
# Surfing on Thin Ice:

## Consumers and Malware, Adware, Spam & Phishing

**A consumer research report by the Consumers' Telecommunications Network**

**November 2006**

**Acknowledgements**

This research was funded by a grant from the Telstra Consumer Consultative Council.

The Consumers' Telecommunications Network's representation of consumers' interests in relation to telecommunications issues is supported by the Commonwealth through the 'Grants to fund Telecommunications Consumer Representations' program of the Department of Communications, Information Technology and the Arts.

Ryan Sengara, CTN's Project Officer, was primary author and researcher, and was assisted by Teresa Corbin, CTN's Executive Director, Sarah Wilson, CTN's Policy Advisor, and Annie McCall, CTN's Information Officer.

CTN would like to acknowledge the contributions made by its Council members and their organisations in developing and advertising the survey and report: Robin Wilkinson (Tasmanians with Disabilities), CTN Chairperson, Stephen Gleeson (Community Information Strategies Australia Inc.), Jack Crosby, Myra Pincott (Country Women's' Association Australia), Nan Bosler (Australian Seniors Computer Clubs Association), Len Bytheway, Ross Kelso (Internet Society of Australia), Maureen Le Blanc (Australian Council of Social Services), Darrell McCarthy (Better Hearing Australia), and Nicholas Agocs (Ethnic Communities Council of WA). Likewise, we would like to thank members of the Telstra Consumer Consultative Council for their assistance developing and advertising the survey.

We would like to thank CTN members and other consumers who completed the survey, and also thank the groups that advertised it through their networks, including the Australian Consumers' Association, TEDICORE, Consumer's Federation of Australia, National Council of Women Australia, Australian Financial Counselling and Credit Reform Association, NetAlert, the Australian Competition and Consumer Commission's ScamWatch, the Australian Communications Industry Forum's Consumer Council, and Telstra Consumer Affairs.

**Enquiries**

Phone: +61 (02) 9572 6007
E-mail: ctn@ctn.org.au
Website: www.ctn.org.au
Unit 2, 524-532 Parramatta Road
Petersham, NSW 2049 Australia

# Consumers' Telecommunications Network

# Consumers and Malware, Adware, Spam & Phishing

# November 2006

## Table of Contents

# Introduction

## About CTN

The Consumers' Telecommunications Network (CTN) is a national peak body of organisations and of individuals representing community interests in developing national telecommunications policy. We advocate policies for better access, quality of service and affordability of telecommunications for all residential consumers. Our members represent rural and remote consumers, people with disabilities, Deaf consumers, Aboriginal and Torres Strait Islander peoples, low income consumers, consumers from non-English speaking backgrounds, young people, women, pensioners, superannuants and consumers in general. E-security is among CTN's top issues for 2006-2007, as identified by our Board, and in October 2006 CTN became a partner in the Australasian Consumer Fraud Taskforce.

## Background

### What is malware, adware, Spam and phishing?

Malware, adware, Spam and phishing are among the many e-security threats currently facing Australian consumers. Malware can be described as software designed to infiltrate or harm a computer system, often without the owner's knowledge, and can include spyware[1], computer viruses[2], trojan horses[3], worms[4], and fraudulent diallers[5]. Malware may also be used to gain remote control over computers, potentially for illegal purposes, becoming "botnet" or "zombie" computers[6]. Adware[7] can be described as software designed to deliver advertisements to consumers or collect information about a consumers' use of a website. Spam[8] is described by the Government as unsolicited commercial electronic messages. Phishing[9] can be described as techniques used to gain personal information for purposes of identity theft, usually using fraudulent e-mail. Through technical, financial and other means, malware, adware, Spam and phishing all have the ability to directly affect the quality, accessibility, and affordability of Internet access[10] for Australian residential consumers.

### Consumer challenges and concerns

With Australians accessing the Internet in growing numbers[11], e-security has become a major concern for residential telecommunications consumers[12]. The most popular computer programs are vulnerable to attack[13], as are new types of online services and technologies[14]. Even security products themselves, designed to protect consumers from threats, are not always effective and are vulnerable to attacks[15]. What's more, e-security threats are constantly evolving[16], and form only part of a wider set of concerns around the use of the Internet, including privacy, child protection and online transactions[17].

Furthermore, the accessibility and reliability of information available to consumers about e-security can be questioned. First, there are no universally accepted definitions of security threats, and the terminology and concepts used to describe them can be confusing[18]. Second, with the size of the Internet security market reaching billions of dollars[19], there is room for commercial agendas to impact the way information is presented. Third, sources of information that may be considered 'independent', such as government agencies and community groups, may face challenges to reaching the wider public with campaigns.

**Australian consumer safeguards, consumer education and reporting**

In 2003, the Australian Government passed the Spam Act[20], which prohibited the sending of Spam via email, short message service (SMS), multimedia message service (MMS) or instant messaging. The Australian Communications and Media Authority (ACMA) is responsible for the enforcement of the Act. In 2006 ACMA released the SpamMATTERS system, a plug-in for e-mail programs and an online form[21] that can be used to report Spam to the Government.

In March 2005 the Government announced results of a review of spyware, concluding that the most dangerous forms of spyware were already covered by existing legislation, specifically the Criminal Code Act 1995 (Cth), the Trade Practices Act 1974 (Cth), the Australian Securities and Investments Commission Act 2001 (Cth) and Corporations Act 2001 (Cth), the Privacy Act 1988 (Cth), the Criminal Law Consolidation Act 1935 (SA), the Telecommunications Act 1997 (Cth), and the Telecommunications (Interception) Act 1979 (Cth)[22].

In May 2006 the Government announced that it was supporting the Australian Direct Marketing Association (ADMA) and the Internet Industry Association (IIA) to collaborate to develop industry guidelines for online marketers and website operators for the use of adware[23]. At the time of publication of this report, no guidelines had been announced.

In terms of consumer reporting, ACMA's SpamMATTERS and the Australian Competition and Consumer Commission's Scamwatch program[24] both provide reporting facilities. AusCERT[25], the national Computer Emergency Response Team run out of the University of Queensland, also has a reporting facility for "computer security incidents", and the Australian Federal Police's High Tech Crime Centre[26] provides a reporting facility for online crime.

In terms of consumer education, commercial companies provide a range of information to consumers, including security alerts, online glossaries and encyclopaedias. All of the aforementioned government agencies provide information on e-security, as does NetAlert[27], Australia's Internet safety advisory body. In late October 2006, as this report was being

finalised, the Commonwealth's Department of Communications, Information Technology and the Arts (DCITA) launched www.staysmartonline.gov.au[28], which aims to provide information to home users and small businesses on securing a computer, on smart transacting online, and on kids safety online.

**Recent research**

Aside from a steady stream of media articles covering online security, we uncovered only two recent research reports focusing specifically on Australian residential consumers' experiences with online security. DCITA has published *Trust and Growth in the Online Environment*[29], and *Exploration of Future Electronic Payment Markets*[30]. Both touch upon online security in the context of supporting consumer confidence to conduct online transactions, and the former report found that computer viruses and Spam were the most common threats faced by consumers, but that most consumers did not take many measures to protect against them.

## Aims

If consumers are encouraged, and even expected to complete important transactions or access important information online, basic consumer rights[31] must be met to ensure the accessibility, affordability and quality of online services. This CTN research aims to investigate residential consumers' experiences with e-security and to identify areas of concern and their implications on telecommunications policy and regulation in Australia. The research explores:

1. The awareness, knowledge, personal experience and opinions of consumers with malware, adware, Spam and phishing.
2. The sources of information consumers use to learn about e-security issues and their opinions on accessibility and reliability of these sources.
3. The awareness, knowledge, personal experience and opinions of consumers with the measures they can take to guard against e-security threats.
4. The impact of security threats on consumer use of the Internet and other technologies.
5. What consumers want done to improve their e-security.

## Methodology

After conducting a literature review we constructed a survey of 42 multiple choice and free-answer questions. The survey was conducted online through our website and was promoted to our members and other consumers through a range of groups (see *Acknowledgements*). The survey ran from 29 June to 31 July 2006. The total sample size is 254.

