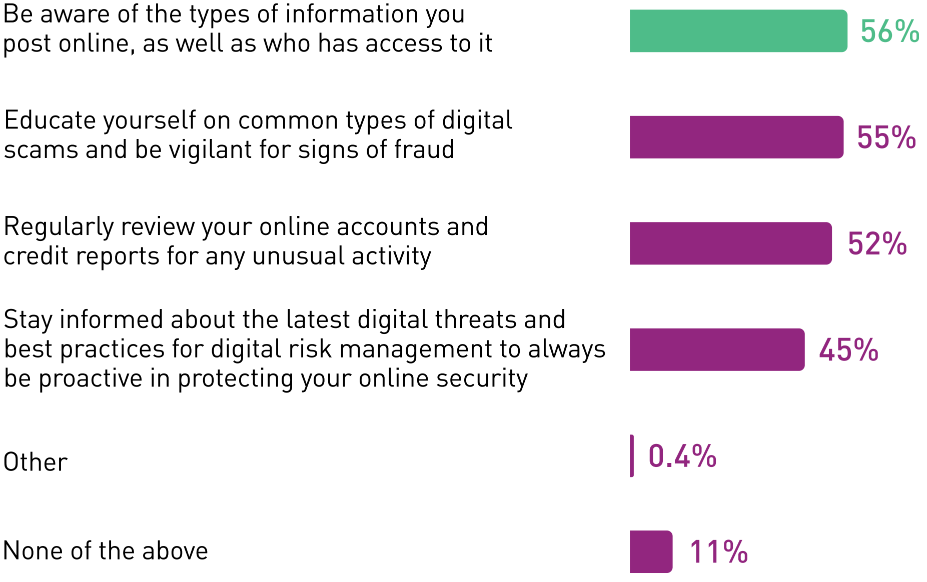
2 in 5 (40%) Australians have invested in antivirus/antimalware software to enhance the security of their phones, laptops or home computers. A little over 1 in 5 (21%) have allocated funds for a firewall and just under 1 in 5 (18%) have spent money on a VPN (Virtual Private Network).

Over 1 in 10 (12%) back up their data on a daily basis, while close to 1 in 5 (18%) back up their data weekly.

More than 1 in 5 (22%) Australians rarely or never change their passwords, while the same percentage (22%) change their passwords quarterly.

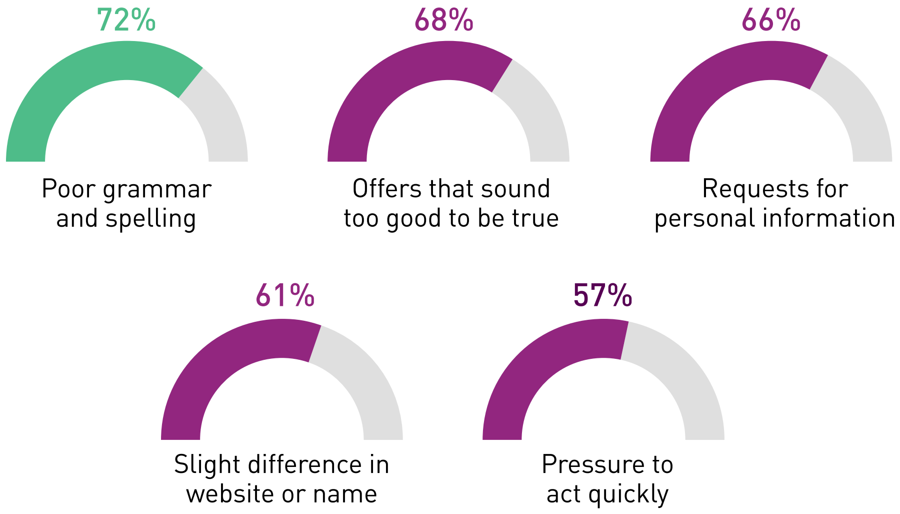
Staying 'scam savvy'

Which of the following 'scam savvy' security measures do you take?



Multiple answers allowed

What are the key red flags you look for when checking for scams?



