Australian Government
Australian Communications and Media Authority

Australia's regulator for broadcasting, radiocommunications, telecommunications and online content

www.acma.gov.au

Australia in the Digital Economy

Report 1: Trust and confidence

Australia in the Digital Economy

Report 1: Trust and Confidence

March 2009

Published by the Australian Communications and Media Authority

Canberra Office
Purple Building, Benjamin Offices
Chan Street, Belconnen
PO Box 78,
Belconnen ACT 2616

Tel: 02 6219 5555
Fax: 02 6219 5353

Melbourne Office
Level 44, Melbourne Central Tower
360 Elizabeth Street, Melbourne
PO Box 13112 Law Courts
Melbourne VIC 8010

Tel: 03 9963 6800
Fax: 03 9963 6899
TTY: 03 9963 6948

Sydney Office
Level 15, Tower 1 Darling Park
201 Sussex Street, Sydney
PO Box Q500
Queen Victoria Building NSW 1230

Tel: 02 9334 7700, 1800 226 667
Fax: 02 9334 7799

Contents

1. EXECUTIVE SUMMARY 1

2. INTRODUCTION 3

2.1 Report background 3
2.2 Research objectives 3

3. METHODOLOGY 5

3.1 ACMA-commissioned consumer survey 5
3.1.1 Survey design 5
3.1.2 Data analysis 6
3.1.3 Limitations of the commissioned survey's methodology 6
3.2 Roy Morgan Single Source Australia Database 7
3.3 Definition of terms 7

4. PERCEPTIONS OF THE INTERNET 9

4.1 Concerns about the internet 13
4.2 Trust in the internet 18

5. BEHAVIOURS 20

5.1 Precautionary behaviours 20
5.1.1 Adult online behaviours 20
5.1.2 Behaviours of social networkers 21
5.2 Measures to minimise risk 24
5.3 Cybersafety 25

6. SKILLS AND CONFIDENCE IN INTERNET USE 29

6.1 Skills and confidence 29
6.1.1 Skill level by socio-economic and demographic profile 30
6.2 Confidence and competency 39

7. CONCLUSION 40

1. Executive Summary

This report is the first in the ACMA *Australia in the Digital Economy series* highlighting changing trends in the take-up and use of the internet by Australian consumers.

Specifically, it presents the findings of quantitative research into the attitudes and behaviours of Australian internet users regarding their online security. It seeks to build an understanding of the levels of trust and confidence in the internet and the factors which may facilitate or inhibit online confidence.

Australians value the internet and see it as critical to their daily lives. Over 11 million Australians use the internet for a wide range of activities relating to communications, business and social activities. Twenty-seven per cent of Australian internet users trust the internet as a valued source of information and prefer it to traditional media, such as newspapers, radio and the television.

However, while Australians overwhelmingly see the internet as having affected their lives positively, they still have concerns about the potential for the internet to negatively affect their privacy and security.

These concerns currently do not form a barrier to participation in the online environment, as increasing numbers of people use the internet for a wide range of activities including e-commerce and social networking.

This report also found that 36 per cent of Australian internet users consider the level of their internet skills to be above average while a further 45 per cent consider themselves as having average skill levels. Furthermore, many internet users are either self-taught or use other informal networks such as friends and family to build their online knowledge and skill levels. Younger Australians—18 to 30-year-olds, and males, were more likely to perceive their internet skill levels as being above average.

Skill levels are critical to ensuring Australians maximise the benefits of the internet, however, they are also important in ensuring that Australians are able to address any online risks by setting in place appropriate technological or behavioural measures.

Although more than 80 per cent of Australian internet users consider themselves to have average or above average internet skills and have concerns about online security, they are not proactive in protecting themselves online.

This report found that internet users are either not taking, or taking only limited measures to ensure their online security. The lack of action, both behavioural and technical, can be linked to a high reliance by internet users on informal methods of training and acquiring knowledge about the internet. Data presented in this report also shows that Australians have concerns

about keeping up with the pace of technological change. This may also impact on users' awareness of available technical measures to protect home computers from online risks.

While concerns over online security are not currently a barrier to participation, this report highlights the potential need for more formal and continuing education to address knowledge gaps about appropriate and available technical and behavioural measures to mitigate online risks. Equally important is the building of awareness of more appropriate information channels (both government and non-government) about online security threats, and measures to minimise their impact.

These measures would in turn complement the current high level of reliance on informal methods of acquiring internet skills and knowledge of online threats.

2. Introduction

2.1 Report background

Since its inception, the internet has evolved from primarily a research network to an essential form of communications underpinning the developing digital economy. As the internet has become increasingly prevalent in homes and businesses, it has facilitated both economic and social interactions, in addition to alternatives to traditional voice telephony and has emerged as a new channel for the distribution of content.

In Australia, concerns over the integrity of the online environment have also led to a range of initiatives aimed at building trust and confidence in the internet. These initiatives have ranged from increasing consumer awareness of online threats, through tackling spam, to filtering illegal content. Previous research explores these issues[1] and ACMA's website also provides tips for consumers on how to protect their computers against online threats. The information can be found at http://www.acma.gov.au/WEB/STANDARD/pc=PC_310294.

As the statutory authority responsible for communications and media regulation in Australia, ACMA has responsibilities to conduct research into issues relating to internet content and internet carriage services, and to conduct community education (clause 94 of Schedule 5 of the *Broadcasting Services Act 1992*) and report on matters affecting consumers or proposed consumers of carriage services (section 8 (paragraph d) of the *Australian Communications and Media Authority Act 2005*).

This report, *Australia in the Digital Economy: Trust and Confidence*, is part of this process, and aims to contribute to greater understanding of Australians' attitudes and behaviours towards their online security.

2.2 Research objectives

This report presents the main findings of a national survey into attitudes and behaviours of Australian internet users towards their online security in particular:

1. perceptions of the internet as a trusted source of information;
2. the level and type of online protection adopted by internet users;
3. levels of internet competency and sources of internet training;

[1] ACMA, 2008. *Developments in internet filtering technologies and other measures for promoting online safety*, February 2008, http://www.acma.gov.au/WEB/STANDARD/pc=PC_311304, accessed November 2008.

4. levels of awareness and sources of information about threats to online security; and
5. how factors such as age, education level, frequency of internet use and online competency influence the above factors.

3. Methodology

The data in this report is drawn from a number of sources, including the Australian Bureau of Statistics (ABS), private sector data sources from Nielsen Online and Roy Morgan Single Source Australia and a survey into online security attitudes and behaviours commissioned by the ACMA.

3.1 ACMA-commissioned consumer survey

ACMA commissioned the consultancy firm Roy Morgan Research to undertake a national telephone survey in May–June 2008. The survey explored consumer attitudes towards and perceptions of communication services. This survey included a number of questions relating to online security behaviours and attitudes.

3.1.1 Survey design

The survey was tailored to two subgroups:

- fixed-line users (fixed-line survey)—1396 people; and
- mobile phone–users who are not connected to a fixed-line service (mobile-only survey)—241 people.

The 2008 survey questionnaire was based on the survey undertaken by ACMA in 2007 for its *Telecommunications Today* series of reports; however, the number of questions was extended to provide a deeper analysis of access to, and behaviour in, the online environment.

In addition to questions about general household communications, fixed-line and mobile phone–only users were asked specific questions about their use and behaviour regarding their communications preferences. Thus, in the survey of mobile phone–users, respondents were not asked questions about their fixed-line activity.

Fixed-line survey

The electronic WhitePages® was used as the sampling frame for 1396 people and the interviews were undertaken using computer assisted telephone interviewing (CATI). All respondents were aged 18 years and over and screened to ensure that they were the main or joint decision-maker in relation to at least one household telecommunications service.

The target sample was structured to boost the non-metropolitan component with post-weighting by age, gender and location to the true proportions. The sample is outlined in Tables 1 and 2.

Table 1. Quantitative sample: Fixed-line and mobile survey, by age and gender

	Number of interviews		
Age range	Male	Female	Total
18–24	102	98	200
25–34	155	160	315
35–44	119	160	279
45–54	150	165	315
55–64	116	152	268
65–69	49	49	98
70 and over	90	72	162
Total	**781**	**856**	**1,637**

Table 2. Quantitative sample: State/territory of residence and metropolitan/non-metropolitan

	Number of interviews		
	Metropolitan	Non-metropolitan	Total
NSW/ACT	335	229	564
Vic.	284	112	396
Qld	147	178	325
SA/NT	90	51	141
WA	115	47	162
Tas.	19	30	49
Total	**990**	**647**	**1,637**

Mobile-only survey

For the mobile-only survey, Roy Morgan Research surveyed 241 people who had indicated in previous surveys that they used a mobile phone but did not have a fixed-line service in their household. The participants in this survey were asked to confirm their communications use before proceeding.

3.1.2 Data analysis

Results from the survey were analysed using descriptive analysis techniques on socioeconomic and demographic factors to identify any areas with significant differences. Only results with significant differences are reported in this research.

3.1.3 Limitations of the commissioned survey's methodology

CATI surveys

While all survey methodologies have their advantages and disadvantages, there are some specific limitations of CATI surveys which had an impact on the sample:

- CATI surveys exclude people without a fixed-line phone and people with silent numbers; this was addressed by the creation of a mobile phone–only subgroup, as outlined above.
- CATI surveys may also be biased towards those who normally stay at home (e.g., older or retired people, or those whose occupation is home duties). This bias was limited in the survey by scheduling interviews across the day.

Sample size

While all results in this research are statistically significant, the sample size limits any further analysis by smaller subgroups, for example, data at state level or by both gender and age.

Rounding

Discrepancies may occur between the sums of the component items and totals due to the effects of rounding.

3.2 Roy Morgan Single Source Australia Database

Roy Morgan Single Source Australia Database is a survey of individual consumers aged 14 years and over drawn from a large base survey sample (more than 25,000 per year in Australia). The Roy Morgan Research statistics cited in the report were derived from data collected between July 2007 and June 2008.

3.3 Definition of terms

Consumers

For the purpose of this report and unless identified otherwise, a consumer is a survey respondent, who owns, uses or has otherwise accessed telecommunications equipment or services.

Antivirus

Antivirus programs can identify and eliminate a virus by inspecting the contents of a file and then comparing it to a known virus pattern.

Cookie

Information stored on a device for the purpose of tracking an end user's use of a website or registering their preferences. Parcels of text sent from a server to a web client (usually a browser) for authenticating, session-tracking (site maintenance), and for maintaining specific information about users, such as their site preferences or the contents of their electronic shopping carts.

Firewall

A firewall is a software or hardware application which can limit access to a computer from an external network. By limiting access, users can take measures to protect their private data on their computers.

Malware

Viruses, worms, trojan horses, spyware and keystroke loggers are all part of a class of software known as malicious code. Many early forms of malware were written as pranks that were intended to disrupt organisations' functioning rather than cause

serious damage. However, malware is now increasingly used for extortion through denial of service attacks and to perpetrate online fraud.

Online Fraud

The use of personal information to commit theft or fraud online. Online fraud may involve theft through harvesting personal information that has been posted by users on websites to create fake credit accounts, or the use of malware to access banking information or passwords.

Social Networking

Using the internet to build and maintain relationships with other users. Most social networking websites contain personal profile information, blogs, message boards, chat and email.

Spam

Unsolicited messages often sent in bulk to a large number of email addresses.

Spyware

Spyware software can install itself on a user's computer without their knowledge and is used to capture personal information without the user's knowledge for business purposes, such as advertising, or criminal purposes.

Trojan Horse

A Trojan horse is malware hidden in messages or in other apparently innocent software that can be executed at a specific time or under specific circumstances.

Virus

Programming code created as a prank or as a malicious action that secretly affects other programs and causes unwanted consequences. Examples of viruses and destructive programs are Trojan horses, worms and logic bombs.

Worms

A worm is considered to be a subcategory of a virus. However, unlike a virus, a worm has the ability to travel from machine to machine with the assistance of the user in order to carry out its purpose, whether it be to delete data, steal sensitive information or deny service.

4. Perceptions of the internet

Trends in internet use show that the majority (11.3 million in 2007[2]) of Australians are logging on to the internet during any month. The links between internet access and factors such as age, education and income have been clearly established in previous research particularly in the ABS publication, *Patterns of Internet Access in Australia 8146.0.55.001* (2006), and are also shown in Figures 1 and 2 below.

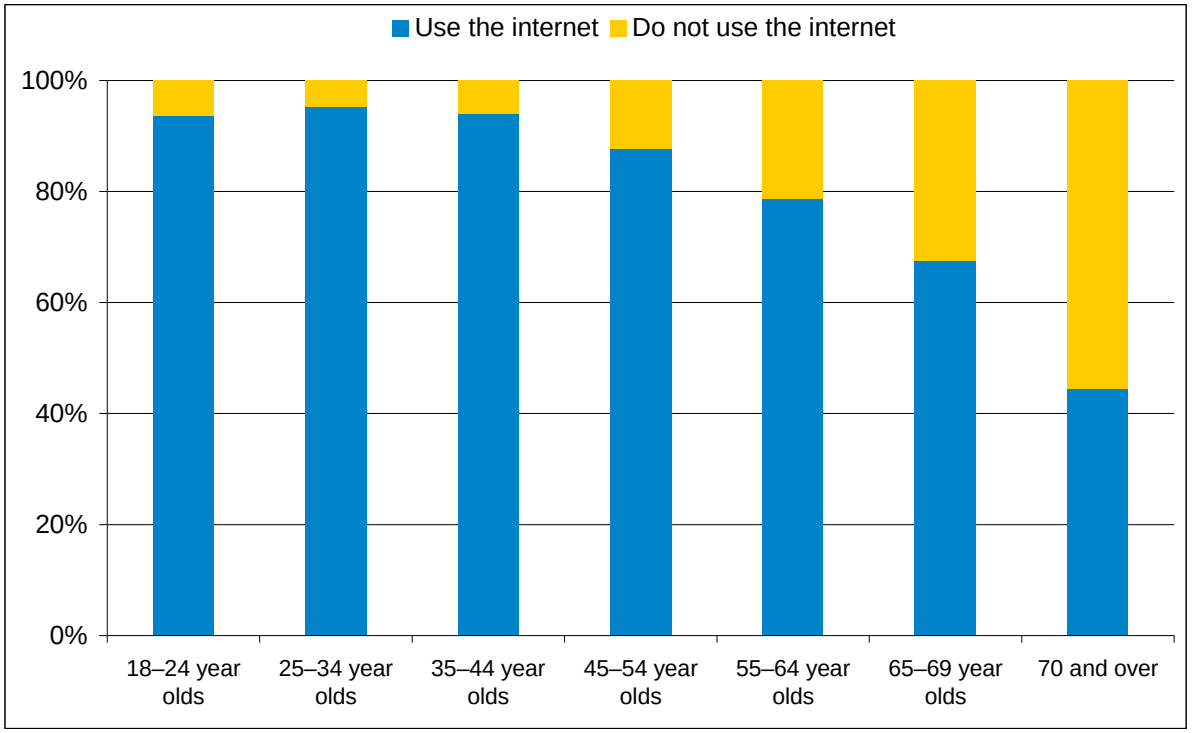
A majority of all age groups are using the internet, except those aged over 70 years. Over 90 per cent of 18 to 44-year-olds were estimated to use the internet, compared with 88 per cent of 45 to 54-year-olds, 79 per cent of 55 to 64-year-olds, 68 percent of people aged 65 to 69, and 44 per cent of those aged over 70 years.

More than 90 per cent of those people who have either completed or are completing tertiary qualifications use the internet, compared with less than 40 per cent of those who responded that primary school was their highest level of education obtained.