Consumers were directed to answer most questions based on their 'personal' online use, which we defined as anything done online not related to their work. When determining the personal vulnerability of consumers to e-security threats, questions concentrated on family computers or computers personally owned, leased or rented. Upon completion of the survey, consumers were directed to educational resources related to the topics covered (see *Appendix*). A limitation of the survey tool we used was that it was non-relational – for example, we were unable to isolate results based on a consumers' answer to a particular question.

We believe the sample offers a fair representation of a wider base of Australian consumers (see *Demographics*). However, CTN is not presenting this as strict quantitative research. Based on an exploratory survey, and supplemented with an on-going literature review, the report offers qualitative insights – a snapshot of consumers' experiences and opinions on areas of e-security that are constantly evolving. Further research across a range of consumer groups is needed (see *Recommendations*). Industry, regulators and government also need to consult widely with consumers about e-security on an on-going basis.

In the *Survey Results* section, data is presented in graphical form, summarised in text and commented on. The comments highlight specific data, identify themes and pull in relevant external information. Analysis is supplemented with direct quotes from consumers' responses .

# Executive Summary

This research investigates Australian residential consumers' experiences with e-security and identifies areas of concern and their implications on telecommunications policy and regulation. Findings and recommendations have been formed through a literature review and an online survey of 254 Australian consumers. In age, gender and location, the collection of consumers we surveyed reasonably represents a wider group of Australian consumers. However, the majority of consumers we surveyed were frequently online, and active once online, and results may therefore not adequately represent consumers who are rarely online.

In summary, though a minority of Australian consumers may be suffering financially as a result of e-security problems, many more may be suffering productivity-wise, and stopping or changing the way they use the Internet because of e-security concerns. Furthermore, though awareness of e-security threats may be reasonably high, consumer understanding of these threats and how to protect themselves against them may be lacking. Consumers we surveyed looked to Internet Service Providers, Government and fellow consumers to take more responsibility for e-security. With the potential for many consumers to be "surfing on thin ice", our recommendations include development of consumer protections, development of consumer education, and further research around e-security issues.

## Key Findings

F1. **The strong majority of consumers had experienced many e-security threats despite using a range of security products and despite current consumer protections.**

- More than 4 out of every 5 consumers we surveyed had experienced Spam.
- Approximately 2 in every 3 consumers we surveyed had experienced computer viruses or spyware.
- More than 1 in every 3 consumers we surveyed had experienced adware, trojan horses, phishing or worms.
- 2 in every 3 consumers we surveyed had used anti-virus software, firewall software, software updates, or anti-spyware software.

F2. **A small but significant proportion of consumers suffered financially, but many more suffered from a loss of productivity and had changed how they used the Internet because of security problems and concerns.**

- More than 1 in every 10 consumers we surveyed had experienced unexpectedly high bills or financial loss as a result of online security problems.
- Many consumers we surveyed commented on the loss of time and frustration they experienced when dealing with e-security problems.
- More than 1 in every 3 consumers we surveyed had stopped or changed the way they made online purchases, paid bills online, or used online banking because of online security concerns.

F3. **Consumer awareness of security threats was reasonable, but understanding and confidence to identify and guard against security threats was a concern.**

- Almost 9 out of every 10 consumers we surveyed answered that they were aware of and understood Spam and computer viruses, and more than 2 out of every 3 answered that they were aware of and understood spyware and adware.
- However, more than 1 in every 4 consumers we surveyed had either never heard of phishing, adware, worms, trojan horses or diallers, did not fully understand how they worked, or did not fully understand how they might get them.
- More than 1 in every 2 consumers we surveyed were less than confident they could successfully identify malware, adware, Spam or phishing.
- Almost 1 in every 3 consumers we surveyed rated their understanding of how security products protected them as less than good.
- Approximately 1 in every 3 consumers we surveyed had used security products installed by someone else, and many indicated that they relied on products or other people to manage their e-security.

F4. **A small proportion of consumers were mishandling Spam and phishing attacks.**

- The majority of consumers we surveyed had recognised and ignored phishing e-mails, but more than 1 in every 20 had been confused by a phishing e-mail, or had visited the websites they were asked to by a phishing e-mail.
- The majority of consumers we surveyed had deleted Spam without investigating it further, but more than 1 in every 4 had read or tried to unsubscribe from Spam, and 1 in every 20 had replied to it.

F5. **Use of independent sources of information on e-security was low, and many consumers questioned the reliability and accessibility of information they had used.**

- Less than 1 in every 4 consumers we surveyed had used Government information on e-security, while most used security software companies and the media.
- More than 1 in every 2 consumers we surveyed did not fully trust the sources of information they used, and many raised concerns over the availability and complexity of the information they used.

F6. **Most consumers wanted Internet Service Providers, Government and fellow consumers to take more responsibility to improve e-security.**

- More than 4 out of every 5 consumers we surveyed thought Internet Service Providers should take more responsibility to provide better security online for consumers.
- 2 out of every 3 consumers we surveyed thought Government should take more responsibility to provide better security online.
- 2 out of every 3 consumers we surveyed thought consumers themselves should take more responsibility to provide better security online — Approximately 2 out of every 3 consumers we surveyed did not regularly read end-user license agreements, change passwords once every 6 months, switch to more secure software, or read terms and conditions of websites, while only half regularly used web browser security features.

## Recommendations

R1. **Development of consumer protections**:

a. A central, user-friendly, and well-promoted system for consumers to report e-security threats, and for subsequent investigation, encompassing and extending the Australian Communications and Media Authority's SpamMATTERS, the Australian Competition and Consumer Commission's ScamWatch, the Australian Federal Police's High Tech Crime Centre and AusCERT's reporting systems.

b. Test cases, case studies and audits of existing consumer protection legislation to ensure adequate protection from current and emerging e-security threats.

c. Informed consumer consent to the use of adware should be a central principle of Australian Adware guidelines, currently under development by the Internet Industry Association and the Australian Direct Marketing Association.

d. Internet Service providers and software producers should be required to address e-security issues of the products they offer, including providing warnings and consumer education, making software patches available, and providing e-security tools.

e. Action on an international front, possibly forming international information sharing and enforcement arrangements with other governments and agencies, as has been done in the case of Spam.

R2. **Development of consumer education resources:**

a. Up-to-date lists of confirmed e-security threats, especially phishing scams, for consumers to refer to.

b. Using animated demonstrations, real-life examples and plain language to explain how e-security threats work, how to identify them, and how to best deal with them.

c. Using animated demonstrations, real-life examples and plain language, explanations of how e-security products and other e-security measures work, especially in the context of online transactions.

d. Addressing the challenges consumers face maintaining security measures across multiple computers, including work computers.

e. Education resources should be delivered through an independent, central organisation and website – potentially encompassing or extending the NetAlert website or the Stay Safe Online website.

f. Education resources should be widely promoted across all sectors of society, especially to young people, seniors and new computer users.

g. Consumers should be encouraged to take more responsibility for their own e-security by actively accessing information, including www.staysafeonline.gov.au and www.netalert.net.au.

R3. **Further research into consumers and e-security**:

a. The extent of financial loss, emotional distress and productivity loss on consumers as a result of e-security issues – the Productivity Commission may be well-place to conduct such research.

b. The financial capacity of consumers, especially low-income consumers, to effectively protect themselves online, and the viability of subsidised or free e-security products such as e-mail filters.

c. A focus on e-security for consumers under the age of 30.

d. A focus on e-security for consumers who are not regularly online.

e. The most user-friendly ways to present information about online security to beginners, intermediate and advanced computer users of diverse backgrounds.