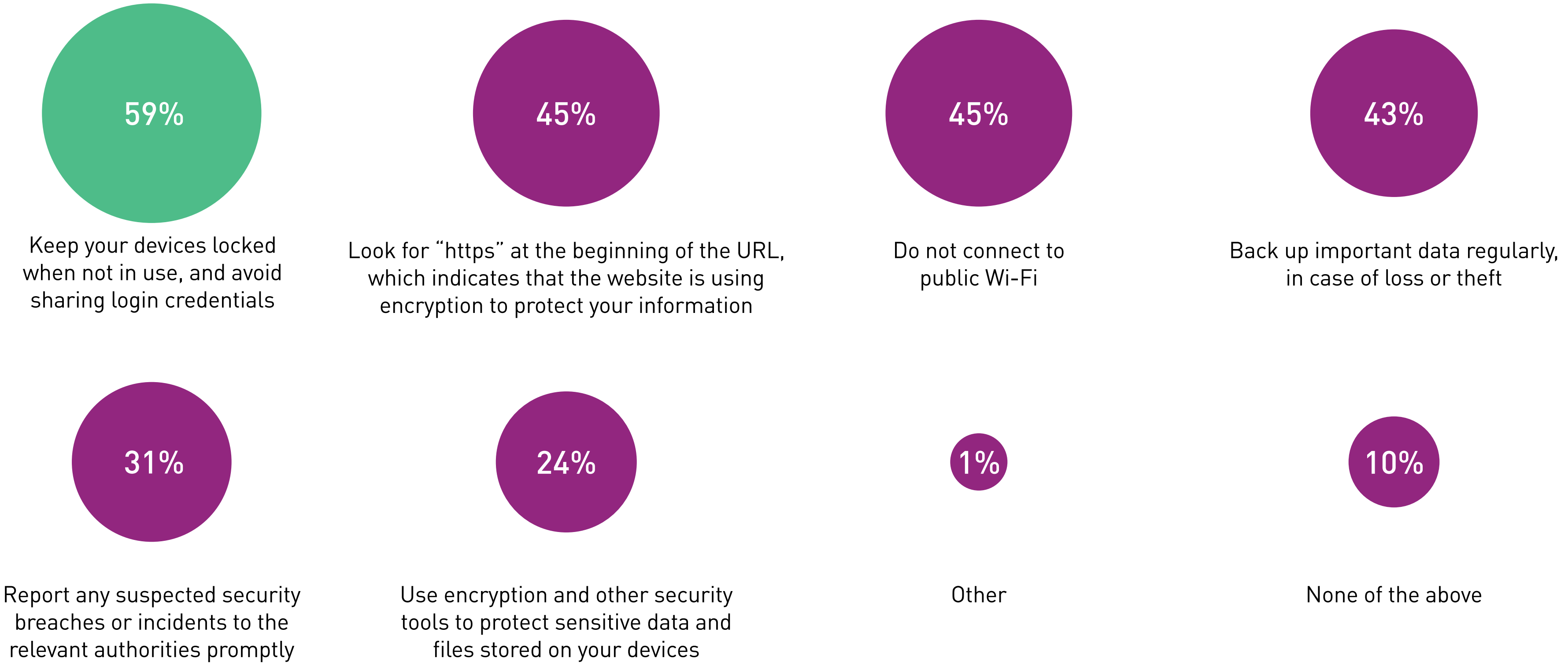
Multiple answers allowed, top 5 answers

The most common security measures adopted by Australians to stay 'scam savvy' include being mindful of the types of information they share online and who has access to it (56%), educating themselves about common types of digital scams and remaining vigilant for signs of fraud (55%) and regularly reviewing their online accounts and credit reports for any suspicious activity (52%).

The key scam red flags highlighted by Australians are poor grammar and spelling (72%), offers that seem too good to be true (68%) and requests for personal information (66%).

Data security measures

Which of the following data security measures do you take to protect yourself?

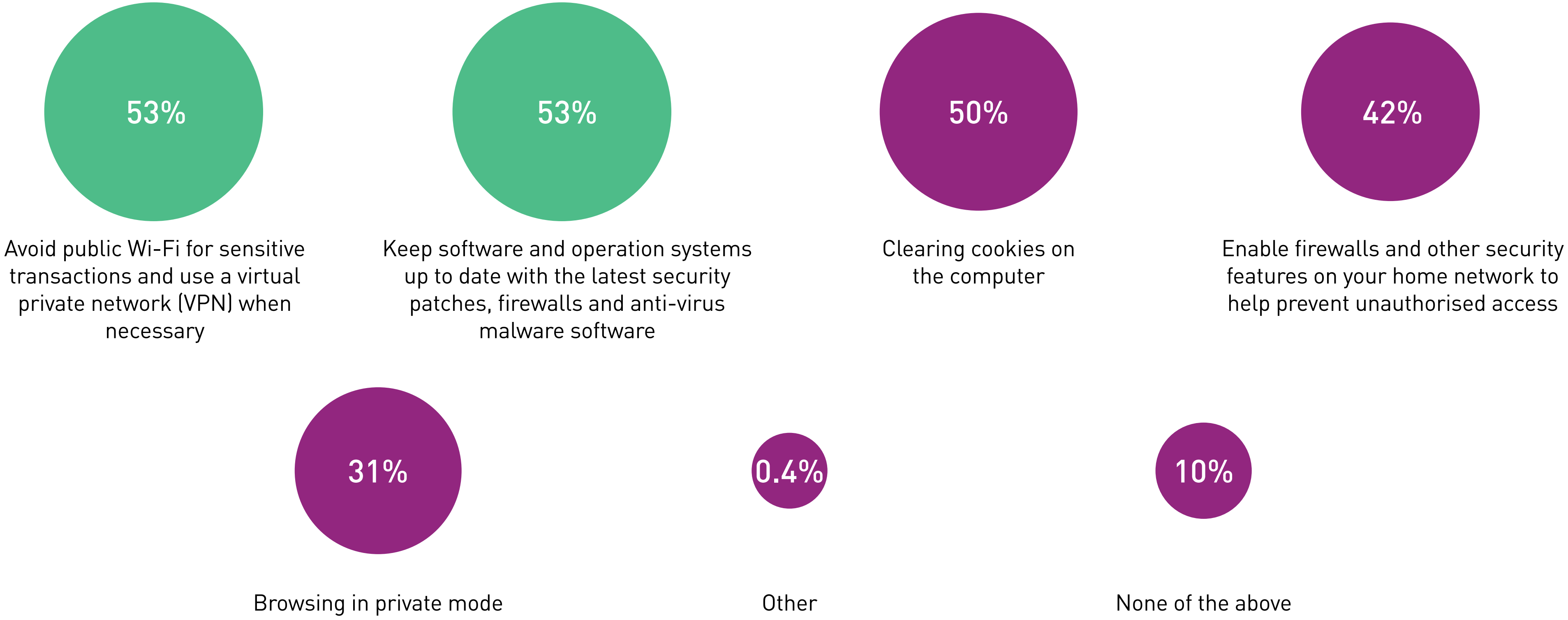


Multiple answers allowed

The most common data security measures adhered to by Australians include keeping their devices locked when not in use and refraining from sharing login credentials (59%), looking for "https" at the beginning of a URL to ensure encryption for information protection (45%) and avoiding public Wi-Fi (45%).