It is generally accepted that higher educational levels usually indicate higher incomes. This report will therefore focus on the highest educational level achieved as a substitute for other socioeconomic factors such as personal income level.

[2] ABS, 2008, *Household use of information technology*, Australia, 2006 to 2007, 8146.0, http://www.abs.gov.au/Ausstats/abs@.nsf/mf/8146.0, accessed November 2008.

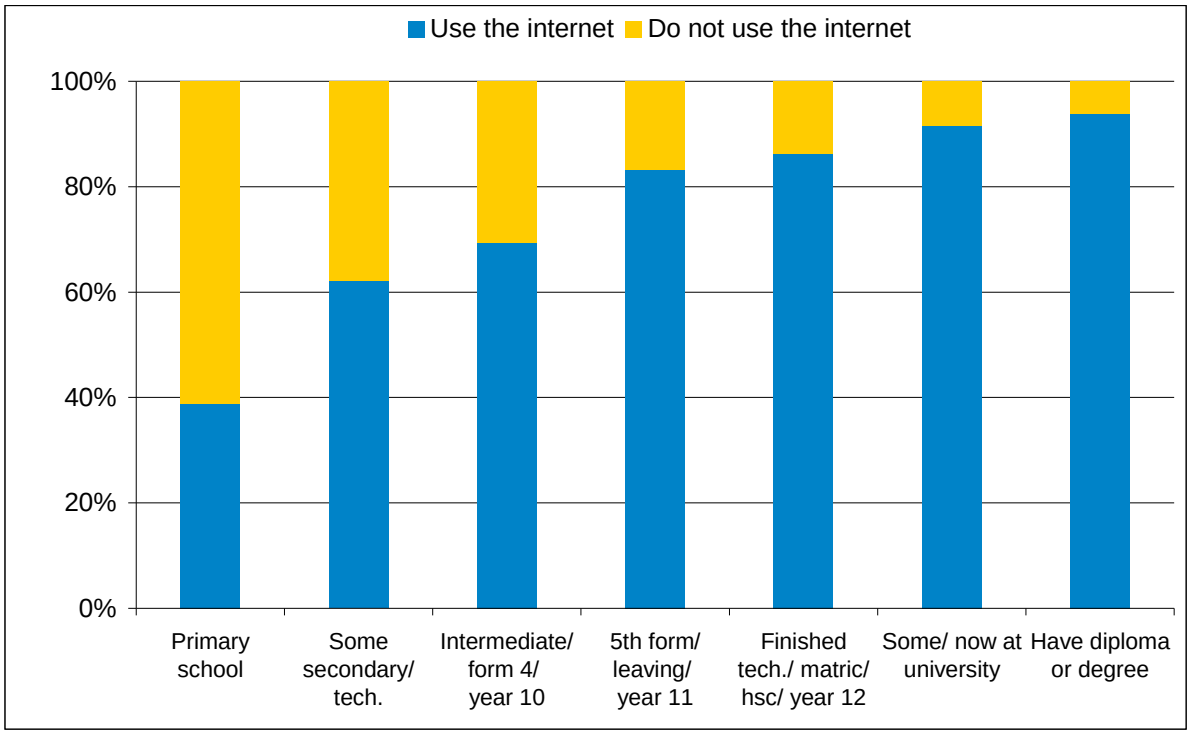
Figure 1. Internet users, by age



Note: excludes respondent category 'cannot say'.

Source: ACMA-commissioned consumer survey May–June 2008, internet users aged 18+, (n = 1348).

Figure 2. Internet users, by education level



Note: excludes respondent category 'cannot say'.

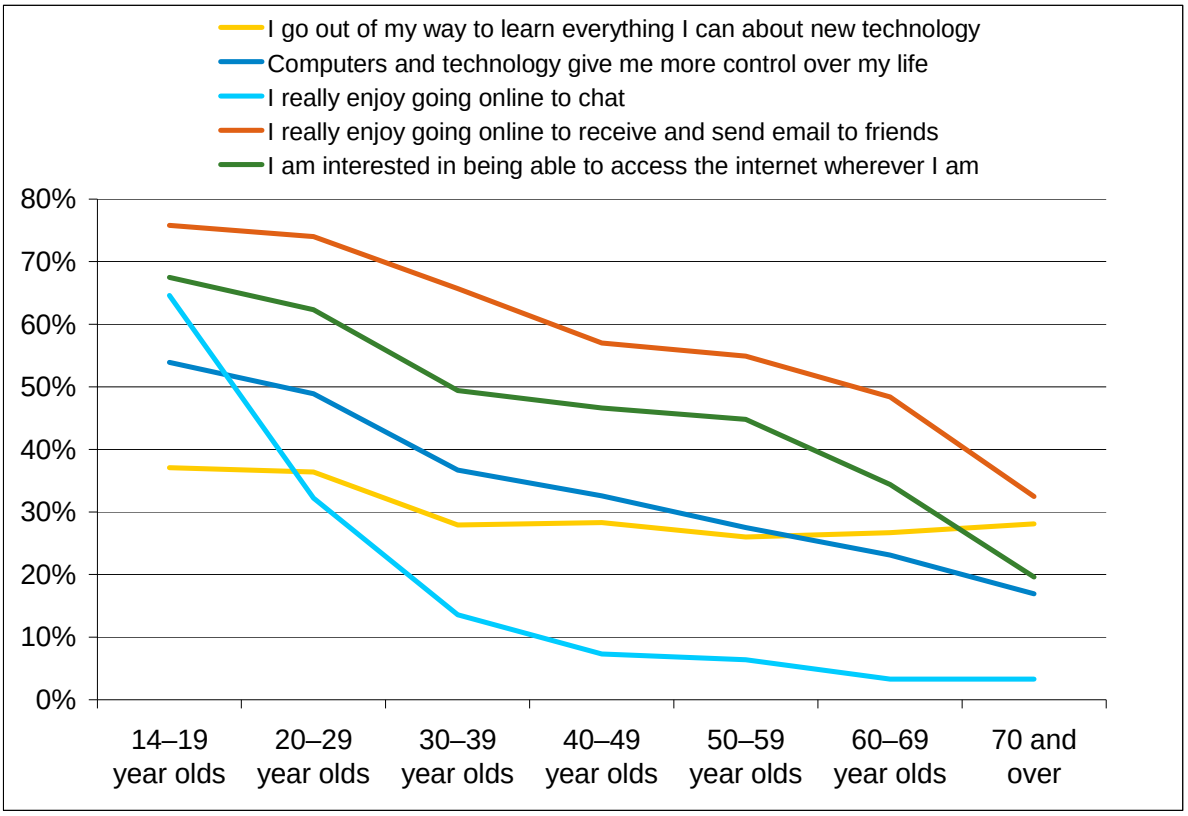
Source: ACMA-commissioned consumer survey May–June 2008, internet users aged 18+, (n = 1348).

Data obtained from Roy Morgan Single Source Australia confirm that younger age groups are more likely to value the internet and find it an integral part of their lives.[3] Figure 3 reveals that 49 to 54 per cent of those aged under 30 years stated that computers and technology gave them more control over their lives, compared with approximately 17 to 23 per cent of those aged 60 years and over. A majority of 14 to 19-year-olds value the internet as a communications tool, with more than three-quarters of this group stating that they 'really enjoy' going online to receive and send emails to friends.

The data also revealed that 62 to 68 per cent of those aged under 30 years responded that they would like to be able to access the internet from wherever they are.

Positive attitudes towards the internet decrease with age. Over three-quarters of 14 to 19-year-olds enjoy going online to receive and send emails to friends, compared with 48 per cent of those 60 to 69-year-olds, and 33 per cent of those aged over 70 years.

Figure 3. Internet users' attitudes about the internet, by age

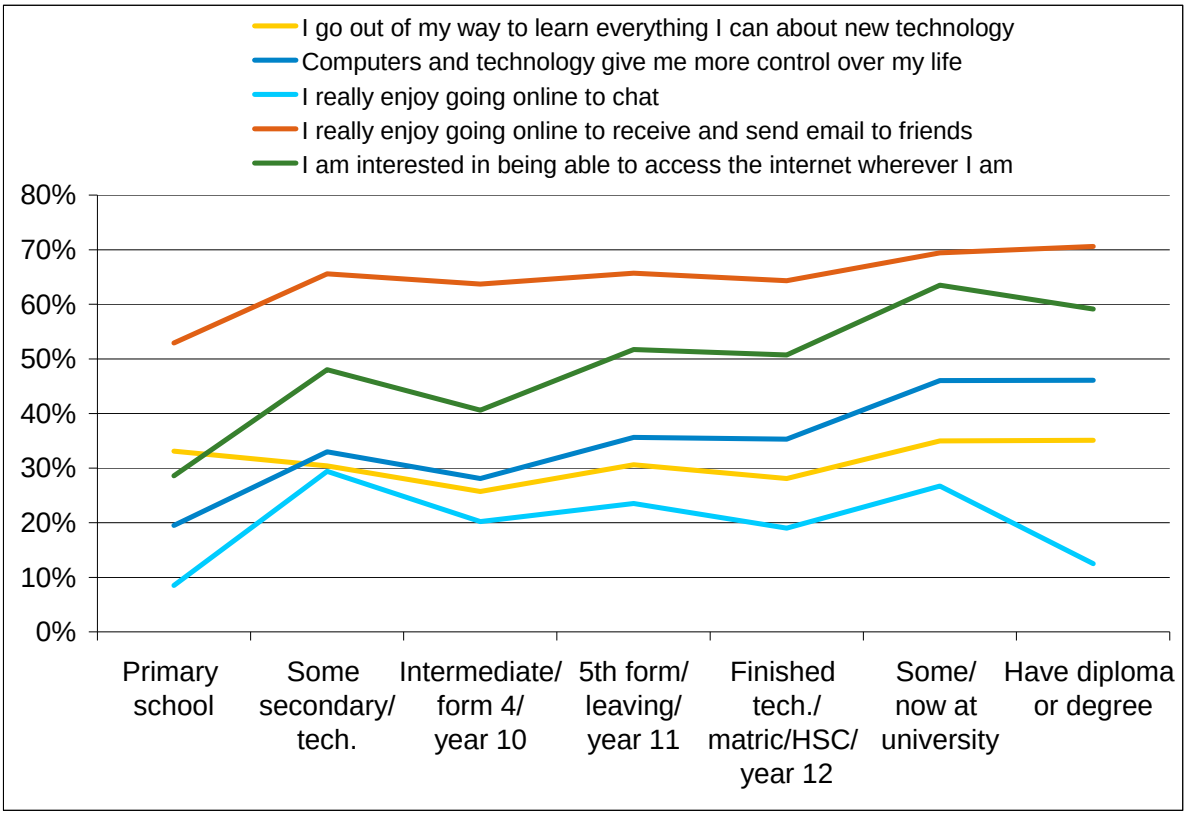


Source: Roy Morgan Single Source Australia Database, internet users aged 14+, Jan 08–Jun 08, (n = 10329).

[3] Roy Morgan Single Source Australia Database, Australians Aged 14+.

There is a weaker relationship between educational attainment and attitudes to the internet (Figure 4). However, variations in positive responses depended on the various issues examined. With the example of flexibility of internet access, 27 per cent of internet users whose highest level of educational attainment was primary school responded positively to the statement 'I am interested in being able to access the internet from wherever I am', compared with 59 per cent of those who have obtained or are in the process of obtaining a degree or diploma. This contrasts with positive responses to the statement, 'I go out of my way to learn everything I can about new technology', where responses ranged from a minimum of 26 per cent to a maximum of 35 per cent.

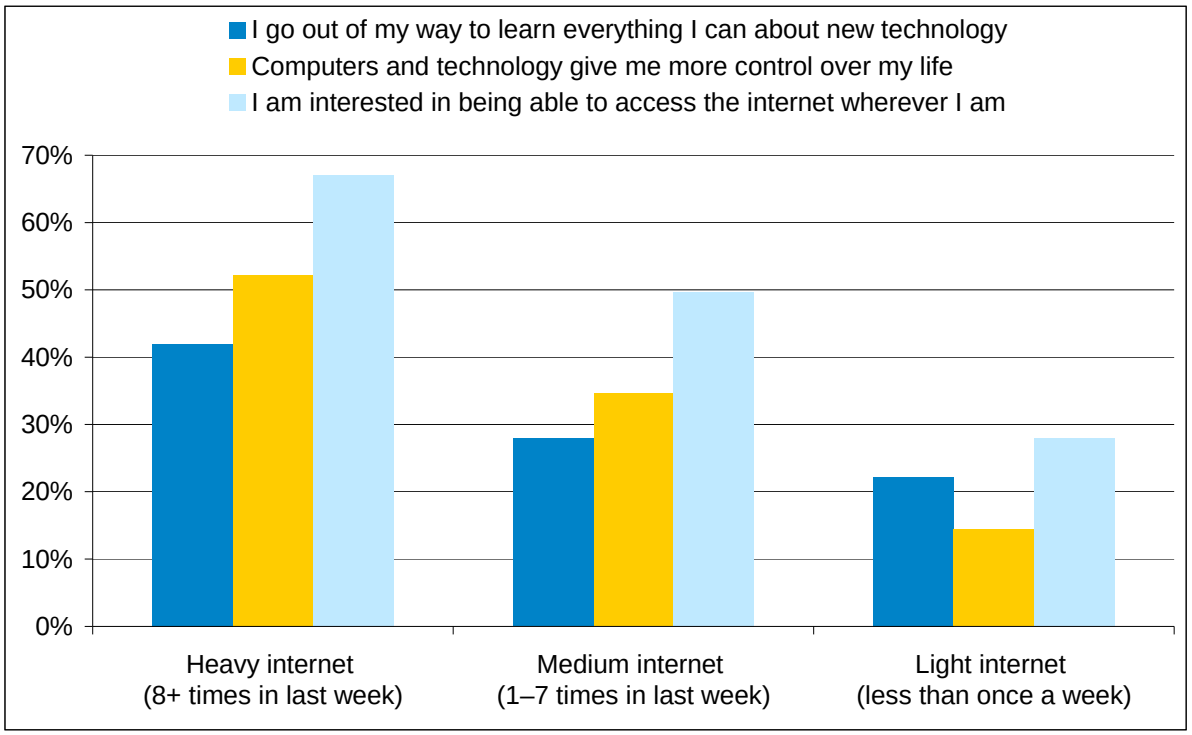
Figure 4. Internet users, by highest education level obtained to date



Source: Roy Morgan Single Source Australia Database, internet users aged 14+, Jan 08–Jun 08, (n= 10329).

Figure 5 shows that a correlation also exists between positive attitudes towards the internet and frequency of internet use, which indicates that this is more than a socioeconomic relationship. The relationship between frequency of internet use and age is explored in the ACMA report *Telecommunications Today Report 6: Internet Activity and Content*. This report revealed that 18 to 24-year-olds and 25 to 34-year-olds are more likely to be heavy users of the internet and that this relationship declines with age. These findings indicate that the internet holds a higher value to younger Australians—the majority of whom are connected to the internet and use it more frequently. Given that young Australians are more likely to be frequent users, they are the core group to which awareness and educational campaigns should be tailored.

Figure 5: Attitudes towards the internet by frequency of use



Source: Roy Morgan Single Source Australia Database, internet users aged 14+, Jan 08–Jun 08, (n=9490).