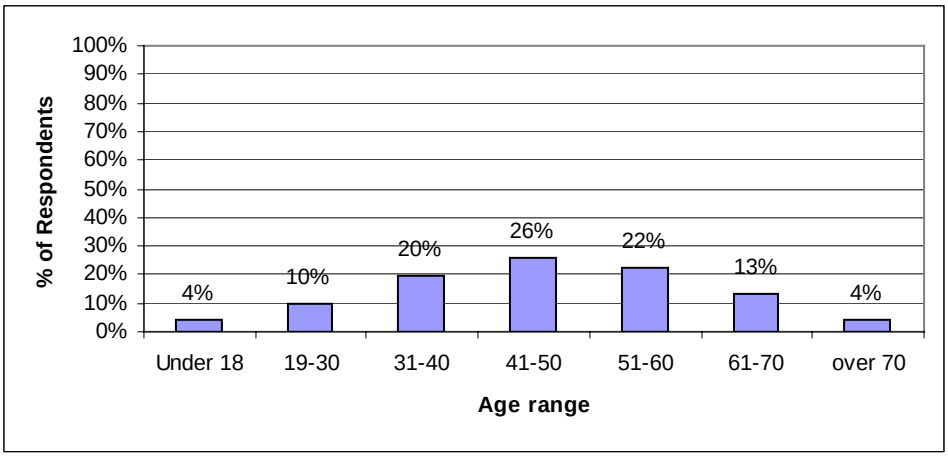
f. The best distribution channels to reach beginners, intermediate and advanced computer users of diverse backgrounds with information about e-security, including point-of-sale information, and computer user and community groups.

g. How the speed of an Internet connection, data download limits, or choice of operating systems may impact a consumer's ability to protect against e-security attacks.

# Data and Analysis

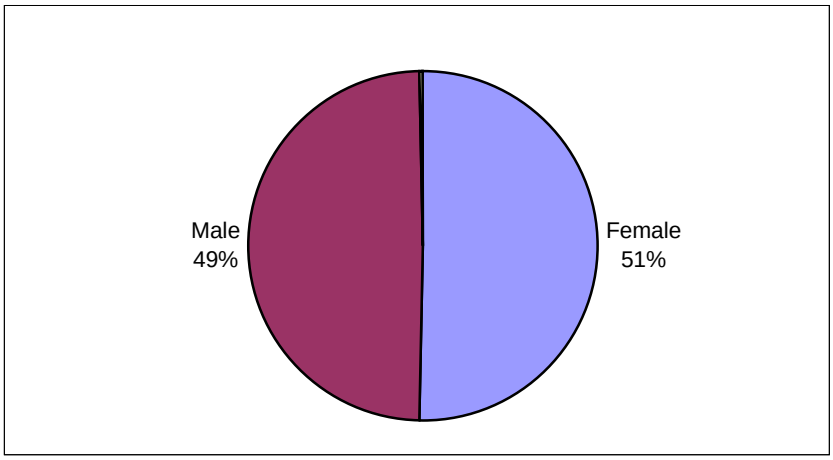
## Demographics

### 1. What is your age range?



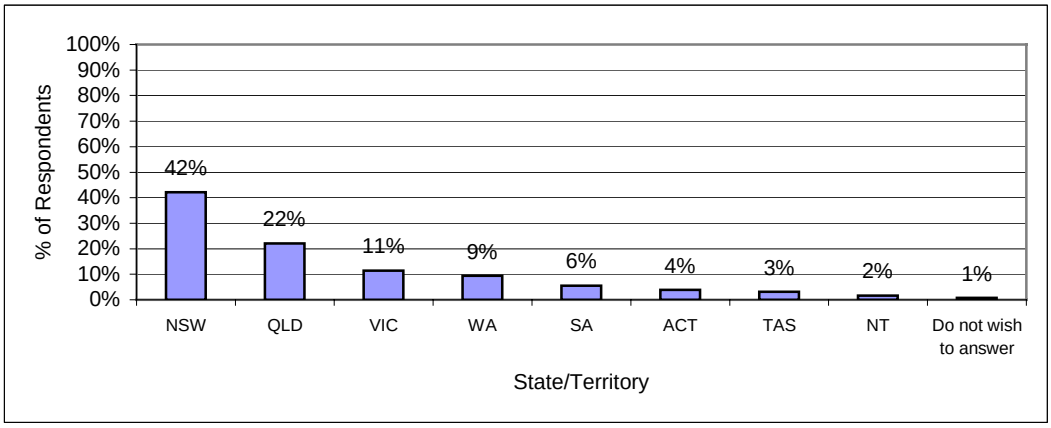

Summary: 4 per cent of consumers surveyed were under the age of 18, 10 per cent between the ages of 19 and 30, 20 per cent between 31 and 40, 26 per cent between 41and 50, 22 per cent between 51 and 60, 13 per cent between 61 and 70, and 4 per cent over 70.

### 2. What is your gender?



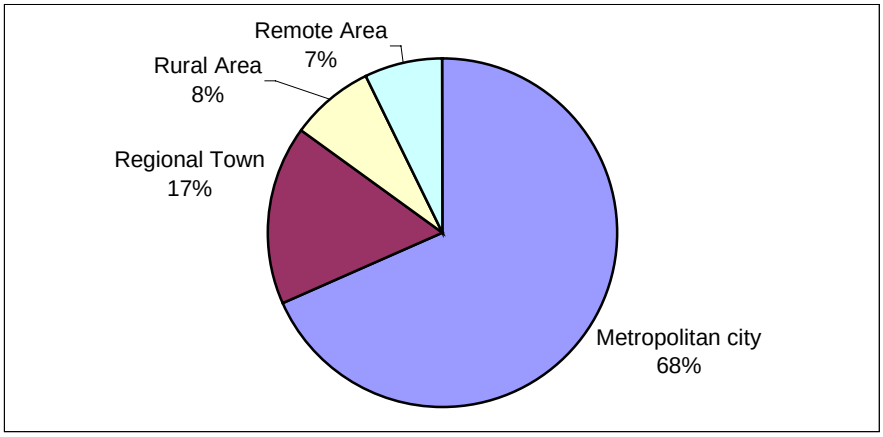

Summary: 51 per cent of consumers surveyed were female and 49 per cent were male.

**3. In which state or territory do you primarily live?**




Summary: 42 per cent of consumers surveyed primarily lived in NSW, 22 per cent in QLD, 11 per cent in VIC, 9 per cent in WA, 6 per cent SA, 4 per cent in the ACT, 3 per cent in TAS, 2 per cent in the NT, and 1 per cent did not wish to answer.

**4. What type of area do you live in?**




Summary: 68 per cent of consumers surveyed lived in a metropolitan city, 17 per cent in a regional town, 8 per cent in a rural area, and 7 per cent in a remote area.

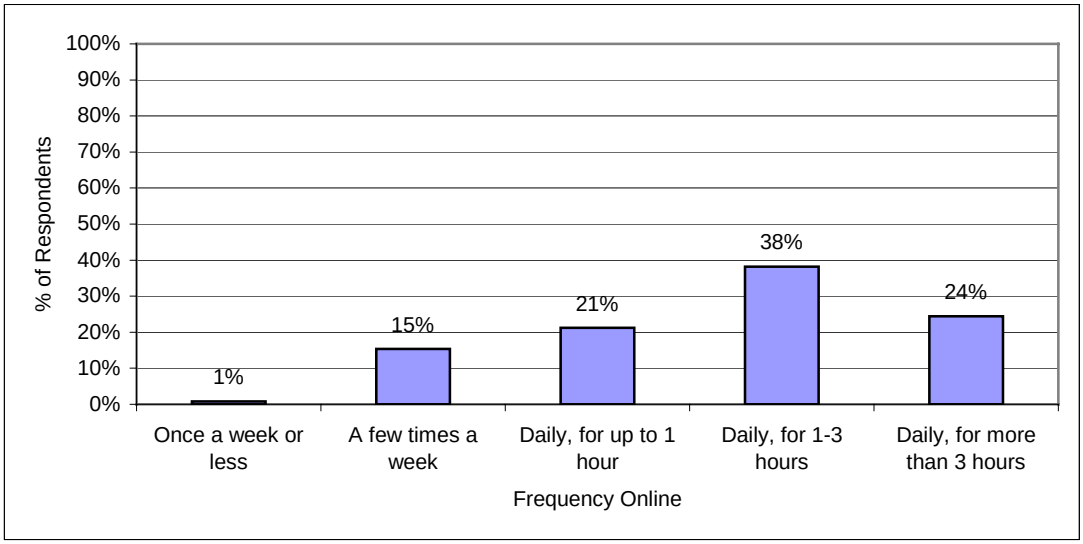
Comments (for 1-4):

This sample of consumers is weighted slightly towards older consumers when compared to the wider Australian population[32]. Considering consumers under 30 years of age may be accessing the Internet more frequently than any other age group in Australian society[33], we believe there is a strong need for specific research on young people and malware, spyware, adware and phishing. The split in gender is in line with national proportions[34].