Digital security measures

Which of the following software and/or digital security measures do you adhere to?

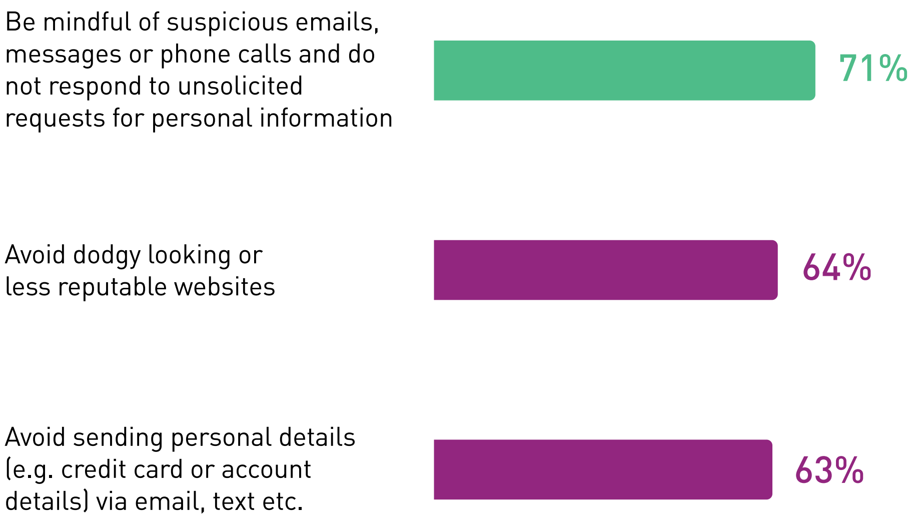


Multiple answers allowed

The most common software and digital security measures followed by Australians include avoiding public Wi-Fi for sensitive transactions and utilising a virtual private network (VPN) when necessary (53%), keeping software, operating systems, firewalls and antivirus/ antimalware software up to date with the latest security patches (53%) and clearing cookies on their computers (50%).

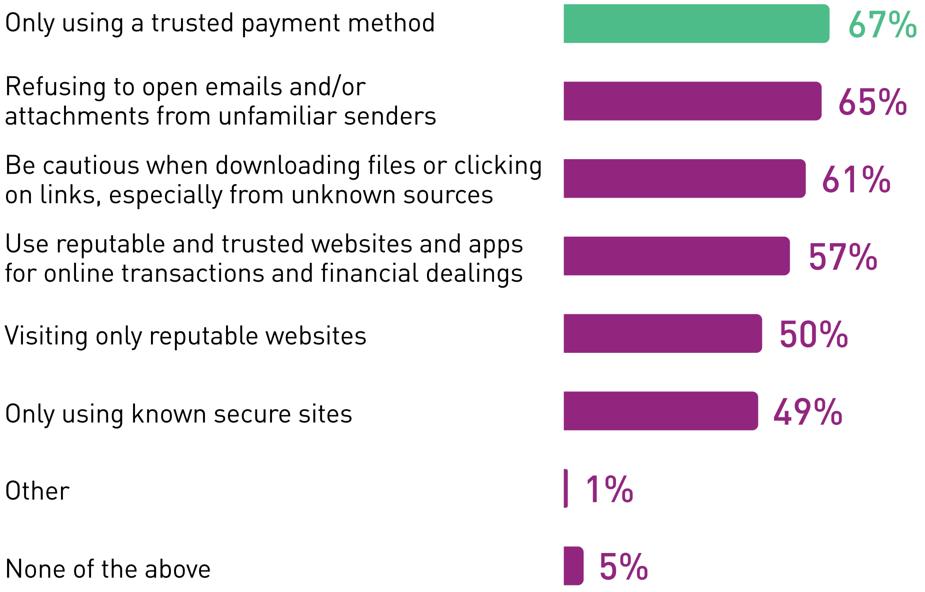
How are we protecting ourselves?

Which of the following security measures around sharing information do you adhere to?



Multiple answers allowed

Which of the following security measures around choosing reputable providers do you adhere to?



Multiple answers allowed

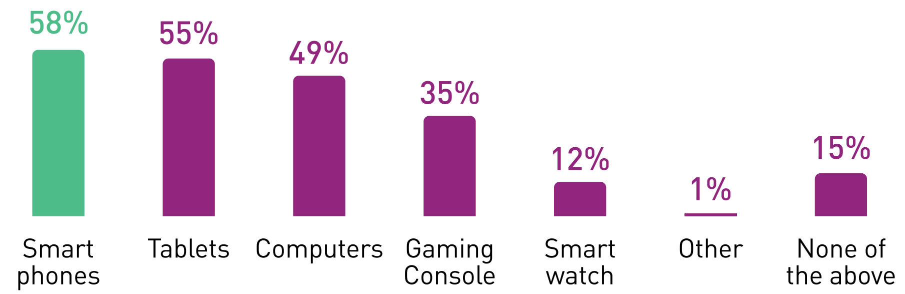
Over 7 in 10 (71%) Australians prioritise security by being cautious of suspicious emails, messages or phone calls and refraining from responding to unsolicited requests for personal information.

When selecting reputable providers, the most commonly followed security measures are using trusted payment methods only (67%), refraining from opening emails and attachments from unfamiliar senders (65%) and exercising caution when downloading files or clicking on links, particularly from unknown sources (61%).