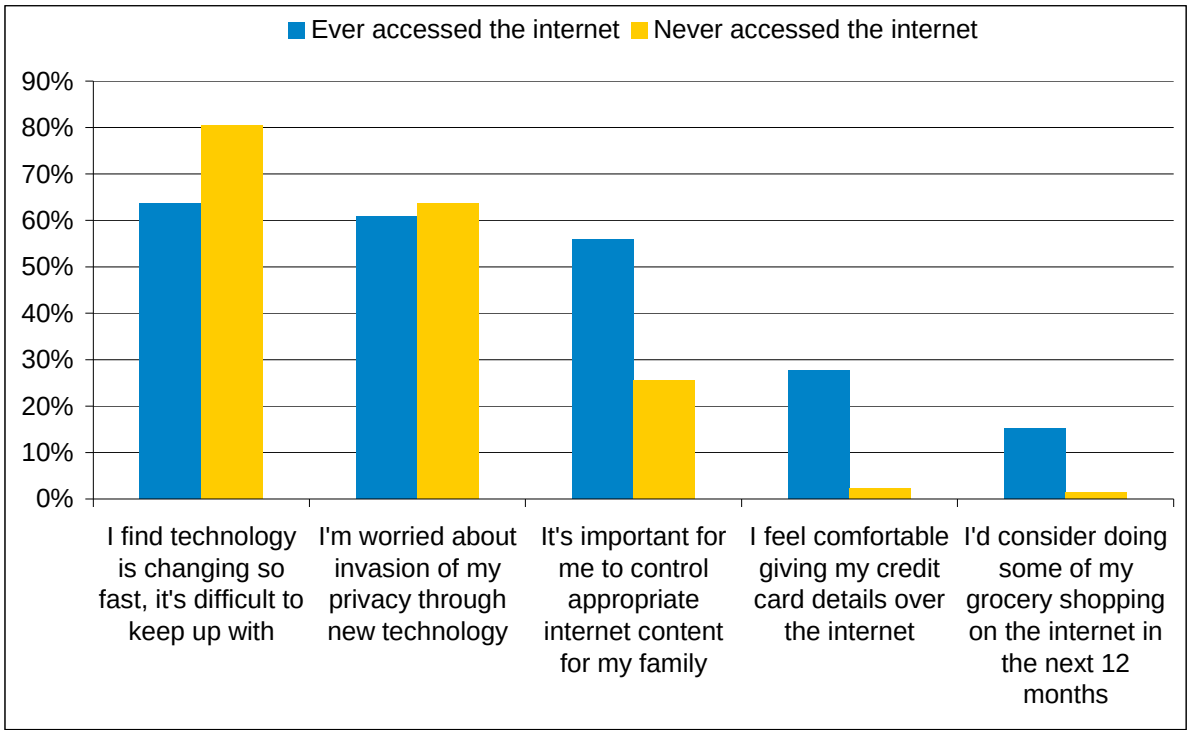
4.1 Concerns about the internet

The continued development of the digital economy at least in part hinges upon consumers' willingness to undertake activities such as online transactions, which is in turn affected by concerns about the security of the online environment. While a majority of internet users are positive about the internet, they are still concerned with security issues associated with new technology.

Users are particularly concerned about invasion of privacy and feeling unable to keep up with the perceived fast-pace of changes in new technology. Approximately equal numbers of both internet users and non-users (61 per cent and 64 per cent respectively) responded that they were worried about the potential for invasion of privacy through new technology (see Figure 6).

Those who have never accessed the internet are more likely to feel that they are out of their depth with technology and are less comfortable with the idea of giving credit card details over the internet, which is a key factor in their non-usage.

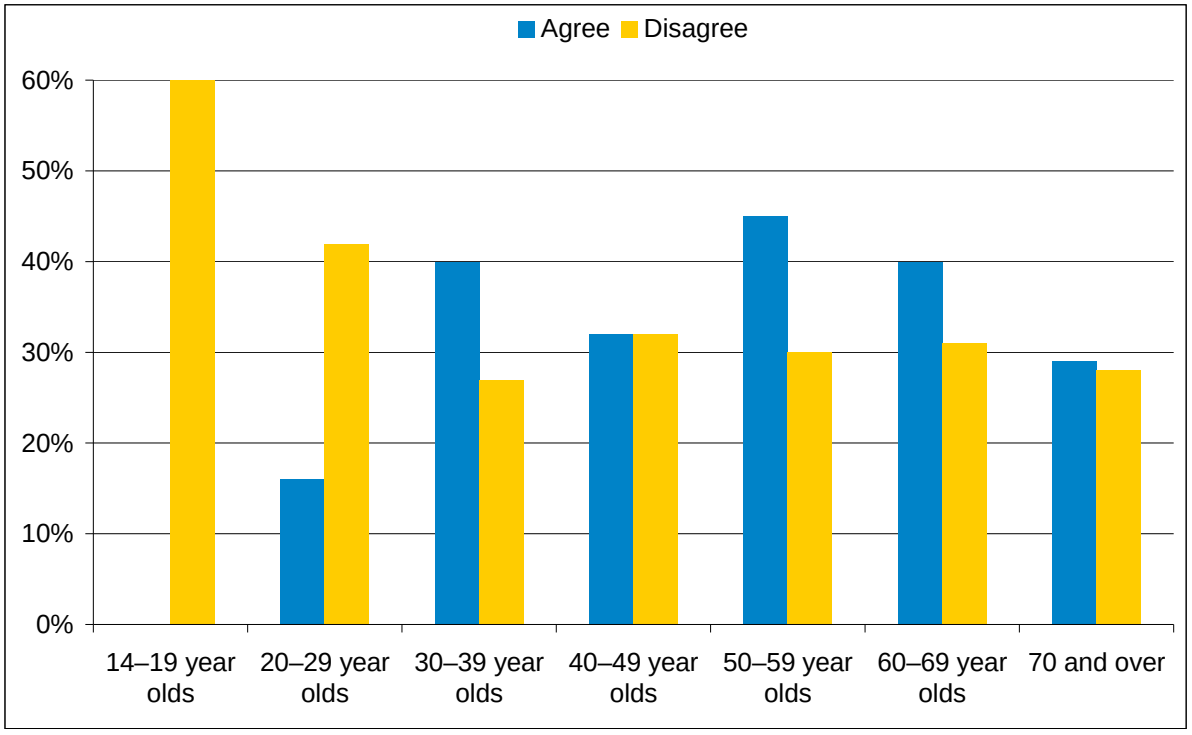
Figure 6. Internet attitudes: Concerns with the internet



Source: Roy Morgan Single Source Australia Database, Australians aged 14+, Jan 08–Jun 08, (n = 8280 users and 2049 non-users).

Young Australians are least intimidated by the complexity of the internet, regardless of whether or not they use it (Figure 7). None of the 14 to 19-year-old internet non-users agreed with the statement 'I feel intimidated by the complexity of the internet', compared with, 40 per cent of 30 to 39-year-olds, 45 per cent of 50 to 59-year-olds, 40 per cent of 60 to 69-year-olds and 28 per cent of those aged 70 and over.

Figure 7. Internet non-users responses to the statement "I would like to use the internet but feel intimidated by the complexity of it all", by age

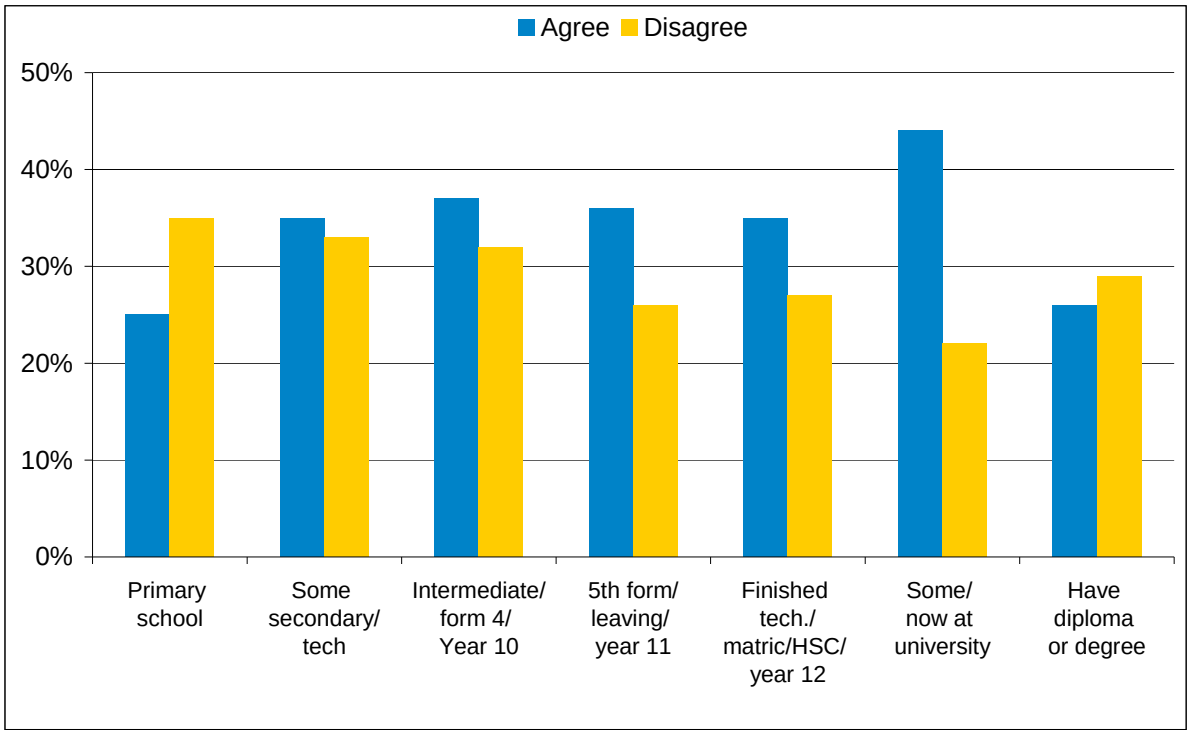


Note: excludes respondent category 'cannot say'.

Source: Roy Morgan Single Source Australia Database, internet non-users aged 14+, Jan 08–Jun 08, (n= 2049).

Figure 8 demonstrates a weaker relationship between internet non-users and the highest education level obtained. This is consistent with findings regarding positive attitudes towards the internet discussed earlier in this report (Figure 4).

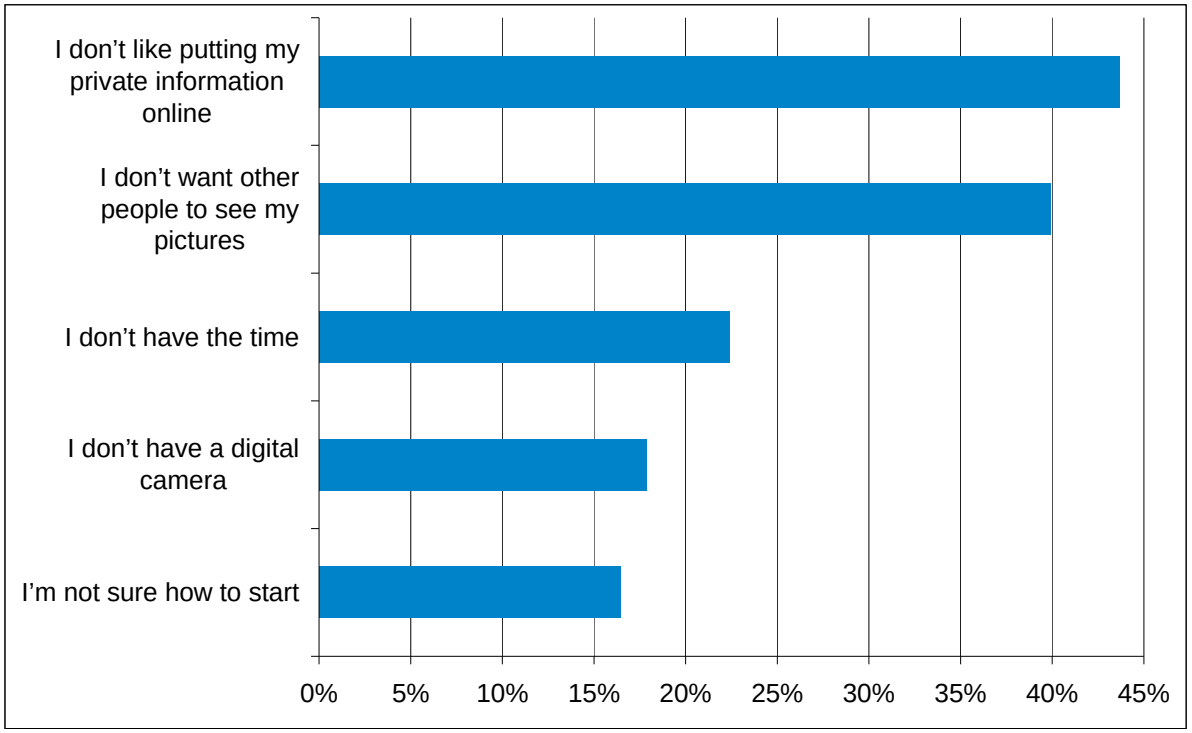
Figure 8. Internet non-users who feel intimidated by the complexity of the internet, by education level



Source: Roy Morgan Single Source Australia Database, internet non-users aged 14+, Jan 08–Jun 08, (n = 2049).

People are concerned with a range of privacy issues, including being personally identifiable online. For example, research shows that people from both Australia and New Zealand are concerned about putting their photos online. In a survey of internet users in May 2008 (Figure 9), 44 per cent of respondents to a question about why they did not upload photos to the internet indicated that they do not like to put their private information online. A further 40 per cent specifically did not want other people to see their pictures.

Figure 9. Barriers to uploading photos to the internet



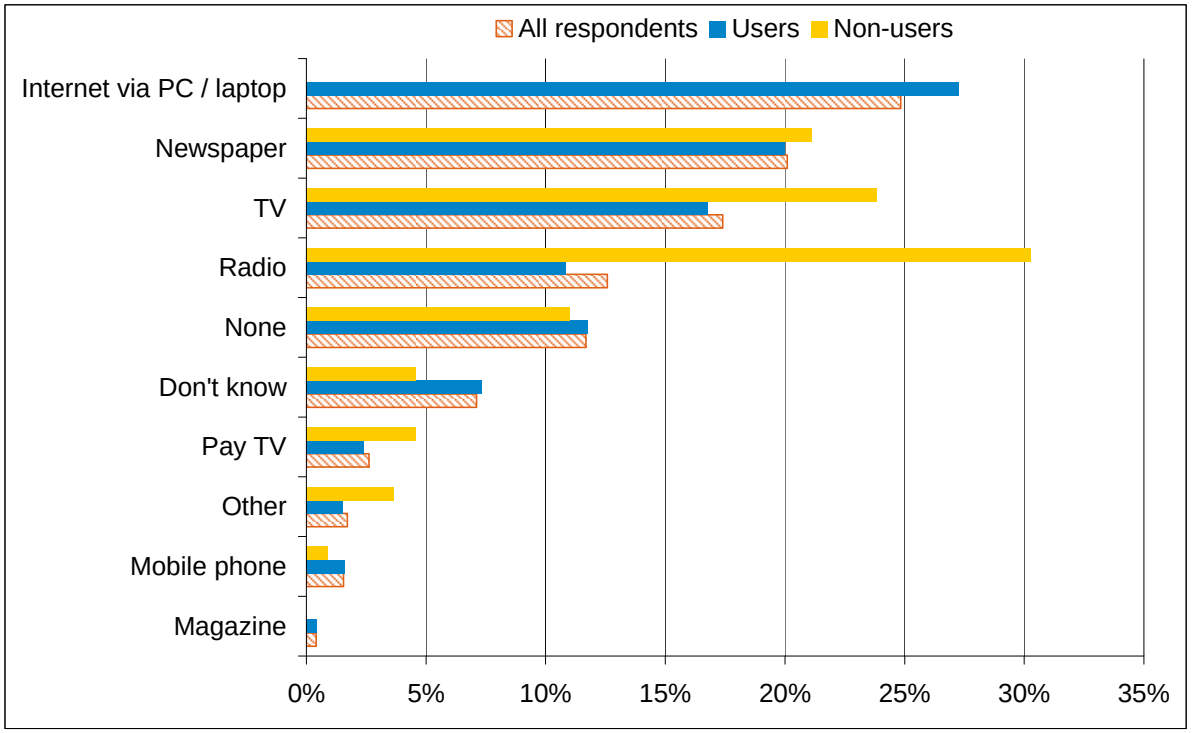
Source: Nielsen Online Consumer Generated Media Report 2008 – Volume 1, Australians and New Zealanders aged 16+, (n=723).