Consumers from every state and territory are represented in the results, though compared to the wider Australian population[35], there are a larger proportion of consumers from New South Wales and fewer consumers from Victoria. Regional towns may be slightly underrepresented in favour of metropolitan cities and rural/remote areas, but the split in location is nonetheless roughly in line with national figures[36].

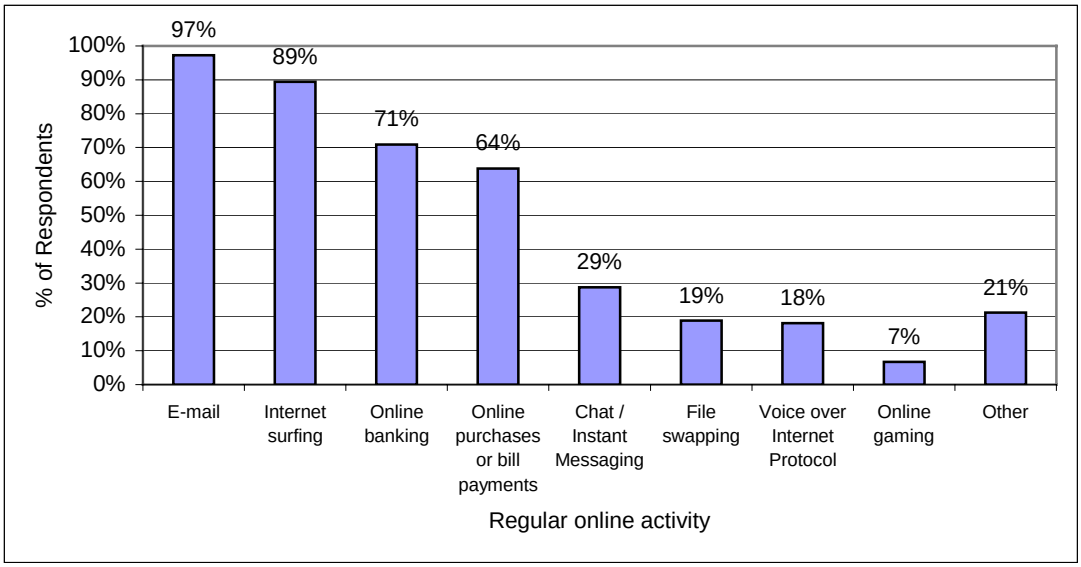
## Going Online

### 5. Approximately how frequently are you online for personal use?




Summary: 1 per cent of consumers surveyed went online for personal use approximately once a week or less, 15 per cent a few times a week, 21 per cent daily for up to 1 hour, 38 per cent daily for 1-3 hours, and 24 per cent daily for more than 3 hours.

### 6. Which of the following do you regularly do while online for personal use?

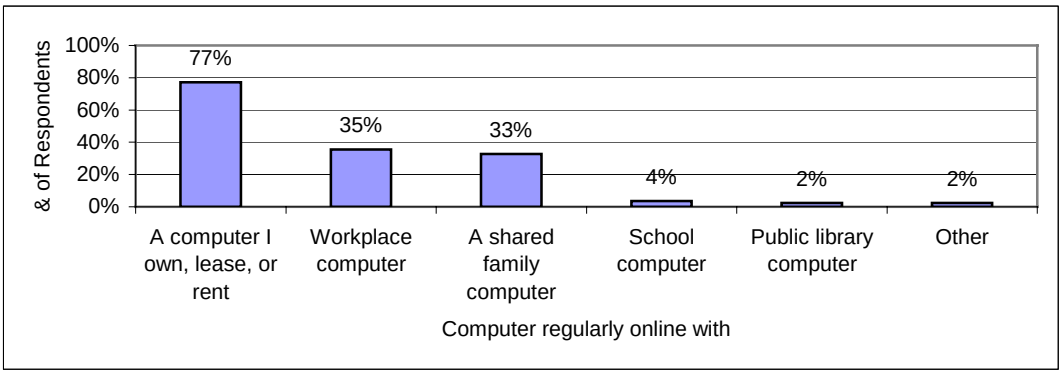



Summary: 97 per cent of consumers surveyed regularly used e-mail while online for personal use, 89 per cent surfed the Internet, 71 per cent used online banking, 64 per cent made online purchases or bill payment, 29 per cent used chat and instant messaging, 19 per cent used file swapping, 18 per cent used Voice over Internet Protocol, 7 per cent used online gaming and 21 per cent did other activities.

Comments for 5 & 6:

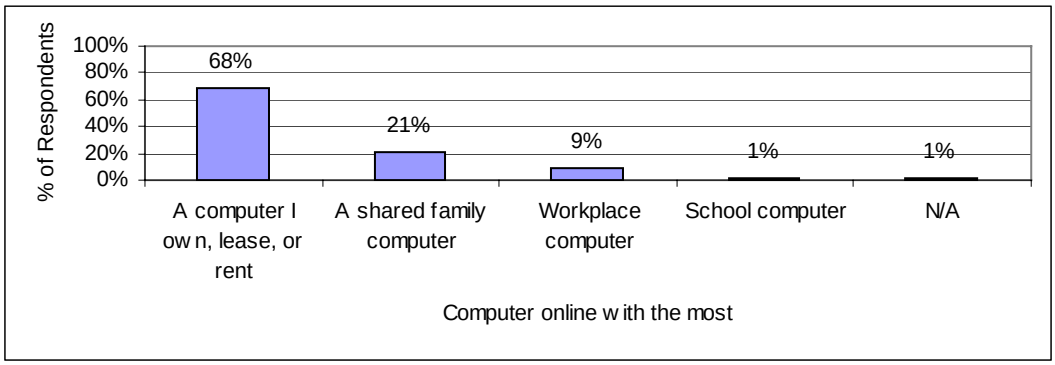
The consumers we surveyed were online frequently and were active once online. 62 per cent were online for personal use for one hour or more every day, and over 60 per cent had made online purchases, paid bills, done banking, surfed the Internet and used e-mail. However, it is unclear just how representative this is of the wider Australian population. Compared to current figures available[1] (the 2006 census may eventually provide more comparable results), consumers we surveyed here were online more frequently than the general population and were more active once online. The results, therefore, may not adequately capture consumers who are either rarely or never online, and hence may understate the overall vulnerability of consumers.

**7. What computers are you regularly online with for personal use?**




Summary: 77 per cent of consumers surveyed were regularly online with a computer they owned, leased or rented, 35 per cent with a workplace computer, 33 per cent with a shared family computer, 4 per cent with a school computer, 2 per cent with a public library computer and 2 per cent with other computers.

**8. What computer are you online with the most for personal use?**




Summary: 68 per cent of consumers surveyed went online the most with a computer they owned leased or rented, 21 per cent with a shared family computers, 9 per cent with a workplace computer, 1 per cent with a school computer and 1 per cent answered Not Applicable (N/A).