Australian families online

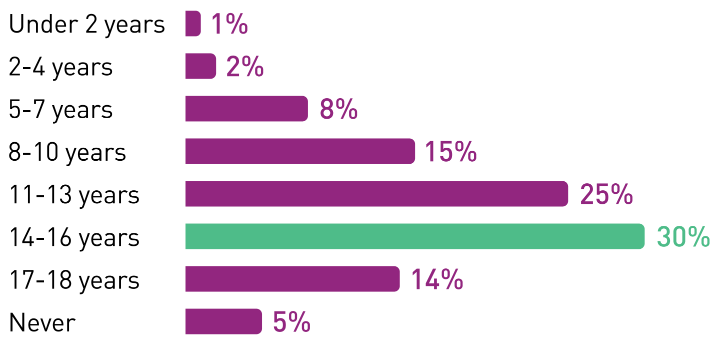
Most children have internet access

Can your child access the internet at home through:



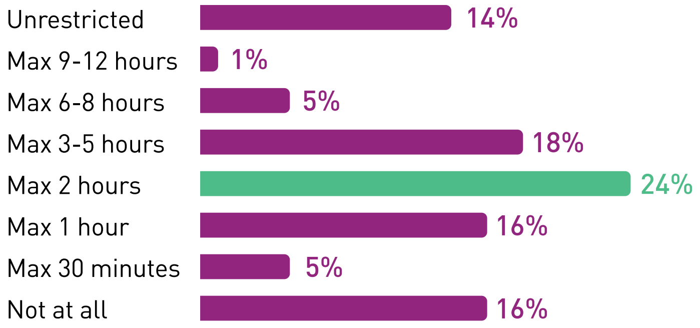
- n = 1,148, has child(ren) 18 years old and below
- Multiple answers allowed

At what age have you or will you allow your child(ren) get online unsupervised by an adult?



n = 1,148, has child(ren) 18 years old and below

What best describes how long you let your child(ren) go online each day for non-school related activities?



n = 1,148, has child(ren) 18 years old and below

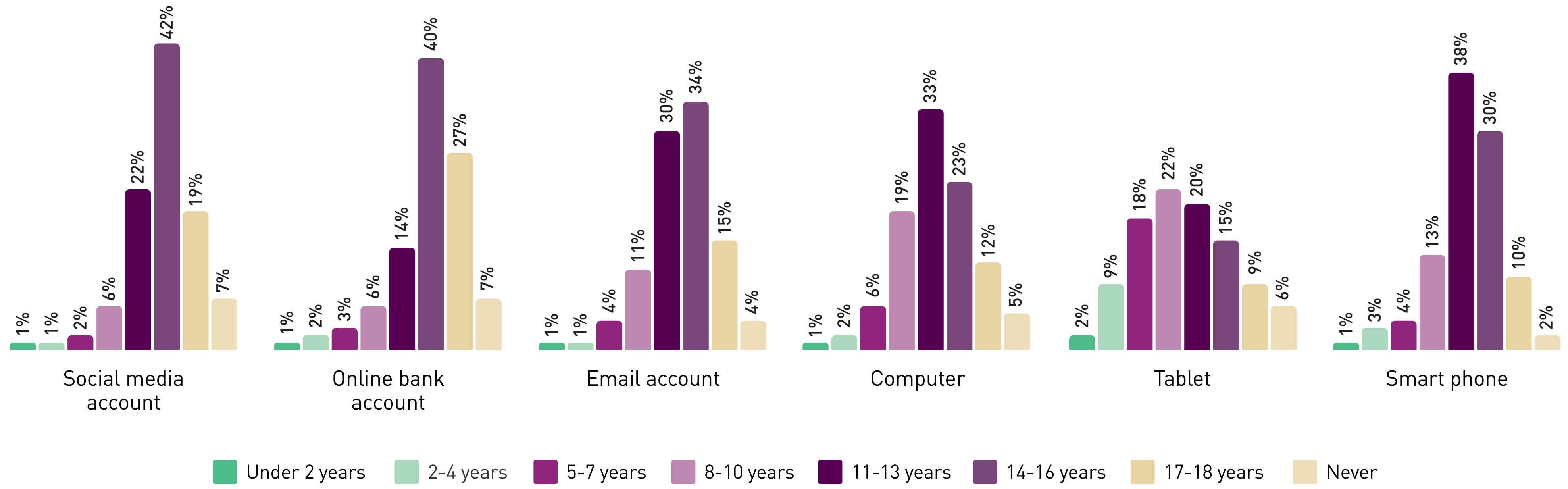
The most common devices that kids use to access the internet at home are smartphones (58%), tablets (55%) and computers (49%).

According to parents who have a child or children aged 18 years or younger, the most common age at which they allow their child or children to access the internet unsupervised is between 14 and 16 years (30%), followed by 11 to 13 years (25%).

The most common response from parents regarding the amount of time they allow their child or children aged 18 or younger to spend online each day for non-school related activities is a maximum of 2 hours (24%). Additionally, 14% reported that their child has an unrestricted amount of time for non-school related online activities each day.

How old are children when they start using socials?

At what age have you or will you allow your child(ren) to take possession of their own:



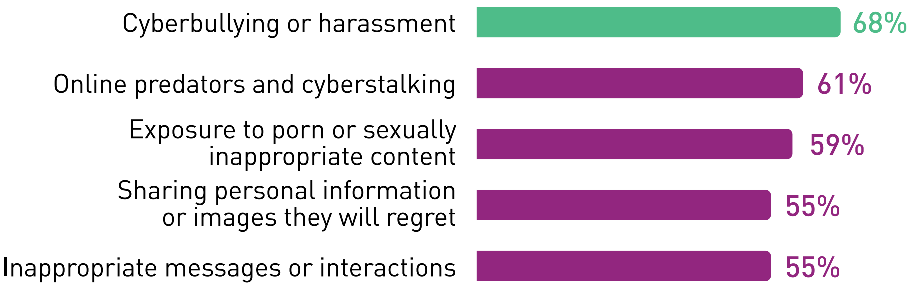
n = 1,148, has child(ren) 18 years old and below

For parents, the most common age at which they allow their child or children to have their own social media account is between 14 to 16 years (42%), followed by 11 to 13 years (22%) and 17 to 18 years (19%).