4.2 Trust in the internet

While consumers are concerned with new technology and the internet, research shows that internet users still rate the internet highly as a source of trusted information. Internet users rate their most trusted sources of information (Figure 10) as the internet (27 per cent), followed by newspapers (20 per cent) and television (17 per cent) while internet non-users place trust in radio (30 per cent), followed by television (24 per cent) and newspapers (21 per cent).

Generally there are three types of information available online: information on products, news and research information, and information obtained through peer-to-peer processes and online communities. Consumers may not be distinguishing between these types of information and may be confusing ease of access with quality of information; a suggested topic for further research.

Figure 10. Most trusted source of information by media type

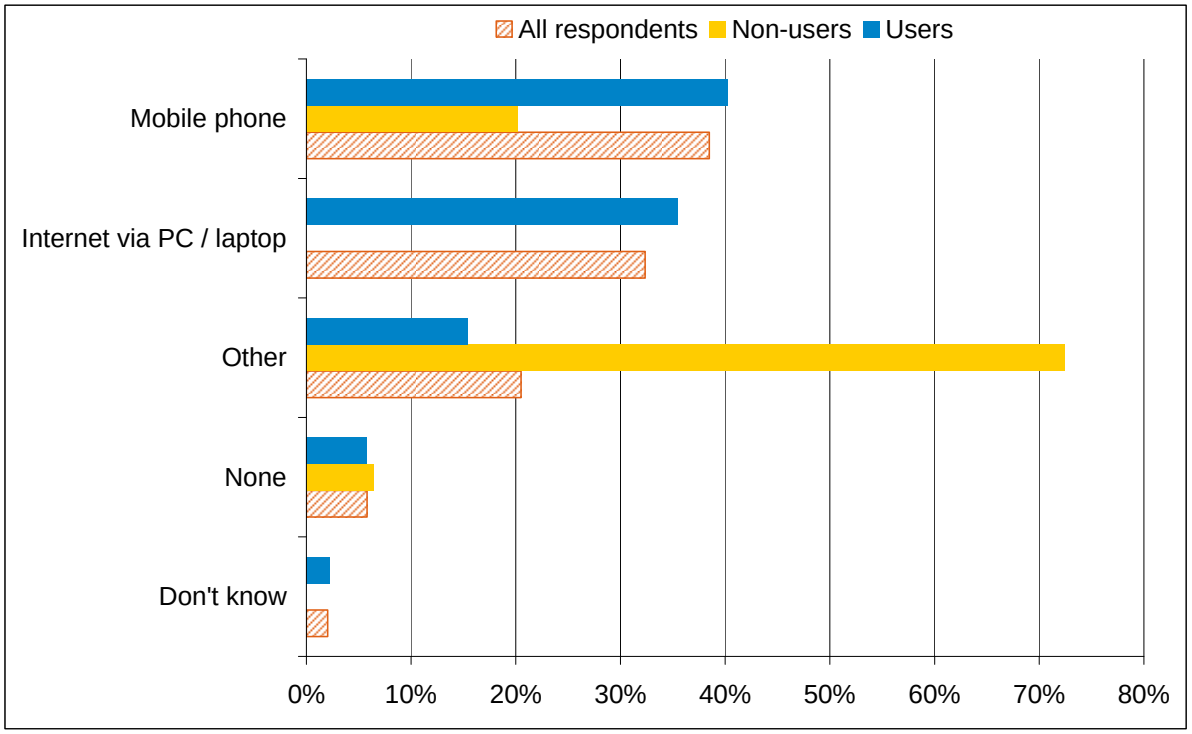


Note: 'All respondents' is the average responses of both internet users and non-users.

Source: Nielsen Online Australian Internet and Technology Report 2008, Australians aged 16+, (n=1456).

Among internet users, the mobile phone and the internet are identified as the preferred methods of communicating with family and friends (Figure 11). For non-internet users, other forms of communication such as the fixed-line phone or in-person communication are the most preferred form of communication with family and friends.

Figure 11. Preferred method to communicate with friends, family and others



Note: 'All respondents' is the average responses of both internet users and non-users.

Source: Nielsen Online Australian Internet and Technology Report 2008, Australians aged 16+, (n=1465).

5. Behaviours

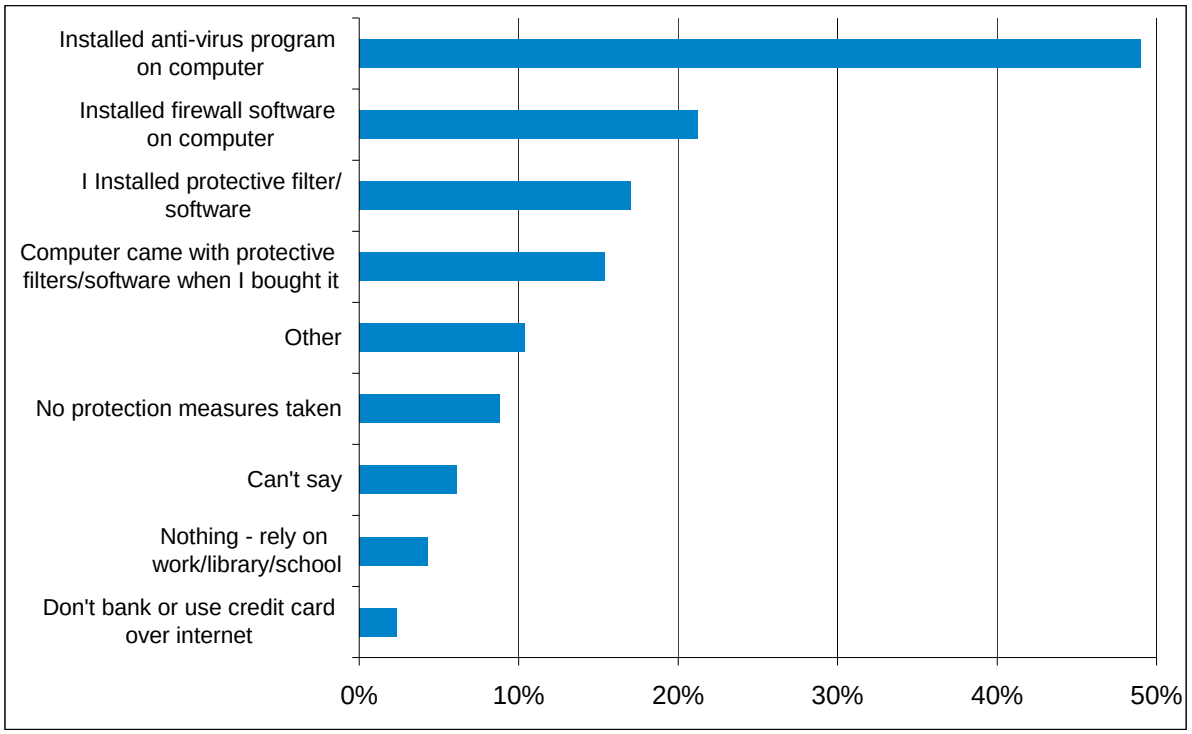
5.1 Precautionary behaviours

5.1.1 Adult online behaviours

Initial findings show that a majority of consumers are performing only one type of risk-mitigation measure.

Figure 12 shows that the installation of anti-virus and firewall programs on computers remain the two most common protective measures for home internet users, with 49 per cent having installed anti-virus software, and 21 per cent installing firewall software. Furthermore, the survey findings clearly showed widespread non-adoption of multiple protective measures as listed in Figure 12.

Figure 12. Internet users' measures against online risks and dangers



Source: ACMA-commissioned consumer survey, May–June 2008, internet users aged 18+, (n = 1346).

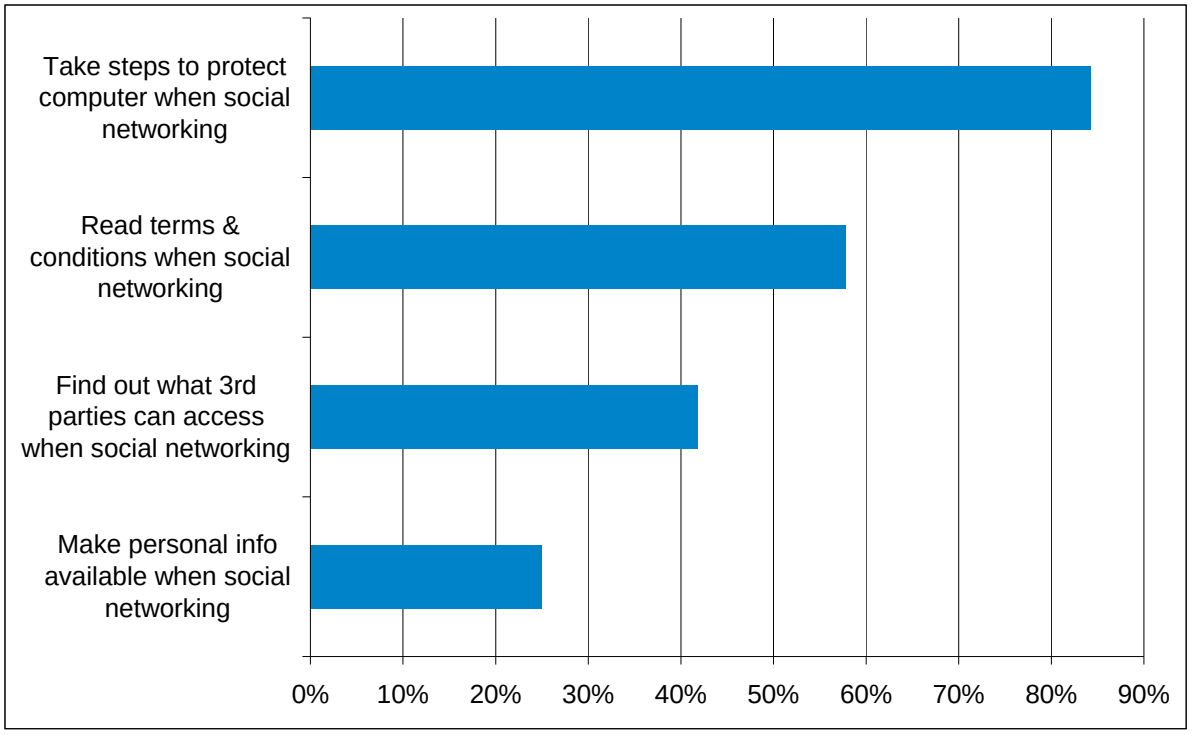
5.1.2 Behaviours of social networkers

While email remains the most popular activity on the internet, technological innovation has provided the setting for a range of new online activities. The internet now enables the development of online communities through social networking sites, which are growing in popularity. Consumers are using online social networking to strengthen ties with friends and family and develop connections with other like-minded people.

ACMA explores this issue in its report *Internet activity and content report* which showed that 56 per cent of online Australians have browsed other internet users' online profiles[4].

However, the rise of social networking has increased concerns over the risks of disclosing personal information online. The following analysis explores whether users of social networking sites and related services are more security-minded than internet users in general. Figure 13 shows that social networkers appear to be more security-aware, with 84 per cent of this group stating that they take steps to protect their computer and their privacy. However, Figure 14 shows that protective measures taken by social networkers to secure their computers from online threats are not very different to those of internet users in general.

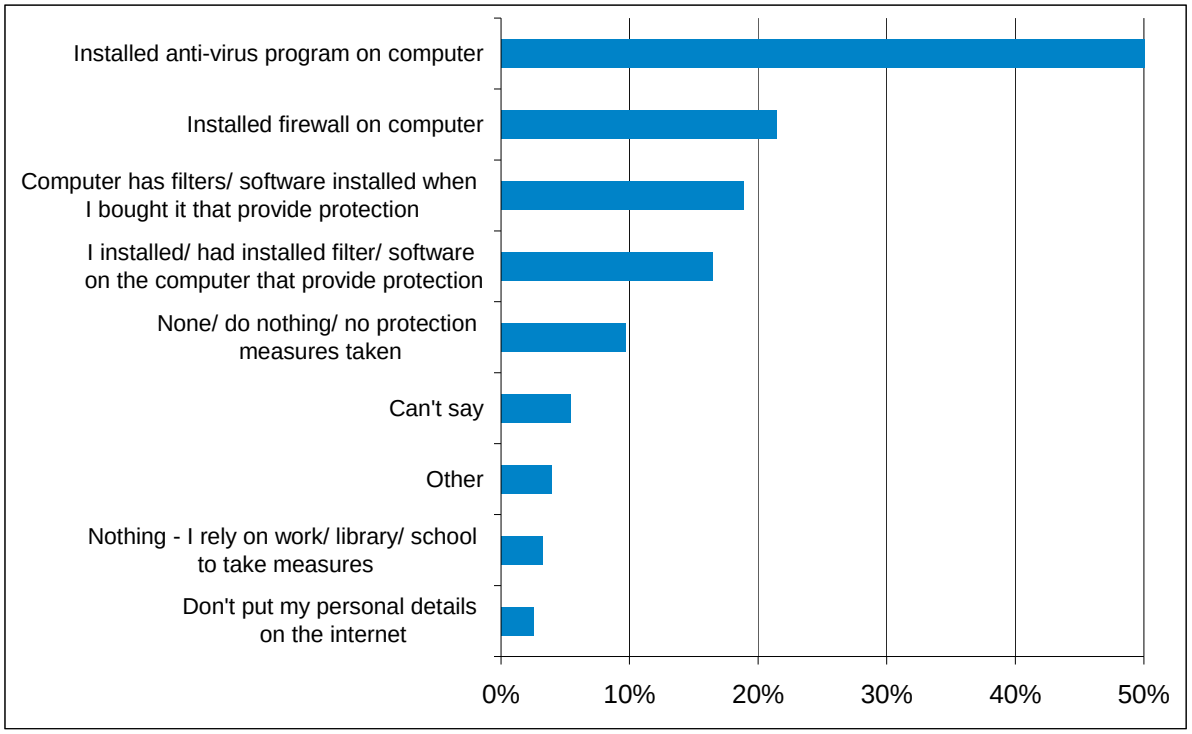
Figure 13. Precautions taken when social networking



Source: ACMA-commissioned consumer survey, May–June 2008, social networkers aged 18+, (n = 450).

[4] ACMA, 2008, Telecommunications Today Report 6: *Internet activity and content*, September 2008, http://www.acma.gov.au/WEB/STANDARD/pc=PC_9058, accessed November 2008.