Comments for 7 & 8:

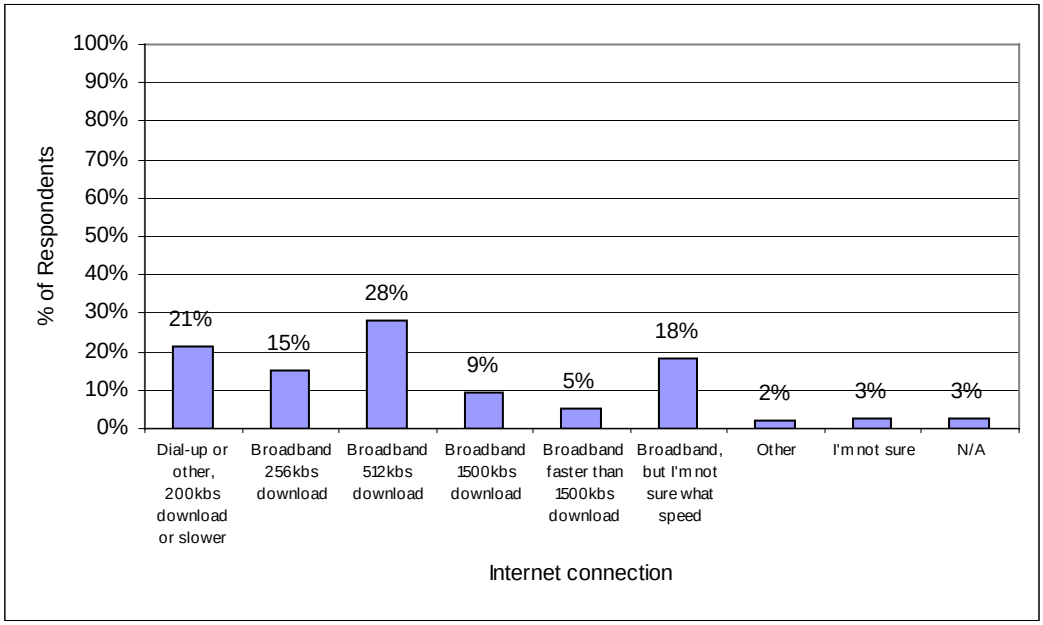
Since most consumers surveyed regularly went online with a computer they owned leased or rented, or a shared family computer, the results highlight the personal financial responsibility many consumers bear for security attacks. Since many consumers also went online for personal use on a workplace or a shared family computer, the results also show that businesses are at risk. Furthermore, since results show that consumers are going online at a range of locations, they may be facing challenges taking consistent security measures across a number of computers – some of which they may own and be responsible for, while others they may not. This finding should be taken into consideration in developing consumer education resources.

Consumer quotes:

*"I had a potentially expensive issue with a trojan virus last year that resulted from poor communication from the IT staff at work which caused a failure in security at home."*

*"It is difficult to keep up to date with best software for…Work or home use."*

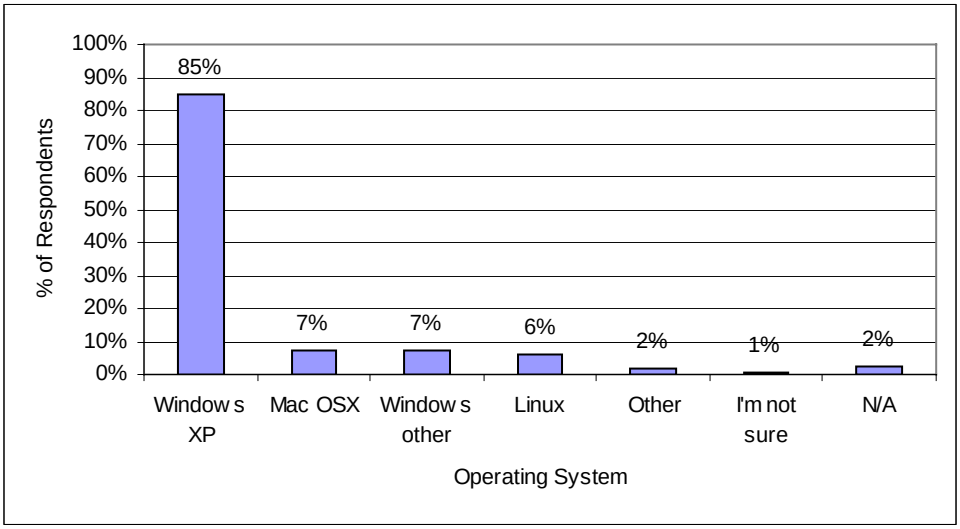
**9. If you go online for personal use with a computer you own/lease/rent, or a shared family computer, what Internet connection(s) do you have?**




Summary: 21 per cent of consumers surveyed had a dial-up or other connection 200kbs download or slower, 15 per cent broadband 256kbs download, 28 per cent 512kbs, 9 per cent 1500kbs, 5 per cent faster than 1500kbs, 18 per cent broadband but unsure what speed, 2 per cent other, 3 per cent not sure and 3 per cent N/A.

Comments: Among those surveyed, there was a mixed bag of Internet service speeds on personal and shared family computers. Most, however, were on connections 512 kilobytes per second (download) or slower. Since software patches are so crucial to online security[37], and some are of a significant size[38], research should look into how the speed of an Internet connection, or data download limits of Internet connections may impact on consumers' ability to protect themselves online.

**10. If you go online for personal use with a computer you own/lease/rent, or a shared family computer, what operating system(s) do you run?**




Summary: 85 per cent of consumers surveyed used Windows XP on a computer they owned/leased/rented or a shared family computer, 7 per cent used other Windows operating systems, 7 per cent Mac OSX, 6 per cent Linux, 2 per cent other, 1 per cent weren't sure and 2 per cent answered N/A.

Comments: The strong majority of consumers surveyed used Windows XP for their personal or family computers, far and above any other operating system. Since Windows XP is a major target of security attacks (see note 13), these results emphasise the high proportion of consumers whose underlying security may be at a high risk. Since many systems come bundled with operating systems and some software can only be run on some operating systems[39], the results may also highlight a lack of adequate or informed consumer choice, especially when buying a new computer – something further research should investigate and education campaigns should address.

Consumer quotes:

*"I strongly recommend to all my friends that they never connect to the Internet from Microsoft Windows unless they have a high-level understanding of how to protect themselves."*

*"…on a previously owned PC we experienced spyware, adware, viruses etc - this contributed to my switch to the MAC OSX platform."*

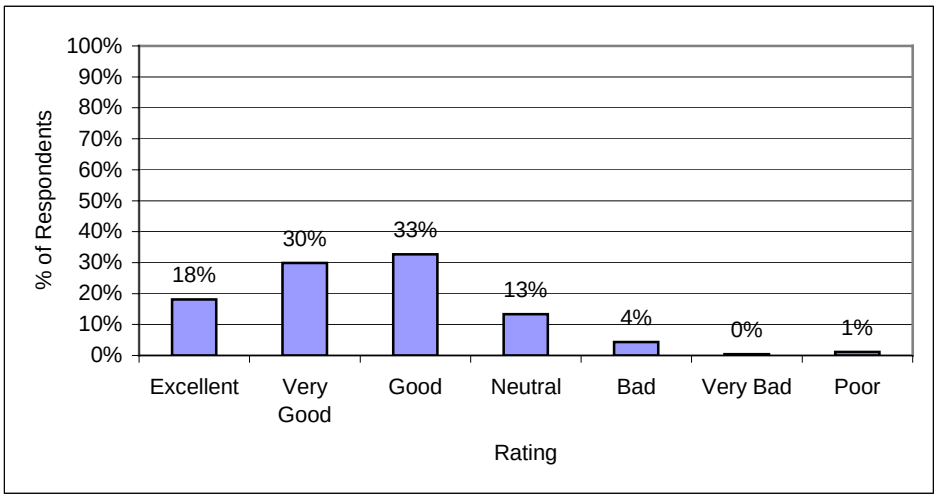
*"I run all my major activity on Linux desktops and servers. I use MS Windows only for trivial activities or necessary software that will only run on Windows."*

*"Microsoft has a lot to answer for. They have distributed a very insecure operating system without educating or alerting their customers to the fact. They also have used their monopoly position to hoodwink people into a "Windows addiction" back with Win 3.1 and 95 (VERY INSECURE) making it very difficult for people to switch to other more secure platforms."*

*"Government, security software companies, and ISPs should play a greater role in educating users about more secure alternatives and the risks that users run by running Windows."*

## Security Threats

**11. On the whole, how would you rate your awareness and understanding of online security threats?**




Summary: 18 per cent of consumers surveyed rated their awareness and understanding of online security threats as 'excellent', 30 per cent as 'very good', 33 per cent as 'good', 13 per cent as 'neutral', 4 per cent as 'bad', 0 per cent as 'very bad', and 1 per cent as 'poor'.