Family safety online

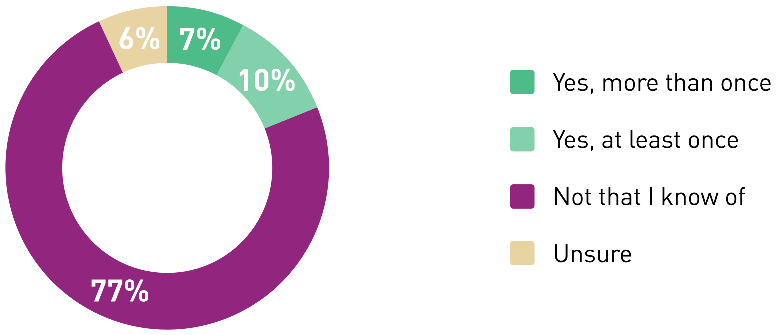
What concerns parents the most?

What are you most concerned your child will be exposed to through technology?



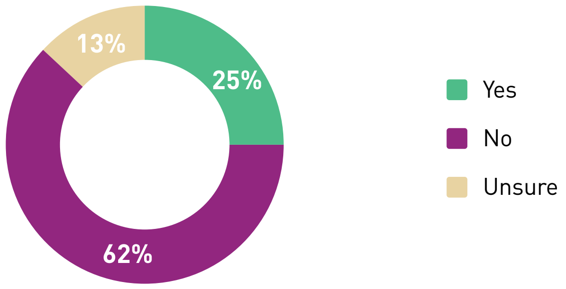
- *n = 1,148, has child(ren) 18 years old and below*
- *Multiple answers allowed, top 5 answers*

Have any of your children ever met someone in real life they only know from online?



n = 1,148, has child(ren) 18 years old and below

Do your child(ren) have friends or acquaintances online that you have no idea who they are?



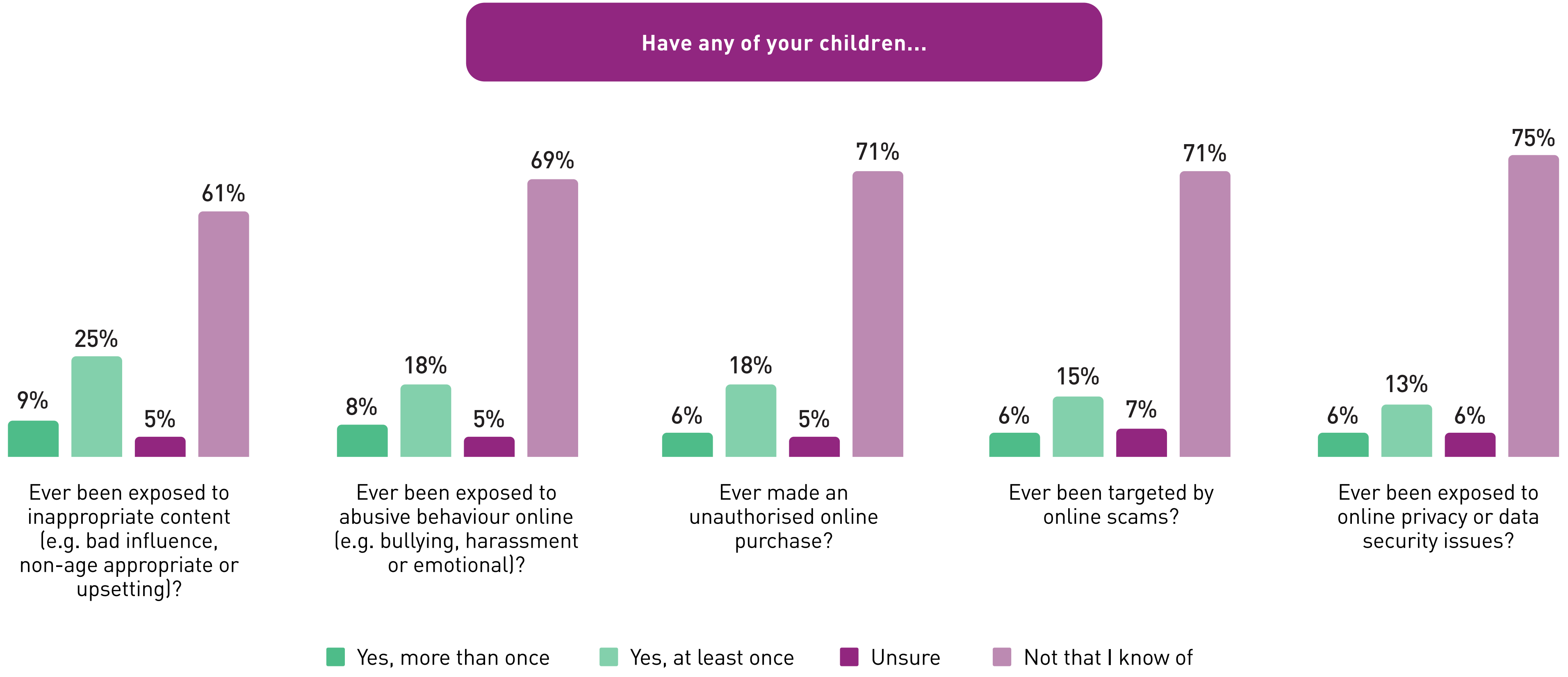
n = 1,148, has child(ren) 18 years old and below

Over 2 in 3 (68%) parents with a child or children under 18 are most concerned about their child or children being exposed to cyberbullying or harassment through technology. This is followed by concerns about online predators and cyberstalking (61%) and exposure to porn or sexually inappropriate content (59%).