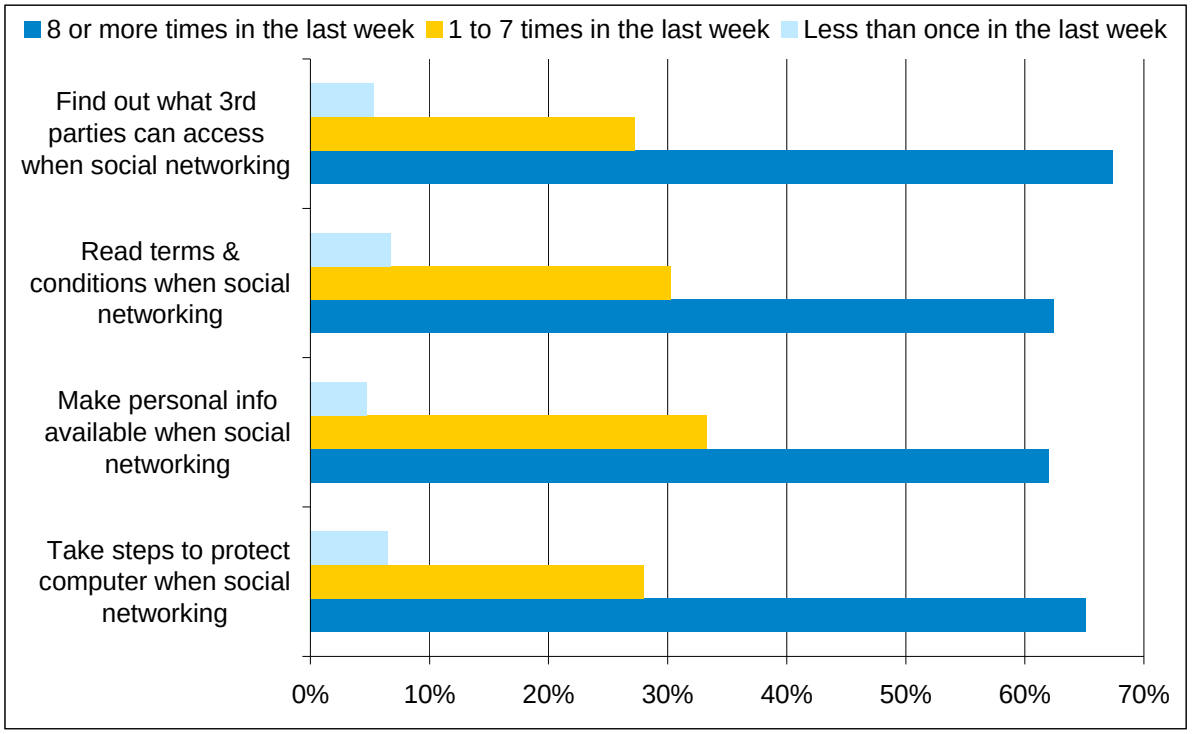
Figure 14. Social networkers' measures against risks and dangers



Source: ACMA-commissioned consumer survey, May–June 2008, social networkers aged 18+, (n = 450).

Social networking precautionary behaviours are also linked with frequency of internet use. Figure 15 illustrates the different measures taken by those who accessed the internet eight times or more in the last week compared with those who accessed the internet less frequently.

Figure 15. Precautions taken when social networking, by frequency of internet use



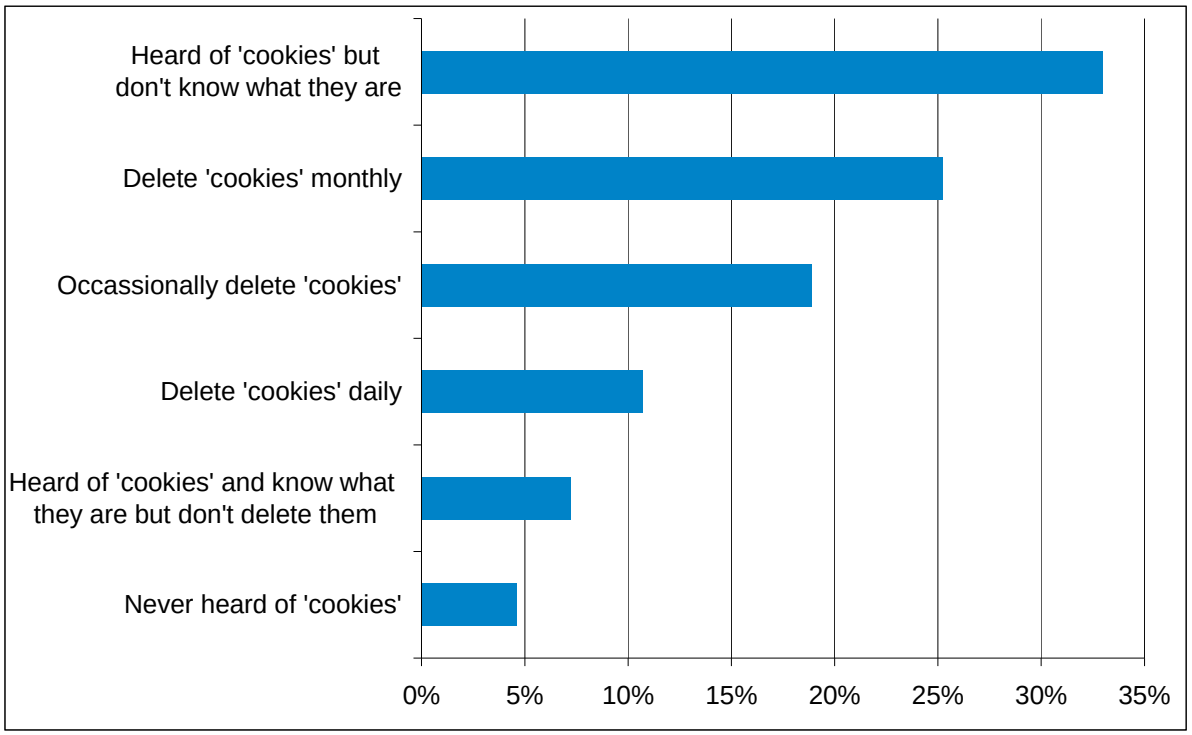
Source: ACMA-commissioned consumer survey, May–June 2008, social networkers aged 18+, (n = 450).

5.2 Measures to minimise risk

Consumers use a number of methods to mitigate online risk, including a range of proactive measures such as installing software and filters to modifying their online behaviours. One of the behaviours identified was deletion of ‘cookies’. Figure 16 shows that 36 per cent of internet users deleted cookies daily to monthly, 19 per cent occasionally deleted cookies, while a further 33 per cent did not know what cookies were.

The level of a consumer’s knowledge and skills play a part in their approach to online risk mitigation. This is in turn shaped by the channels they use to acquire internet skills and knowledge about online threats. Online skill levels and sources of internet training will be explored further in Chapter 6 of this report.

Figure 16. Internet users’ knowledge of cookies (March 2008)



Source: Nielsen Online Australian Internet and Technology Report 2008, Internet users aged 16+, (n=1456).

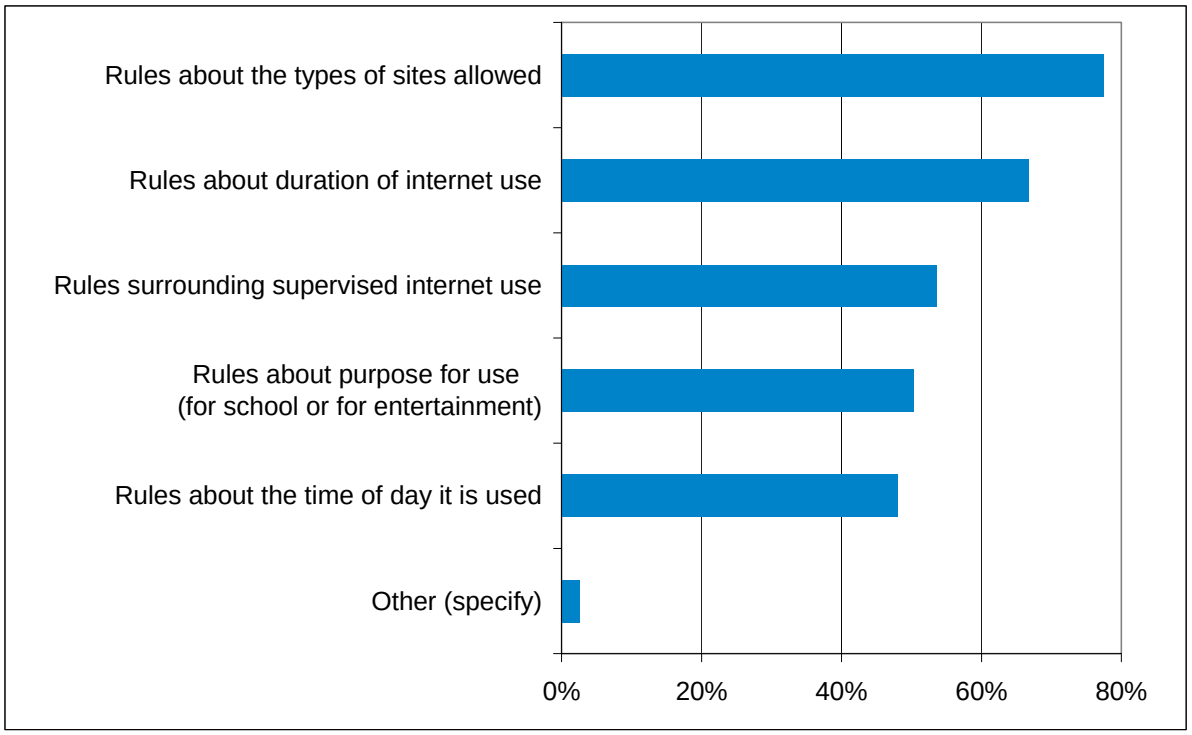
5.3 Cybersafety

Another aspect of online protection highlighted by privacy concerns is the protection of children online. Given the rise of new forms of online interactions such as social networking and the potential for exposure to inappropriate and illegal content, parents are concerned about their children's safety online. In light of these concerns, the majority of parents reported having rules in place regarding some aspect of their children's internet use. These rules cover factors such as direct supervision of internet use, duration and time of day of internet use, types of sites which children are allowed to access and the purpose of internet use (e.g. school versus entertainment). Whether parents actively implemented these rules is also explored in this report.

While the survey allowed for multiple responses, Figure 17 shows that while the majority of parents have some rules in place governing their children's internet use; these covered at most one or two key issues (duration and sites accessed). Of the parents with children who used the internet at home, 78 per cent reported that they had rules regarding the types of sites that could be accessed online by their children, compared with 67 per cent reporting having rules regarding the duration of internet use. In addition:

- 54 per cent reported having rules regarding supervised internet use;
- 50 per cent reported having rules regarding the purpose of internet use; and
- 48 per cent reported having rules regarding the time of day that their children could use the internet.

Figure 17. Parents' rules for their child's internet use



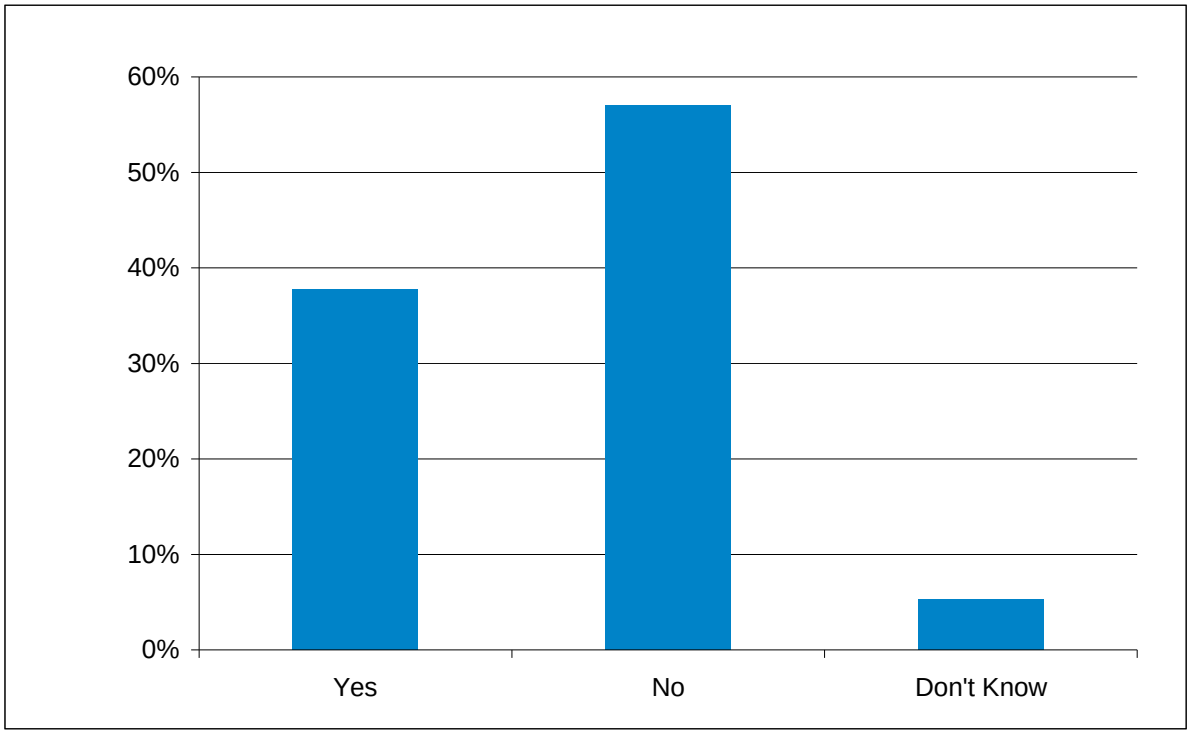
Source: Nielsen Online Australian eGeneration Report 2007-2008, (n=500).

Figures 18, 19 and 20 provide further insight into the perceptions and actions of parents regarding the online safety of their children.

As Figure 18 shows, when parents were asked whether monitoring or filtering software was used on their child's computer, only 38 per cent reported 'Yes'.

These findings are consistent with those explored earlier in this report which show that there is a lower level of reliance on technological solutions relative to other behavioural measures and the perception that it is difficult to keep pace with technological change.

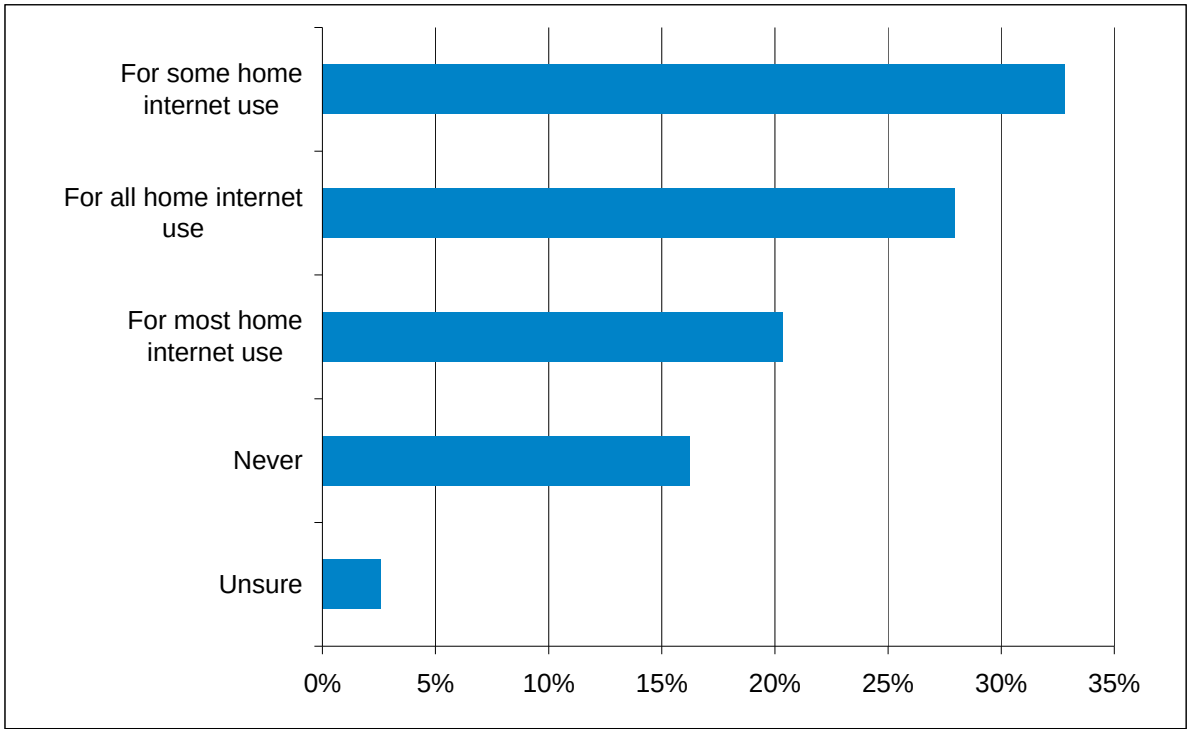
Figure 18. Parents with monitoring or filter software on their child's computer



Source: Nielsen Online Australian eGeneration Report 2007-2008, (n=500).