Comments: On the whole, consumers surveyed rated themselves well – 63 per cent "good" or "very good". However, the relatively low number of consumers rating themselves at an "excellent" level of awareness and understanding shows that there may be some doubt in consumers minds over how much they know about the threats they may face. The next question investigates this area further and results may indicate consumers may not be as aware or understand threats as well as they rate themselves to. Importantly, these results highlight the importance of consumer education in e-security. Written comments we received to this question, as well as other questions, show that some consumers may be frustrated with the e-security knowledge of other consumers, alluding to large gaps in know-how among all consumers.

Consumer quotes:

*"It's confusing, but it's a very complicated area. You can't expect most people to understand."*

*"Often don't know if one thing has more than one word to describe it"*

*"Need to know more, but how?"*

*"Have to be so alert to new threats all the time."*

*"I have grave concerns for the uninformed user out there."*

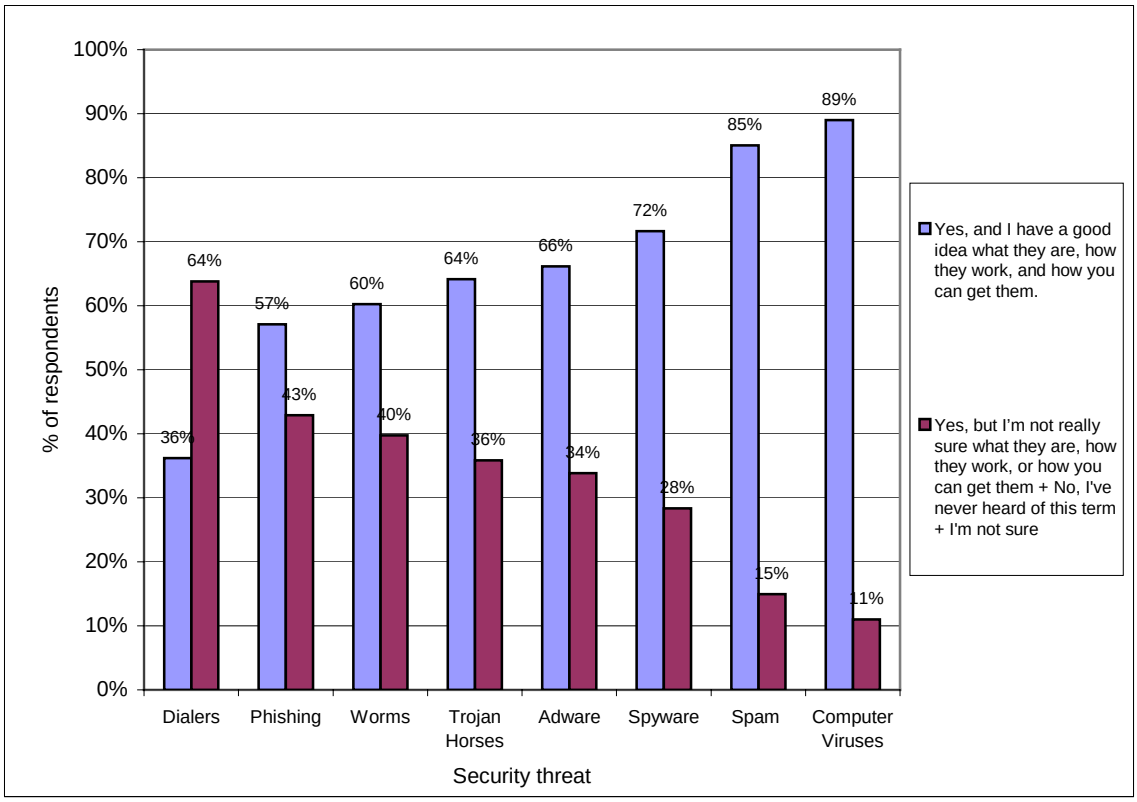
*"Mostly it's just common sense - which seems markedly uncommon to Internet users."*

*"When one experiences things one does not understand - then seek more information…"*

*"I am constantly amazed though, that even given the vast media coverage (sensational or otherwise) regarding threats on the net, gullible people still continue to fall for them."*

**12. Have you heard of "Spyware", "Adware", "Phishing", "Spam", "Computer Viruses", "Trojan horses", "Worms", and "Diallers"?**

| | Diallers | Phishing | Worms | Trojan Horses | Adware | Spyware | Spam | Computer Viruses |
|---|---|---|---|---|---|---|---|---|
| Yes<br>I have a good idea what they are, how they work, and how you can get them | 36% | 57% | 60% | 64% | 66% | 72% | 85% | 89% |
| Yes<br>But I'm not really sure what they are, how they work, or how you can get them | 17% | 24% | 33% | 29% | 20% | 27% | 15% | 11% |
| No<br>I've never heard of this term | 45% | 19% | 6% | 7% | 12% | 1% | 0% | 0% |
| I'm not sure | 2% | 1% | 1% | 0% | 2% | 1% | 0% | 0% |



Comments: On first glance, some of these results are encouraging – almost 9 out of every 10 answered that they were aware of and understood Spam and computer viruses, and more than 2 out of every 3 consumers answered the same for spyware and adware. However, once you look beyond this data to examine the sum of those consumers who did not fully understand these threats, had never heard of them or weren't sure, the results show that a significant proportion of consumers did not have a solid understanding of many of the security threats we listed.

At least 1 out of every 4 consumers surveyed did not fully understand spyware, adware, phishing, trojan horses, worms or diallers. Almost half of consumers surveyed had not heard of diallers, and approximately 1 in 5 had not heard of phishing. Furthermore, written comments highlighted the ever-evolving nature of online nature of threats – rootkits[40] being an example. The results may indicate that a significant proportion of consumers may not be fully aware of, or understand, many of the security threats they may face, suggesting that current consumer education campaigns may be inadequate.

Consumer quotes:

*"Don't know what phishing is, never heard of it."*

*"Is phishing the same as diallers?"*

*"I find that often Norton Anti Virus pops up and will let me know that a worm was trying to get onto my computer and it has stopped it - I don't know exactly what a worm is but it doesn't sound too good."*

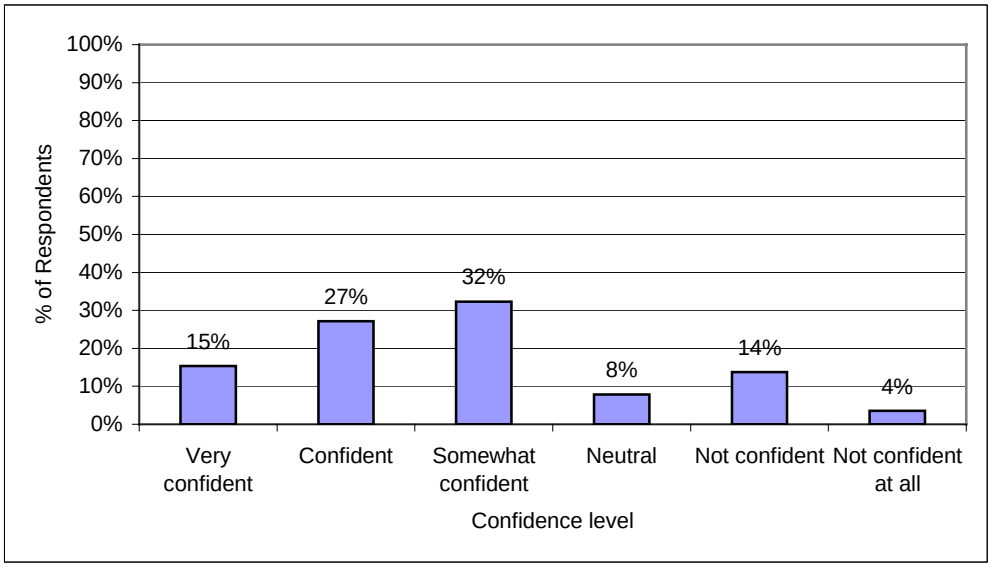
*"Phishing is particularly nasty and most likely to induce mistrust as you feel that you cannot receive communication from your own bank for fear of being tricked."*

*"In most instances the occurrences of harmful viruses come from Spam emails, while Trojan Horse and Worm viruses and dialler come from online gaming and other sites targeted towards children and young adults."*

*"No mention of keyboard sniffing...a very real vulnerability in cafes etc. where people use online banking while on the road."*

*"You didn't mention Rootkits, which are another security threat that the virus scanners and ad ware scanners don't detect."*

**13. On the whole, how confident are you that you can successfully identify these security threats when you're online for personal use?**




Summary: 15 per cent of consumers surveyed were, on the whole, 'very confident' they could successfully identify these security threats when they were online for personal use, 27 per cent were 'confident', 32 per cent were 'somewhat confident', 8 per were cent 'neutral', 14 per cent 'not confident', and 4 per cent were not confident at all'.