More than 1 in 6 (17%) parents have experienced a situation where one of their children met someone in real life whom they only knew online.

1 in 4 (25%) parents report that their children have online friends or acquaintances whose identity they have no knowledge of.

Experiences of children online



n = 1,148, has child(ren) 18 years old and below

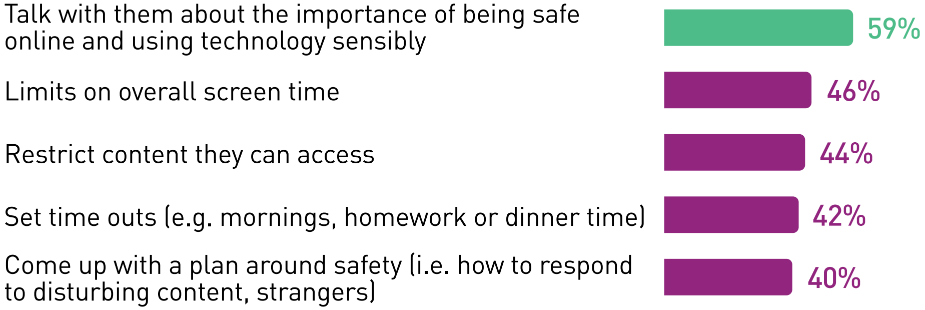
Over a third (34%) of parents with a child or children under 18 have encountered a situation where one of their children was exposed to inappropriate content. Additionally, more than 1 in 4 (26%) have had a child experience abusive behaviour online and almost 1 in 4 (24%) have had a child make an unauthorised online purchase.

Keeping your family safe online

real INSURANCE®

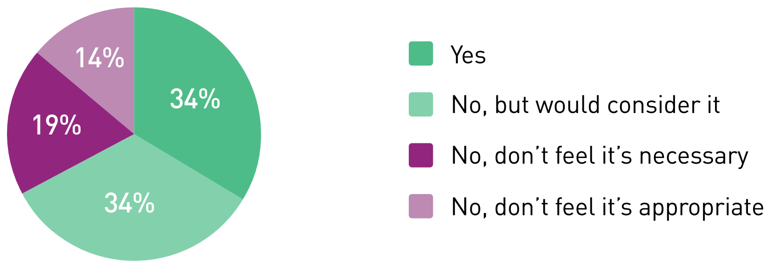
Safety is paramount

Which of the following strategies do you employ to help avoid some of the negative effects of your children using technology?



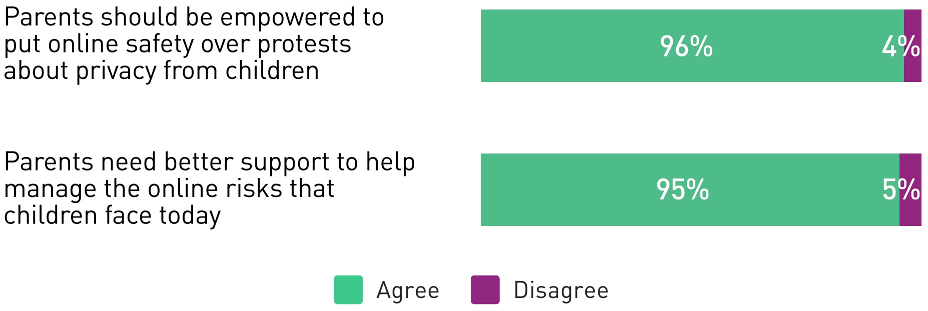
- *n = 1,148, has child(ren) 18 years old and below*
- *Multiple answers allowed, top 5 answers*

Have you ever used your child(ren)'s social media password to check on their activity?



n = 513, Has child(ren) 18 years old and below AND their children have their own social media account(s)

How much do you agree with the following statements?



n = 1,148, has child(ren) 18 years old and below

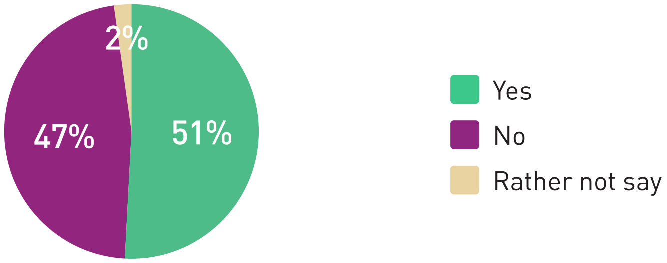
Almost 3 in 5 (59%) parents with a child or children under 18 engage in conversations with their children about the importance of online safety and using technology sensibly to mitigate potential negative effects.

Almost all (96%) parents agree that parents should prioritise online safety over protests about privacy from their children. Furthermore, over 9 in 10 (95%) agree that parents require better support to effectively manage the online risks that children face today.

More than a third (34%) of parents, whose children have their own social media accounts, have accessed their children's accounts using their passwords to check their activity.

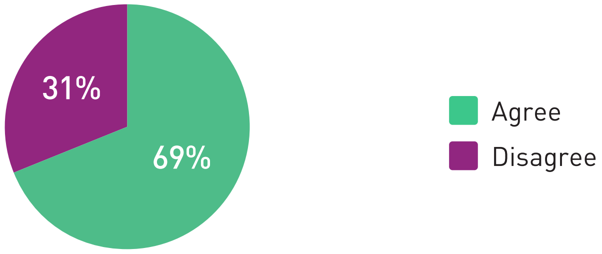
How far do parents go to protect their kids?