The frequency of parental supervision of children's internet activities was also explored in the Nielsen survey. Figure 19 shows that an estimated 33 per cent of parents with children using the internet at home reported supervising some of their child's home internet use. A further 28 per cent of parents reported supervising all home internet activities of their children, just over 20 per cent reported supervising most home internet activities and 16 per cent reported never supervising their children's internet activities.

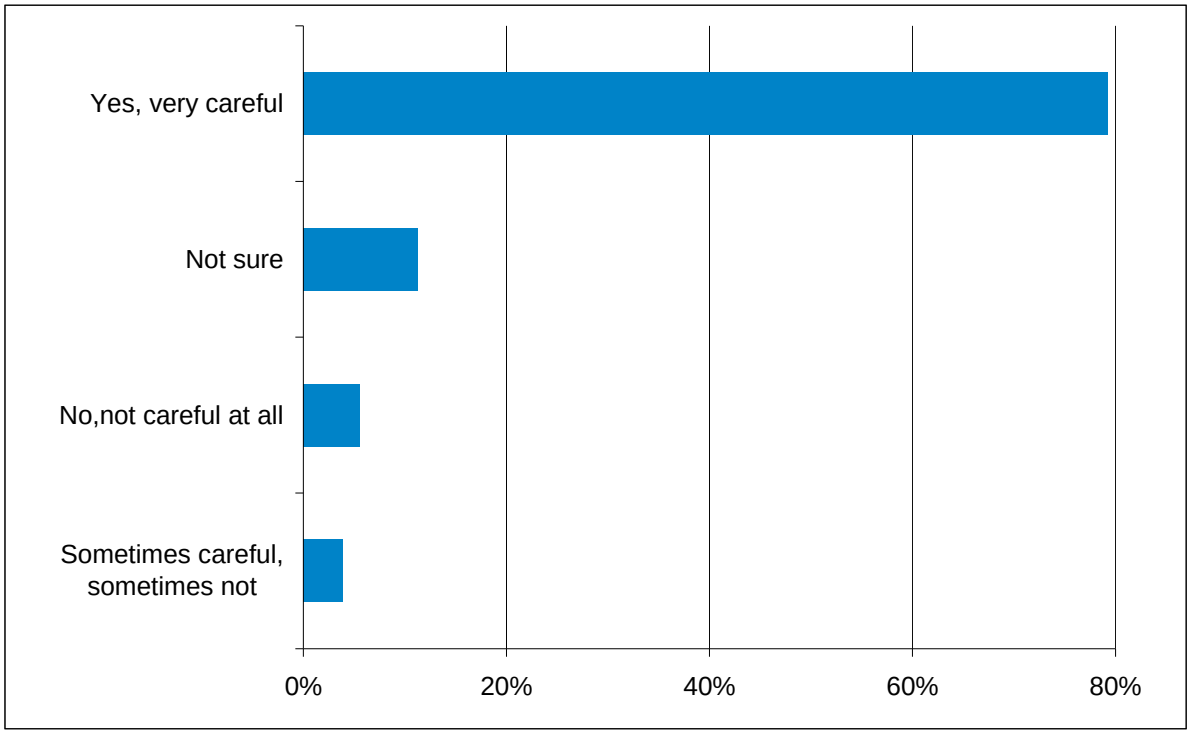
Figure 19. How often parents supervise their child's internet use



Source: Nielsen Online Australian eGeneration Report 2007-2008, (n=500).

Although parents engage in monitoring and filtering behaviours, the majority place trust in their children and believe their child is careful with the type of information they give out about themselves online. Figure 20 highlights this, showing that the overwhelming majority of parents (79 per cent) reported that their children were very careful when providing information online.

Figure 20. Parent perception of care taken by their children in relation to providing information online



Source: Nielsen Online Australian eGeneration Report 2007-2008, (n=500).

6. Skills and confidence in internet use

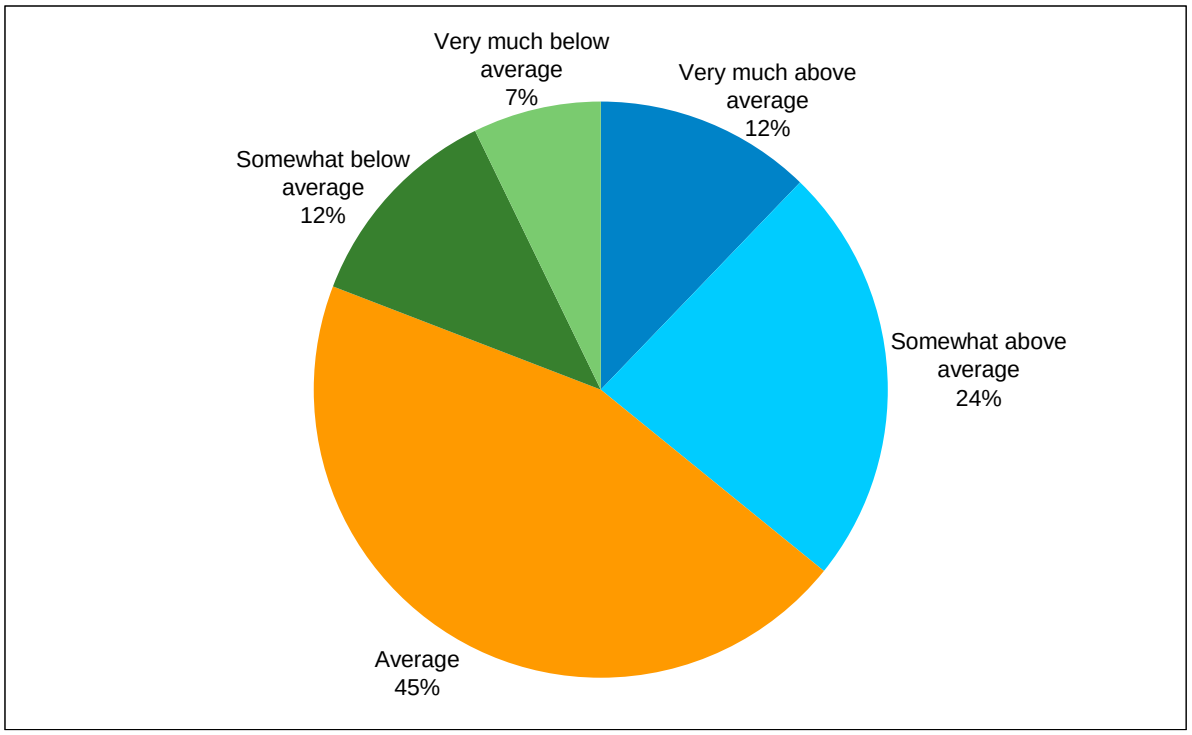
Consumers appear to place a large amount of trust in the internet and see the benefits of online participation as far outweighing the likelihood of breaches of online security and privacy. The levels of trust in the internet are linked to perceived skill levels of individuals and their source of information about the internet.

6.1 Skills and confidence

The level of skill in using the internet underpins consumers' understanding of the risks of undertaking particular activities online and will also affect the sources of information they seek out to protect themselves online.

Eighty-one per cent of internet users are confident in their skills and perceive themselves to have average (45 per cent) or above average (36 per cent) skills in using the internet (Figure 21).

Figure 21. Self-assessed skill level of internet users



Note: Excludes respondent category 'cannot say'.

Source: ACMA-commissioned consumer survey, May–June 2008, internet users aged 18+, (n = 1340).

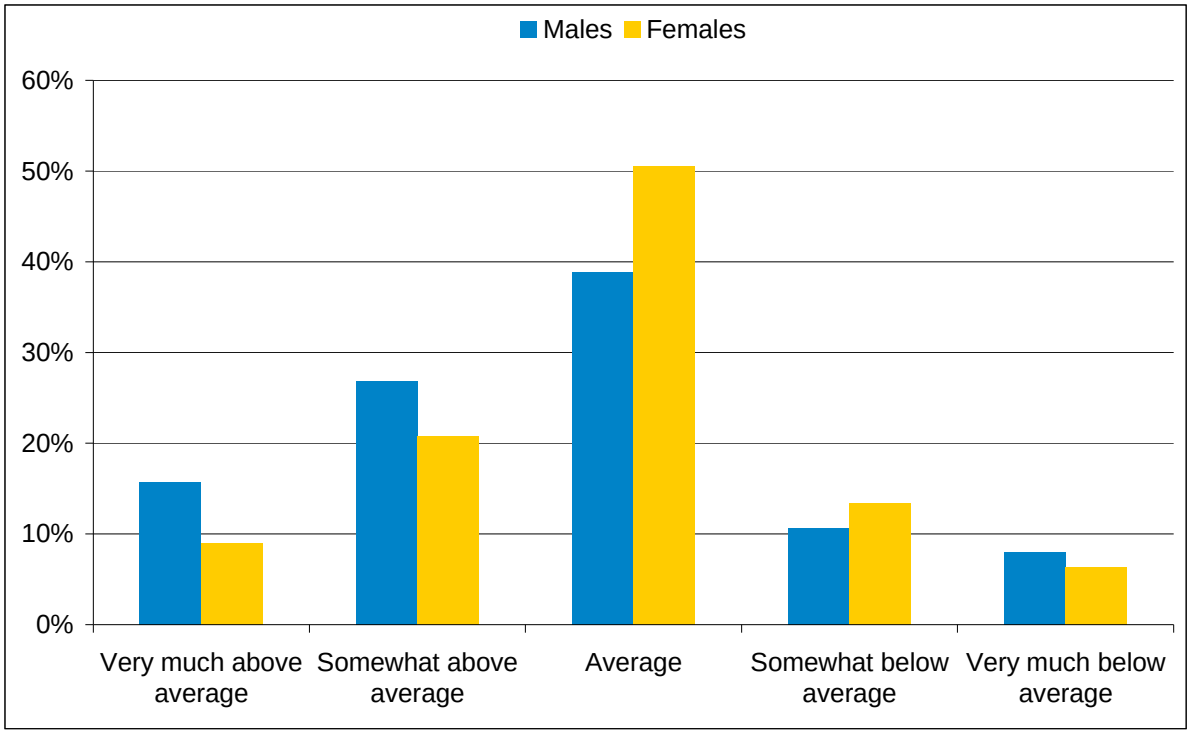
While there is no single profile of those who rate their internet skills as above average, it does appear that males and 18 to 30-year-olds are more likely to be heavy internet users and are also more likely to rate themselves as having above average internet skill levels (Figures 22 and 23).

6.1.1 Skill level by socio-economic and demographic profile

Insights into the reasons for the lack of precaution taken by those self-identified as having a high level of internet skill can be gained by analysing self-perceived skill levels by a range of demographic and socioeconomic factors.

Figure 22 shows that males are more likely to report a high level of internet skill than females, with approximately 43 per cent of males reporting having above average skill levels, compared with 30 per cent of females.

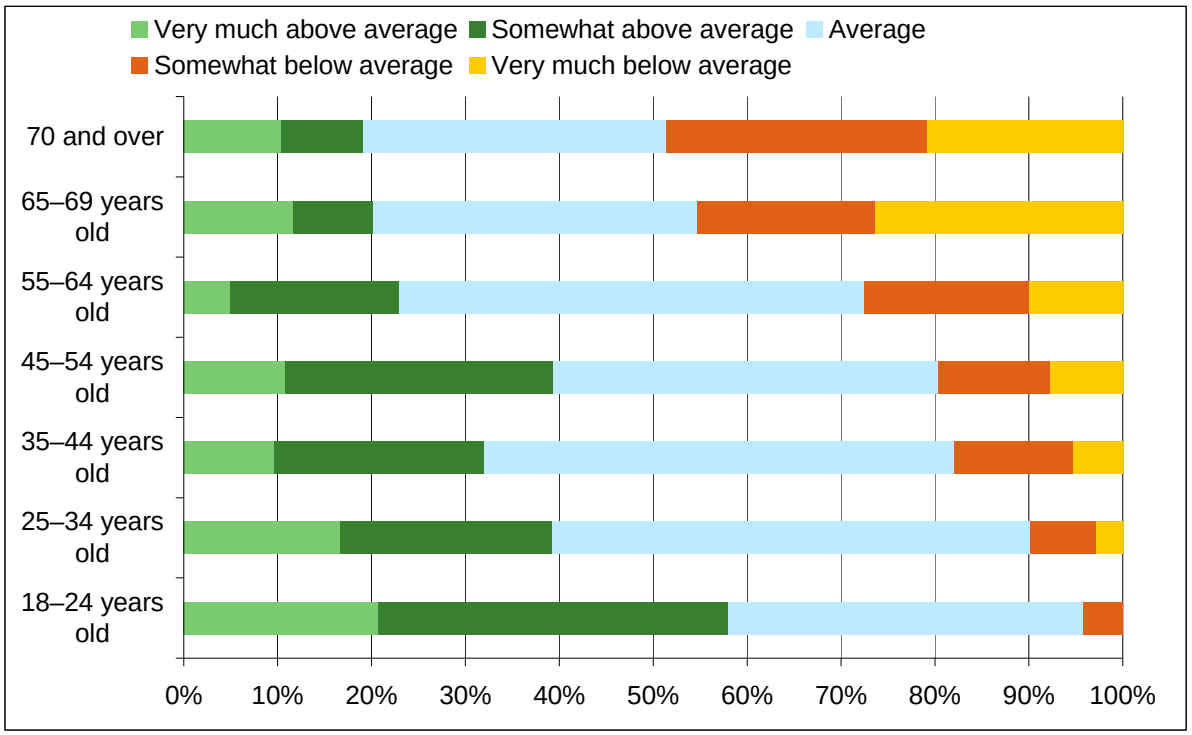
Figure 22. Self-assessed internet skill level, by gender



Source: ACMA-commissioned consumer survey, May–June 2008, internet users aged 18+, (n = 1340).

Age is also a significant factor in shaping self-perception of internet skill level, with younger people having higher self-reported levels of skill (Figure 23). Fifty-eight per cent of 18 to 24-year-olds reported having above average skills and only 4 per cent of 18 to 24-year-olds reported having somewhat below average skills.