Comments: The majority of consumers surveyed were less then confident that they could successfully identify the security threats listed in the previous question. Worryingly, almost 1 in 5 were not confident or not confident at all. These results highlight that many consumers may not be confident in their ability to identify security threats in real-time, showing the danger that many consumers' computers may be compromised (even becoming 'zombies' – see note 11).

Consumer quotes:

*"I update regularly, I follow security bulletins, but I would not bet $1000 that my PC has not been compromised."*

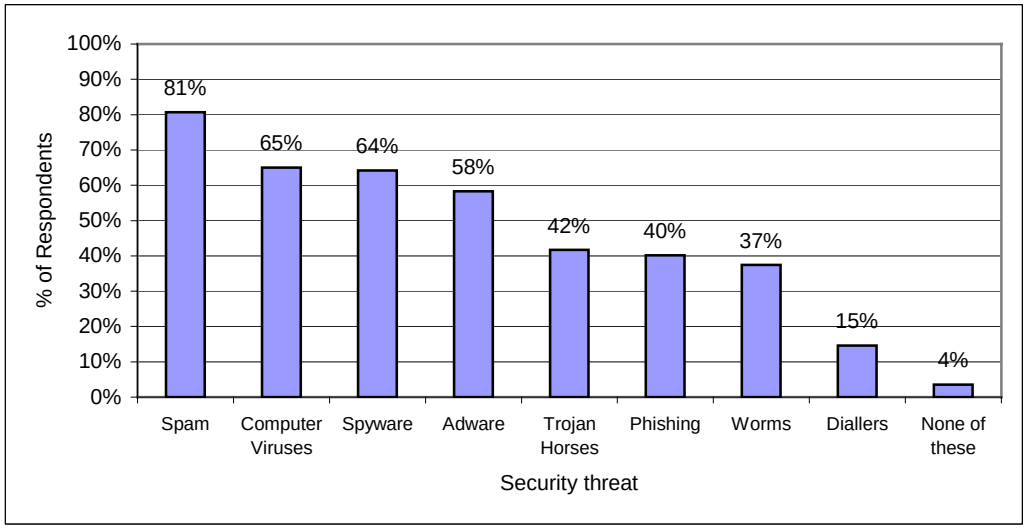
*"I'm a university graduate, yet I find it hard to determine whether I'm at risk with some downloads which purport to be helpful or necessary."*

*"I'd suggest there are many PC's with undetected security problems which are causing a degraded experience for the customer or the ISP."*

*"My wife once clicked [on] a virus that got through. McAfee had simply failed to see the virus, though it was correctly updated."*

*"Provide regular examples of recent examples of security breaches on PCs and what people were doing at the time."*

**14. Which of the following security threats have you experienced while online for personal use either on a computer you own/lease/rent or on a shared family computer?**




Summary: 81 per cent of consumers surveyed had experienced Spam while online for personal use either on a computer they owned/leased/rented or on a shared family computer, 65 per cent had experienced computer viruses, 64 per cent spyware, 58 per cent adware, 42 per cent trojan horses, 40 per cent phishing, 37 per cent worms, 15 per cent diallers, and 4 per cent had not experienced any of these.

Comments: The majority of consumers surveyed had experienced a range of security threats on their personal computers. Spam was clearly the most common (for more than 4 out of every 5 consumers surveyed), but computer viruses, spyware and adware were also typical problems (for more than 3 out of every 5 consumers surveyed). More than 1 out of every 3 consumers surveyed had experienced trojan horses, phishing, and worms. Considering some consumers were not aware of these threats (see Q 12), these figures may even be conservative.

These results highlight that most consumers are being attacked by a wide range of security threats. In particular, despite government action on Spam, it seems to continue to affect Australian consumers. Note that there has been Government action on diallers[41].

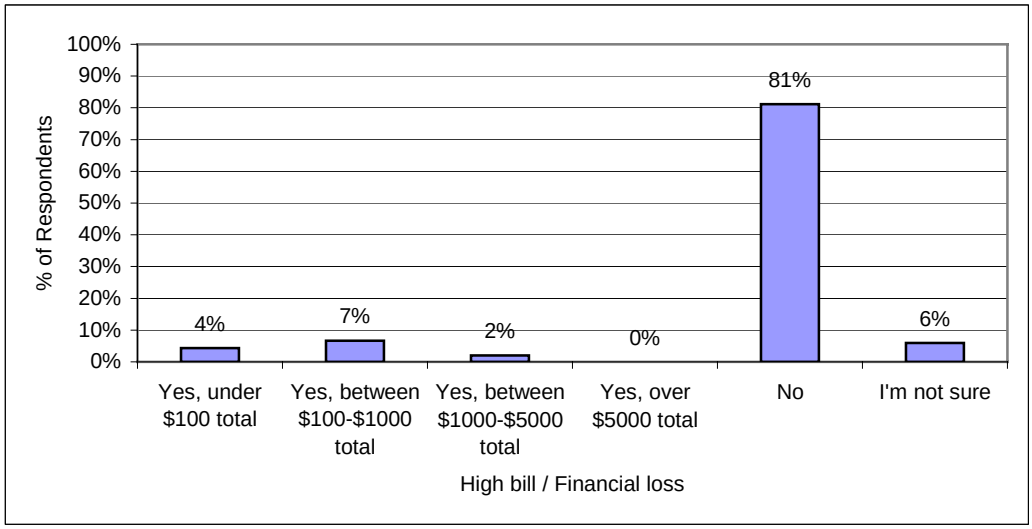
Consumer quotes:

*"SPAM is a serious problem for me."*

*"Had a hideous 3 day experience getting rid of a virus from our sons internet computer"*

*"An internet dialler was downloaded from a dodgy site another family member visited and redirected the call to an international number. The connection was so slow that the person using the computer noticed it and disconnected it. The bill was about $20, we were lucky it wasn't bigger."*

**15. Have you experienced unexpectedly high bills or financial loss that may have been the result of online security problems?**




Summary: 4 per cent of consumers surveyed had experienced unexpectedly high bills or financial loss under $100 that may have been the result of online security problems, 7 per cent between $100 and $1000, 2 per cent between $1000 and $5000, and 0 per cent over $5000, while 81 per cent had not experienced unexpectedly high bills or financial loss, and 6 per cent weren't sure.

Comments: More than 1 out of every 10 consumers surveyed had suffered financial loss or unexpectedly high bills as a result of security problems, with the majority of these losses exceeding $100. These results, combined with written comments we received, highlight the significant burden consumers face as a result of online security issues and hints at their impact on the economy, consumer satisfaction and productivity. Projected to the wider Australian population, consumers as a whole may be experiencing hundreds of millions of dollars of financial loss as a result of security problems, and many may be experiencing emotional distress and spending significant amounts of time dealing with security issues. We recommend further research to investigate the extent of the impact of security threats on consumers (the Productivity Commission may be well placed to do so).