Do you currently or would you ever consider creating a "fake" social media account to monitor your child(ren) without them knowing it was you?



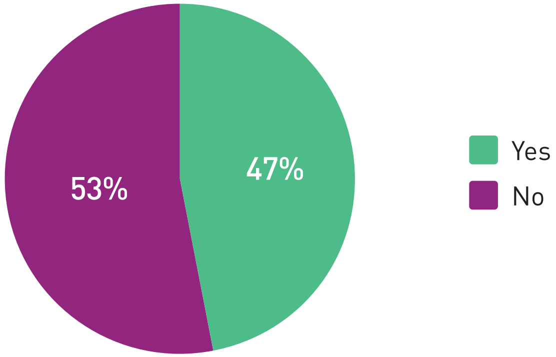
n = 173, has child(ren) 18 years old and below AND children have their own social media account(s) AND have used children's social media account

How much do you agree with the following statement about posting pictures of their child(ren) online?
Parents should not be posting pictures of their children without their permission



n = 1,148, has child(ren) 18 years old and below

Do you get your child(ren)'s consent before posting photos of them online?



n = 1,148, has child(ren) 18 years old and below

More than half (51%) of parents, whose children have their own social media accounts and have used their children's social media accounts, have either created or considered creating a "fake" social media account to monitor their children's activities without their knowledge.

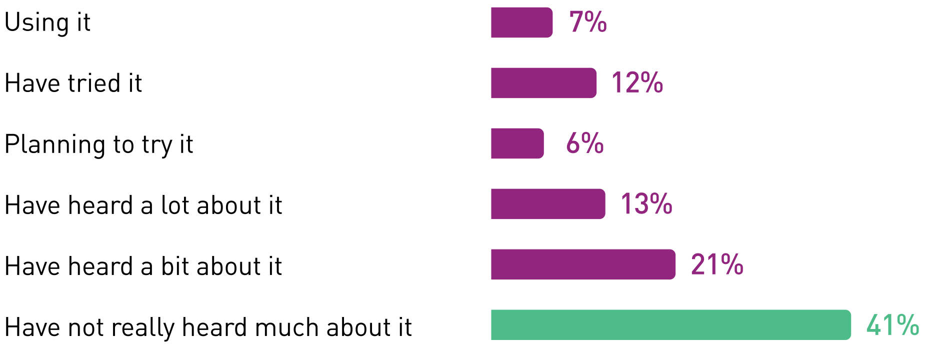
Almost 1 in 2 (47%) parents obtain explicit consent from their children before posting specific photos of them online. Additionally, nearly 7 in 10 (69%) parents agree that parents should refrain from posting pictures of their children without their permission.

Emerging AI language tools

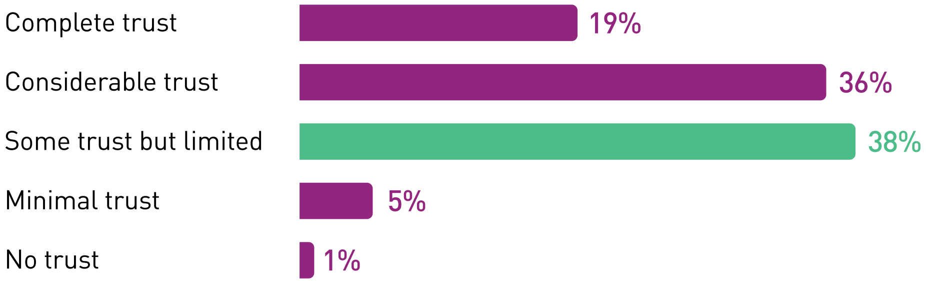
real
INSURANCE®

Aussies are starting to use AI language tools

Have you heard about or used the latest AI language tools like ChatGPT?

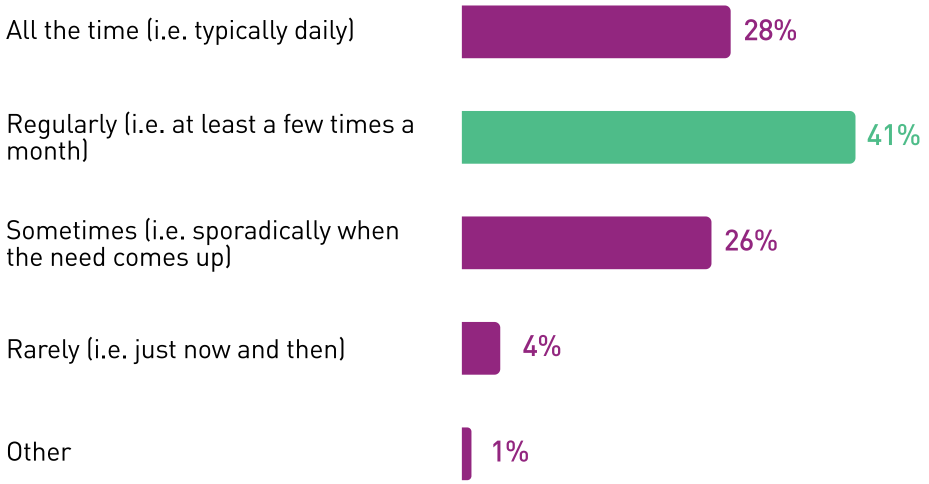


How much do you trust the accuracy of these AI language tools?



n = 341, Currently using AI language tools

How often do you typically use these AI language tools?