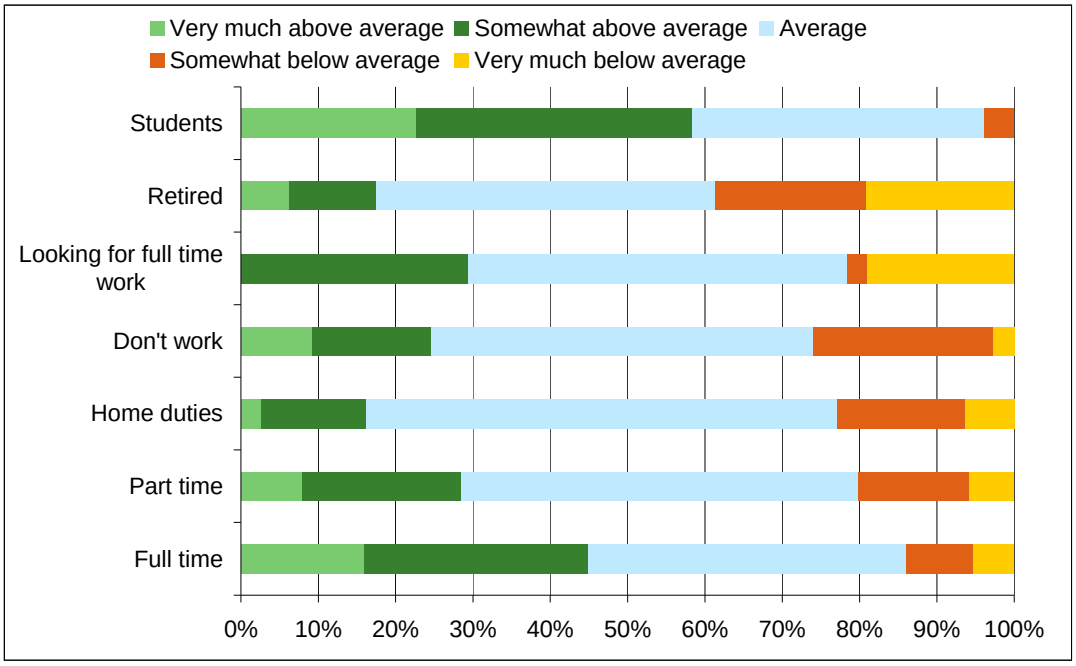
Figure 23. Self-assessed skill level by age



Source: ACMA-commissioned consumer survey, May–June 2008, internet users aged 18+, (n = 1263).

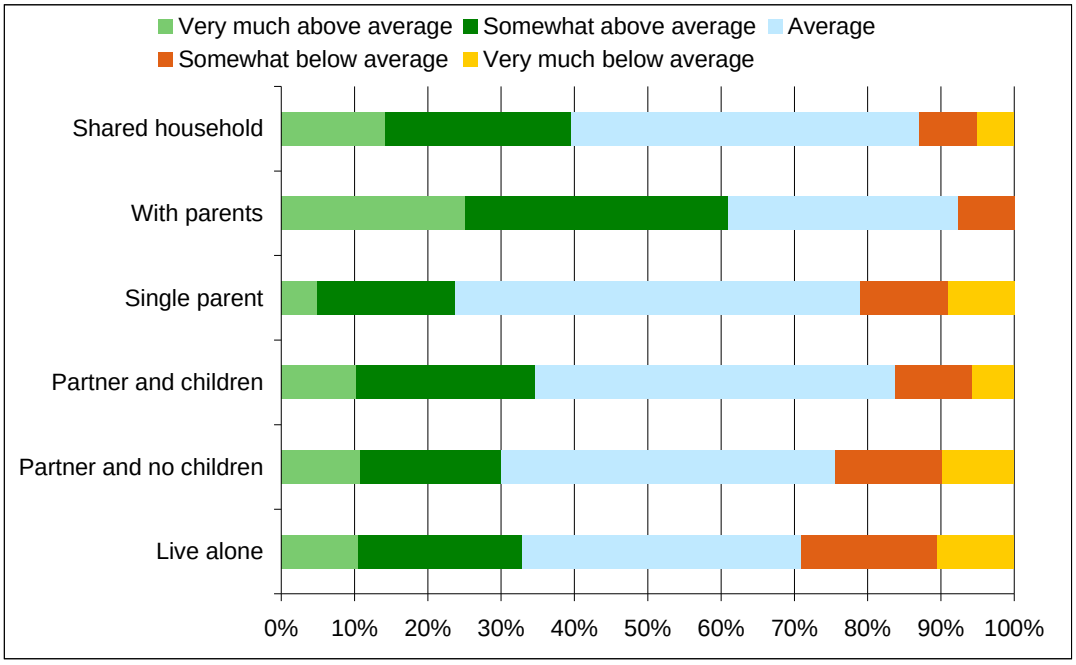
The relationship between self-assessed skill level and work status is less clear. Figure 24 shows that students were more likely to rate their internet skills levels as average or above average. Similarly, it is not clear that household structure plays a major influence on skill levels, as shown in Figure 25. Internet users who live with their parents are more likely to rate their skills as above average. Given that adults who live at home are likely to be younger adults, this suggests that age is an important factor.

Figure 24. Self-assessed skill level, by work status



Source: ACMA-commissioned consumer survey, May–June 2008, internet users aged 18+, (n = 1335).

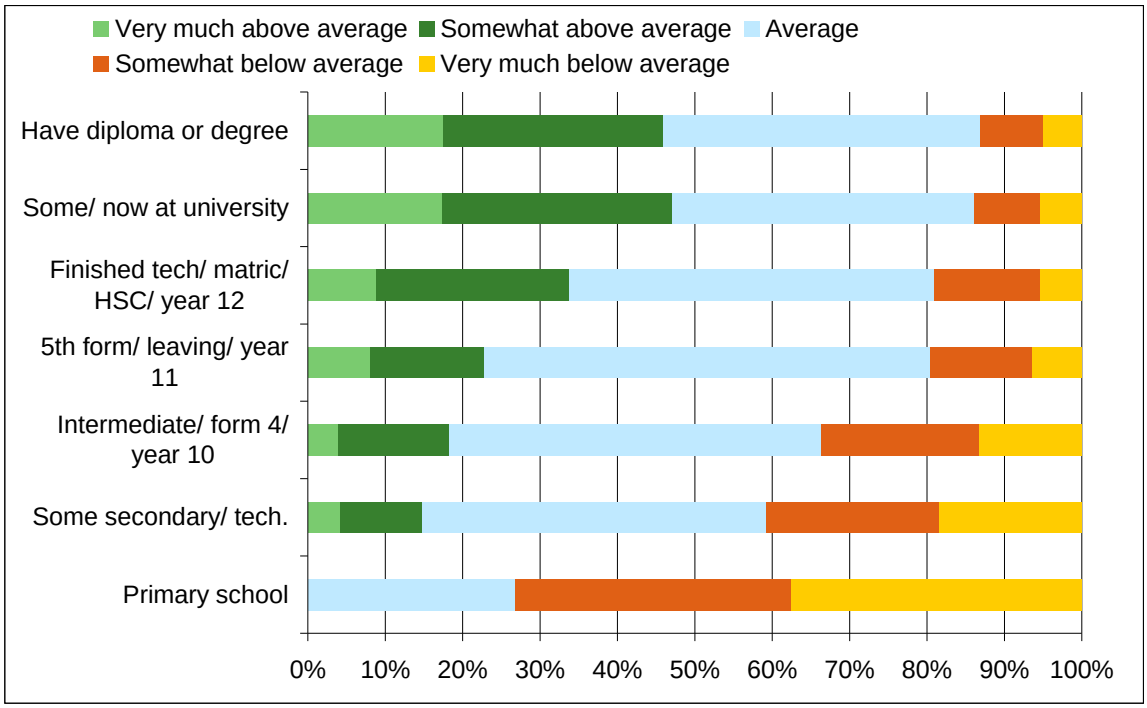
Figure 25. Self-assessed skill level, by household structure



Source: ACMA-commissioned consumer survey, May–June 2008, internet users aged 18+, (n = 1322).

The link between education level and self-assessed skill level is demonstrated in Figure 26. Those stating primary school as their highest level of education obtained are more likely to rate their internet skill level as below average.

Figure 26. Self-assessed skill level, by level of education

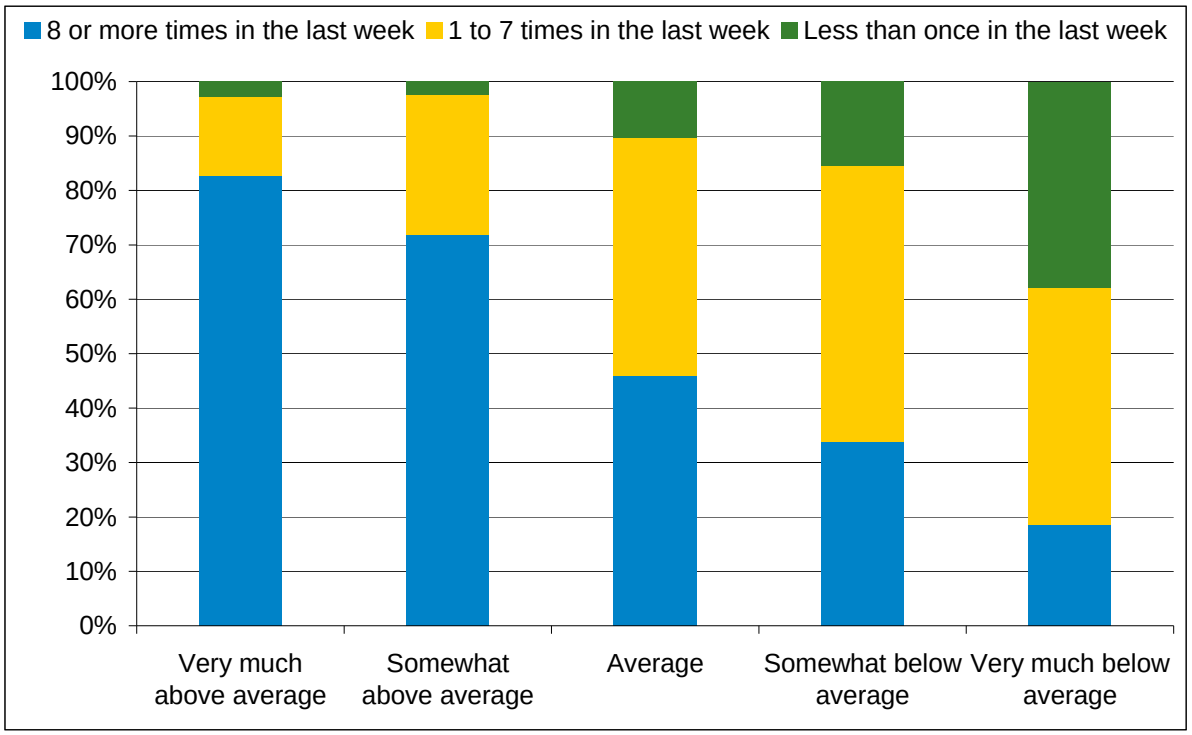


Note: Figures 24, 25 and 26 excludes respondent category 'cannot say'.

Source: ACMA-commissioned consumer survey, May–June 2008, internet users aged 18+, (n =1307).

A strong relationship appears between perceived level of skill and frequency of use (see Figure 27): the more frequently an individual uses the internet, the greater the individual's perceived level of skill. Eighty-three per cent of people self-assessing their internet skill level as very much above average were heavier users of the internet (i.e. using the internet eight or more times in the last week) compared with 72 per cent of people identifying their skills levels as somewhat above average, 46 per cent as average, 34 per cent as somewhat below average and 19 per cent as very much below average.

Figure 27. Level of competency, by frequency of use

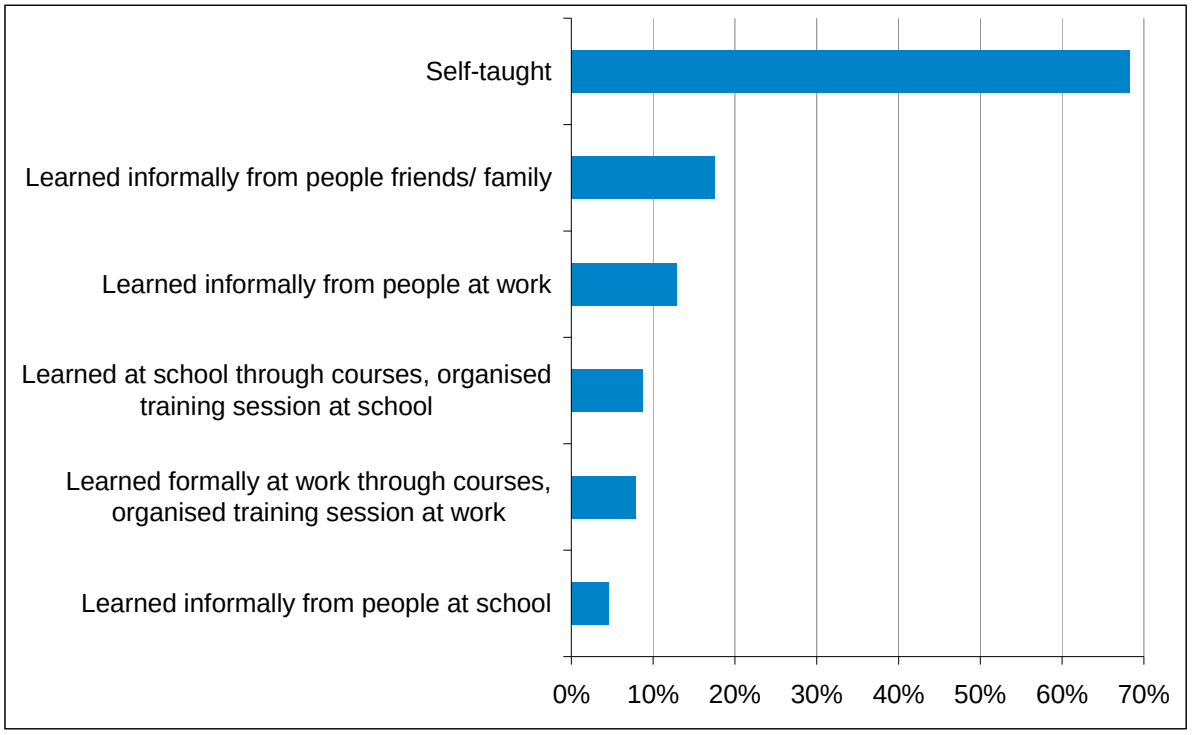


Note: excludes respondent category 'cannot say'.

Source: ACMA-commissioned consumer survey, May–June 2008, internet users aged 18+, (n = 1326).

While 81 per cent of internet users perceive their internet skills as being average or above average, the majority of survey respondents reported use of informal information methods when learning about the internet. Just over 68 per cent of people are self-taught, and less than 18 per cent of people received formal training. This is consistent with findings shown in Figure 28 of the informal nature of consumers' online education. Internet users explore the internet and hone their skills through frequency of use rather than through recognized avenues of training such as formal courses.

Figure 28. Source of training about the internet

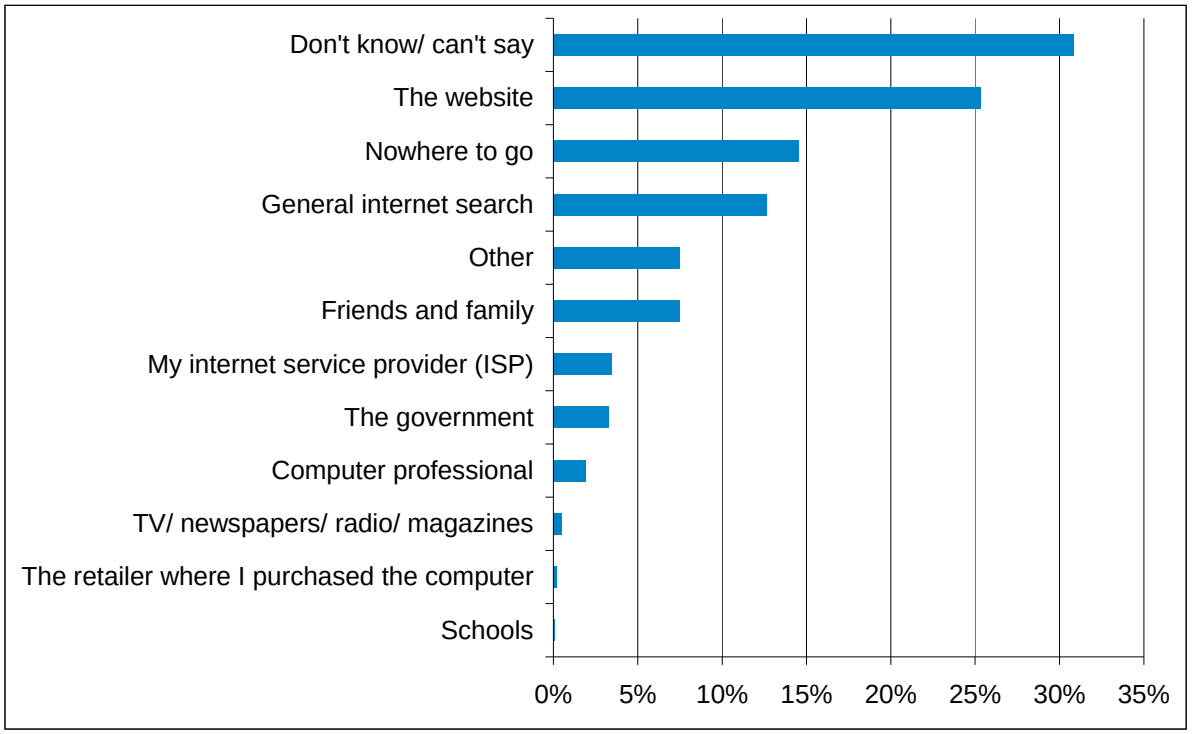


Note: Excludes respondent category 'cannot say'.

Source: ACMA-commissioned consumer survey, May–June 2008, internet users aged 18+, (n = 1324).

The source of people's online security and privacy information is critical to their staying in touch with online security developments. Just over 25 per cent of consumers source information on security for use on social networking websites from the websites themselves, and just fewer than 15 per cent responded that there is nowhere to go for this information (Figure 29). A further 31 per cent reported that they did not know where this information could be obtained.

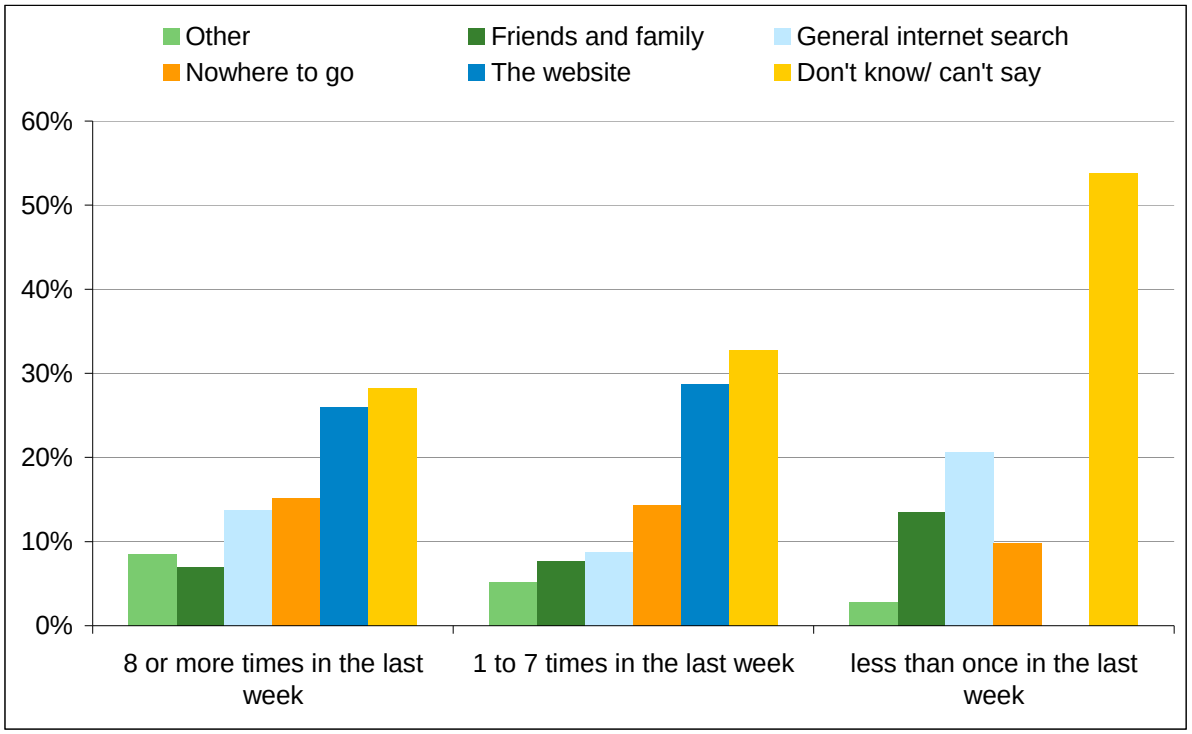
Figure 29. Source of security information when social networking



Source: ACMA-commissioned consumer survey, May–June 2008, social networkers aged 18+, (n = 450).

Figure 30 shows those who use the internet more frequently once again appear to be more security-aware with this group having the lowest proportion of respondents reporting that they don't know where to go for security information relating to social networking sites. However, 28 per cent of users who use the internet more than 8 times a week and who access social networking sites either do not know or cannot say where to access security information about social networking sites, and 26 per cent cite the social networking site itself as the source of their security information regarding social networking sites.

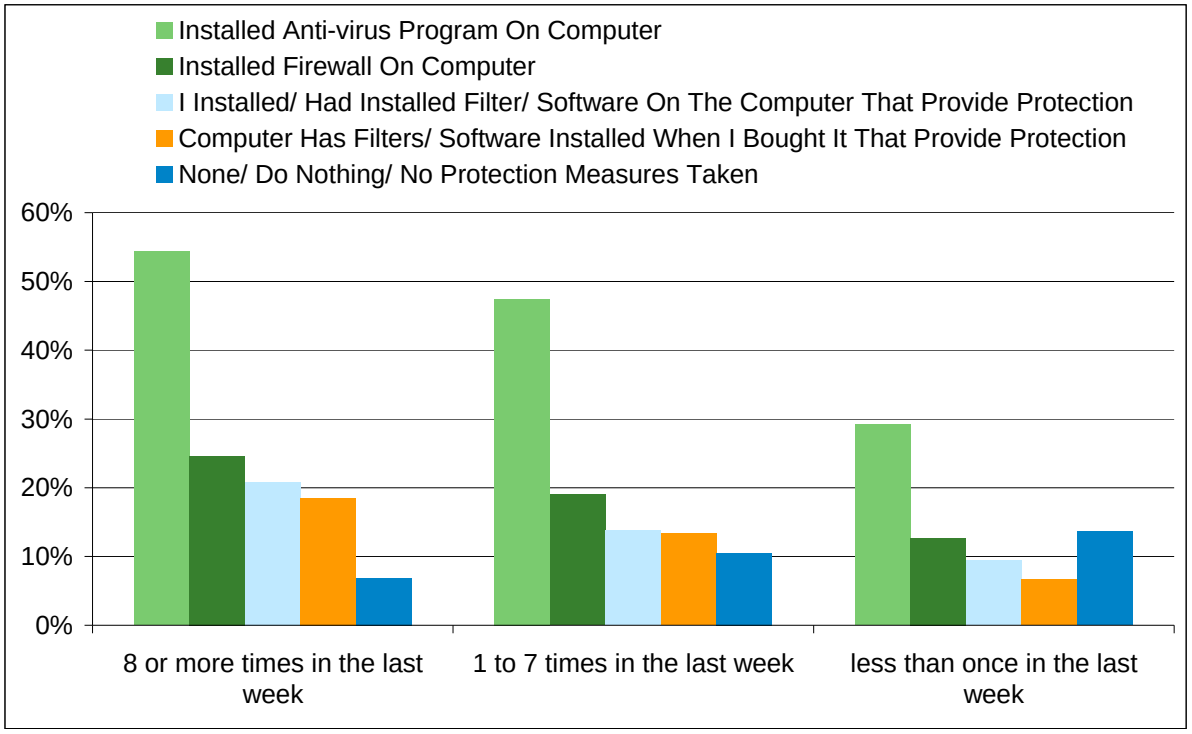
Figure 30. Top five sources of security information when social networking by frequency of internet use



Source: ACMA-commissioned consumer survey, May–June 2008, social networkers aged 18+, (n = 450).

There is a clear relationship between measures taken to mitigate against online risks and frequency of use (Figure 31). Of the consumers using the internet eight or more times in the previous week, 54 per cent reported installing anti-virus software on their computer, compared with 29 per cent of infrequent users (using the internet less than once in the last week).

Figure 31. Measures against online risks and dangers by frequency of internet use



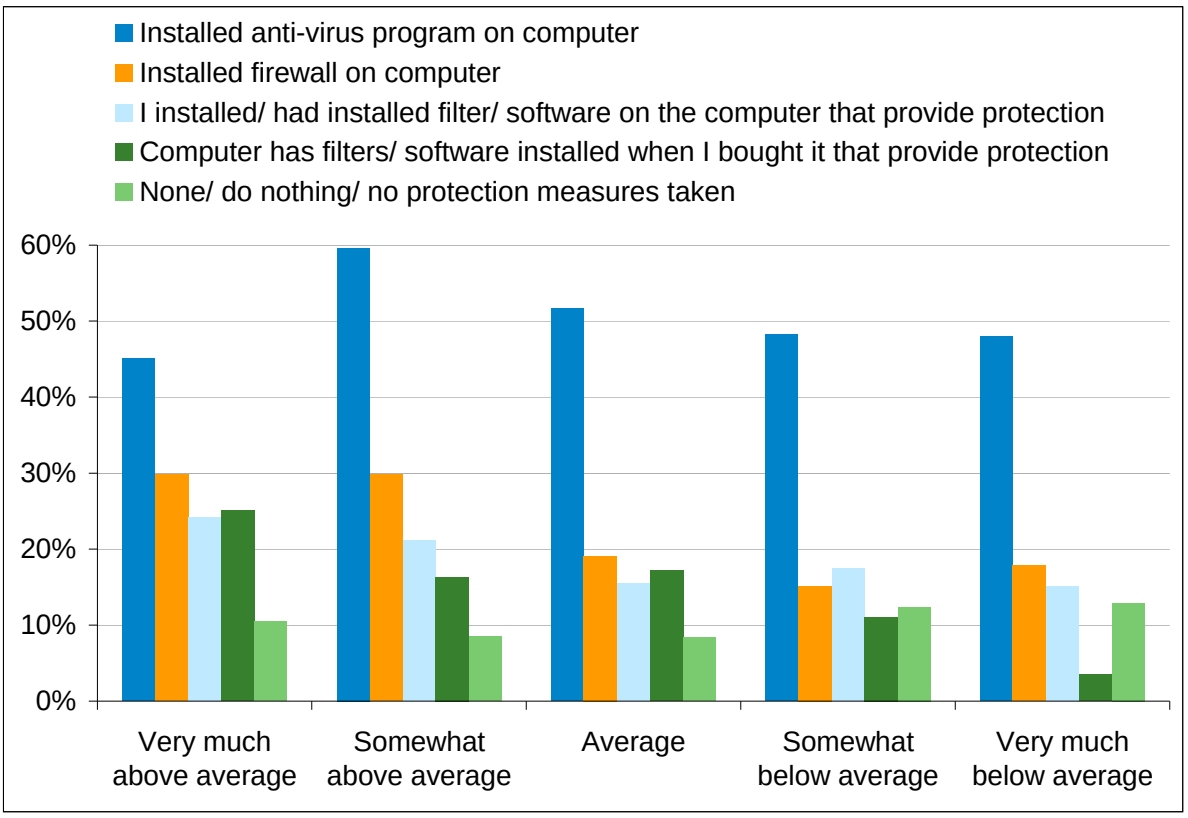
Note: excludes respondent category 'cannot say'.

Source: ACMA-commissioned consumer survey, May–June 2008, internet users aged 18+, (n = 1346).

6.2 Confidence and competency

Internet users who assess their online skills as very much above average are not proactive when protecting their computers against viruses and malicious software. Figure 32 shows that only 45 per cent of those who assessed their online skills as being very much above average installed anti-virus software on their computer (below the responses for other skill levels), 30 per cent installed a firewall themselves, 24 per cent either installed filter or protective software themselves or relied on third parties to install filter or protective software on their computer, just over 25 per cent relied on pre-existing filter software from the place where their computer was purchased and 11 per cent did not take any protective measures at all.

Figure 32. Top five measures against online risks and dangers, by self-assessed skill level



Note: excludes respondent category 'cannot say'.

Source: ACMA-commissioned consumer survey, May–June 2008, internet users aged 18+, (n = 1263).

Once again, this can be linked with the information channels used for education about the internet. While frequent internet users develop their knowledge through trial and error, it appears that a large number are not aware about the dangers that online threats can pose or do not consider themselves at risk from those dangers.

7. Conclusion

Australians' perceptions of the internet, whilst varying with age and education levels, are overwhelmingly positive. Many Australians, particularly those aged under 30 years, consider the internet to be essential to their lives.

While many consumers engage in a wide range of activities online, the majority are concerned with their online privacy and security.

There is also a contradiction in user attitudes expressed about the level of trust in the online environment; concerns expressed about privacy and e-security; and whether the concern leads to action taken by users to minimise the likelihood of their privacy or security being breached.

Many of those with an internet connection at home are relying on minimal practices to secure their information and protect their computers from malicious risks, in part believing that online fraud or identity theft simply will not happen to them. On the available evidence, it appears that this attitude is associated with perceived level of skill and source of internet training.

High levels of skill, whether actual or self-assessed, do not necessarily translate to taking proactive measures to safeguard home computers or personal information. The informal nature of internet education and skill development may reinforce this lack of concern for, or awareness of, the risks of internet use.

With a majority of Australians learning their internet skills through informal channels, there is significant potential for internet users to lack information or underestimate internet risks, further reinforcing complacency.

In order for consumers to continue to trust the internet and to ensure the growth of the digital economy, consumers need to be informed about online risks and ways to protect their computers and themselves from the more negative and harmful aspects associated with internet usage.

There is a critical role for industry and governments in the continuing improvement of consumer awareness. This will include ensuring that internet users are more aware of the online risks and dangers they face and are able to identify appropriate sources of information and training about how to protect themselves online, which can be complemented with informal training.

There is also a critical role for industry and governments to ensure consumers are able to technically address these issues, including changing online behaviours. The key to building online trust and assurance is through embedding this knowledge in the education of current and future internet users. The research presented in this report will facilitate this by helping to raise awareness and inform the targeting of educational campaigns to the varied communities which comprise Australia's online population.