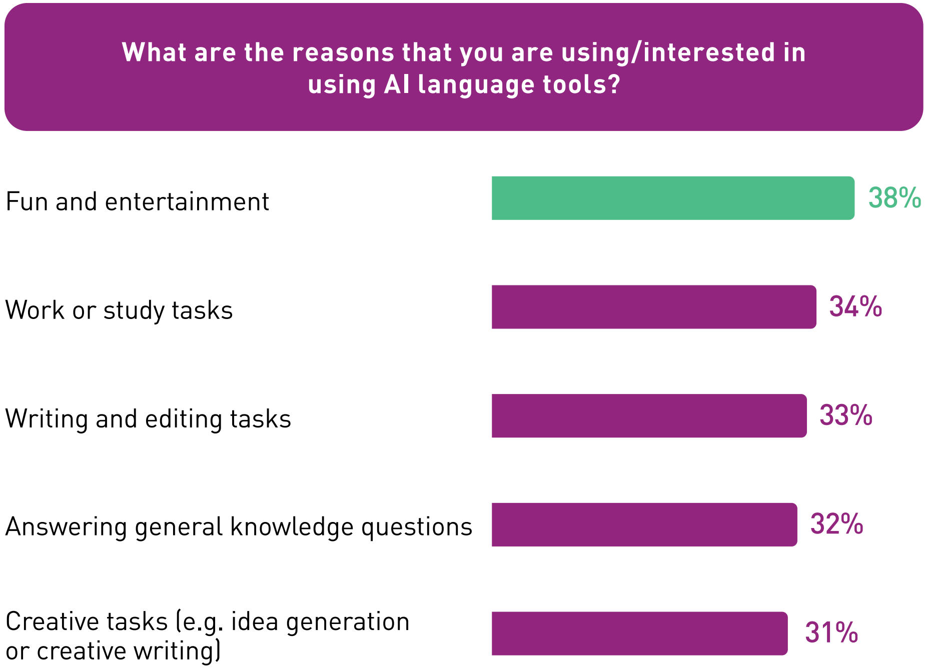
n = 341, Currently using AI language tools

Nearly 3 in 5 (59%) Australians have heard about, tried and used the latest AI language tools like ChatGPT.

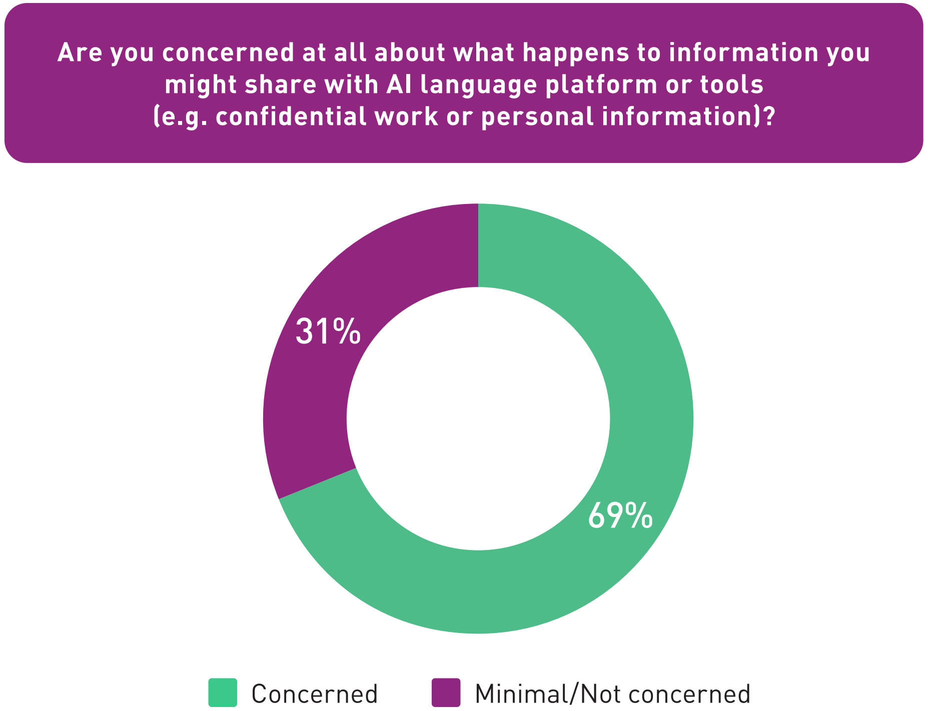
Among those currently using AI language tools, over 2 in 5 (41%) use them regularly, while more than 1 in 4 use them all the time (28%) or sometimes (26%).

More than half (55%) of current AI language tool users trust their accuracy either completely or considerably.

There is concern around information being shared with AI language tools



- *n = 1,295, Currently using, have tried or planning to try AI language tools*
- *Multiple answers allowed, top 5 answers*



n = 1,295, Currently using, have tried or planning to try AI language tools

The main reasons for individuals currently using, having tried or planning to try AI language tools are fun and entertainment (38%), work or study tasks (34%) and writing and editing tasks (33%).

Just under 7 in 10 (69%) of those currently using, having tried or planning to try AI language tools express concerns about the privacy and security of the information they might share with these platforms or tools.

More research from Real Insurance coming soon...

About Real Insurance

Real Insurance is an award-winning provider of insurance products, specialising in life, funeral, pet, travel, car, home, landlords and health insurance. In the market since 2005, Real Insurance has protected the quality of life of many Australians through the delivery of innovative products. Real Insurance is the proud recipient of many product and service awards, most recently being announced a winner of the 2023 Product Review award for Life Insurance and Funeral Insurance, and Feefo's 2023 Gold Trusted Service Award across a range of products. Real Insurance is a trading name of Greenstone Financial Services Pty Ltd.

real
INSURANCE®