Consumer quotes:

*"I get viruses all the time, and spend considerable time removing them…"*

*"I find much of my scarce available time is taken up deleting SPAM and worse…I am concerned that when away, my mail box will overflow with unwanted emails."*

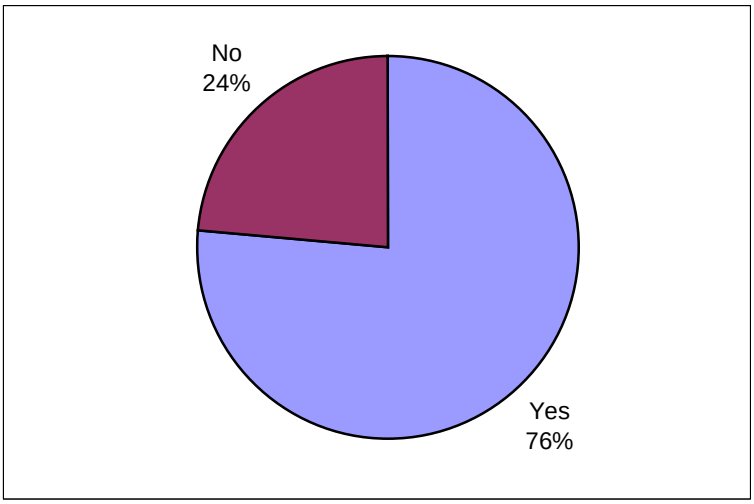
*"My daughter (who was 10) clicked on an unsolicited icon for a porn site which ended up costing me over $600 in Telstra bills."*

*"I have three networked computers at home going through a router and all are firewalled, have virus and spyware protection and still the PC's have at times been infected to such a degree that I have to have them formatted and the operating systems re-installed etc. This comes at a cost of at least $80 to $100 each time."*

*"I understand the who, what, when and where, however it's still a pain in the ar$e to have to deal with these 'security threats'."*

## Information About E-Security

**15. Have you actively tried to find information about online security issues?**




Summary: 76 per cent of consumers surveyed had actively tried to find information about online security issues, while 24 per cent had not.

Comments: The strong majority of consumers surveyed had actively tried to find information about online security issues. The results indicate a demand among consumers for information about online security, and highlights the importance of having accessible and reliable information available. As more consumers go online (see Note 1), the overall demand for information should continue to increase, making it crucial to have established, independent sources of information consumers can turn to.

Results also indicate that consumer education campaigns must also target beginners and inactive consumers (some of whom may be inactive by circumstance). Having mandated distribution of resources at point of sale or when signing-up for an Internet connection would be proactive, as would be free, in-person security training as part of new computer or Internet connection packages.

Consumer quotes:

*"Have to be pro-active"*

*"It's out there if you look for it. But the average internet-connected person needs to have it shoved in their face and to have it made clear"*

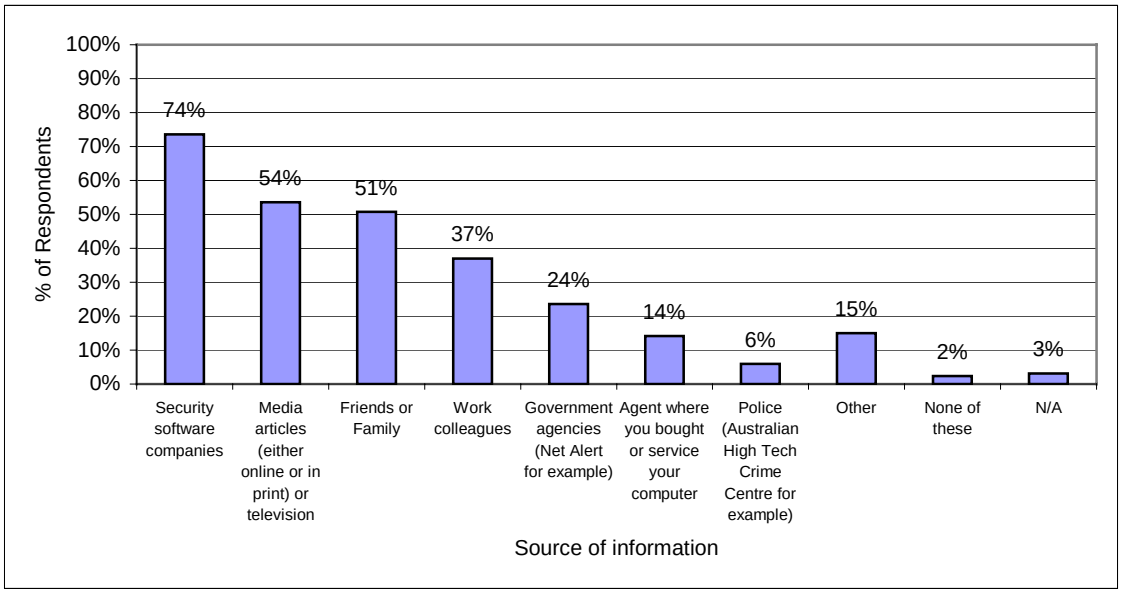
*'There is enough information online to fill an encyclopaedia, but your average Joe is too lazy and disinterested to learn more about security."*

*"Plenty of info if you have time/inclination to seek it amongst other competing demands."*

*"When you are not a confident computer user and you get a virus it is sometimes very daunting to go to a site and get the tools to fix the problem."*

*"Experience is a great teacher"*

**16. What sources of information about online security have you used?**

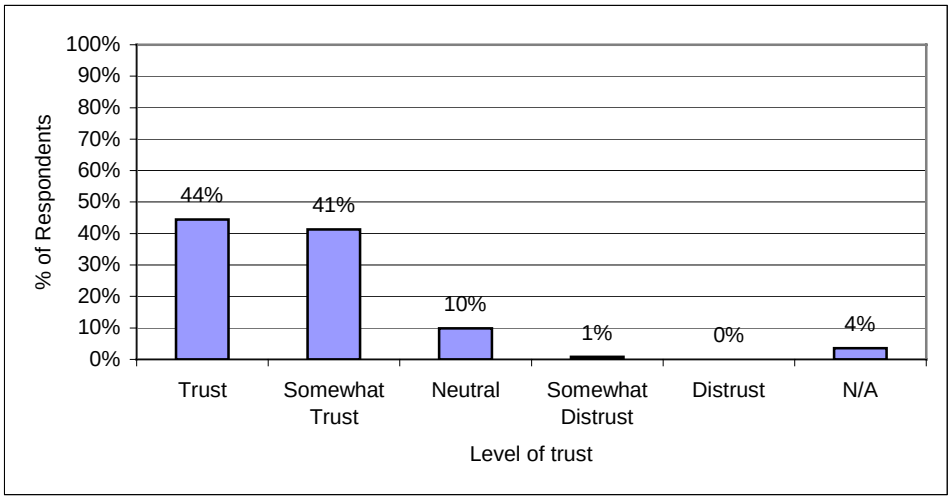



Summary: 74 per cent of consumers surveyed had used security software companies for information about online security, 54 per cent had used media articles or television, 51 per cent had used friends or family, 37 per cent had used work colleagues, 24 per cent of government agencies, 14 per cent had used agents where they bought or serviced their computers, and 6 per cent had used the police. 15 per cent of consumers surveyed had used other sources of information for online security, 2 per cent hadn't used any of the options listed and 3 per cent answered N/A.

Comments: Security software companies were the most used sources of information used by consumers surveyed, by a significant margin, followed by media articles. As alluded to in the *Introduction* to this report, considering the possibility that commercial interests may influence the information produced by such groups, we must explore how critical consumers are of the information they access – something the next question begins to investigate.

Importantly, these results may also show a limited reach of 'objective' sources of information (government agencies and police), which were used by less than 1 in every 4 consumers surveyed. There appears to be an opportunity for Government agencies to use the popularity of media as a vehicle to reach a greater proportion of consumers with independent information. Advertising campaigns using both commercial and public outlets (such as the ABC and SBS television and radio) is a logical option.

**17. On the whole, how much do you trust the sources of information you've used?**




Summary: On the whole, 44 per cent of consumers surveyed trusted the sources of information they've used, 41 per cent somewhat trusted sources they've used, 10 per cent were neutral, 1 per cent somewhat distrusted, 0 per cent distrusted sources they've used, and 4 per cent answered N/A.

Comments: Though consumers doubtlessly had different experiences with different sources of information, the results highlight that, on the whole, many consumers may be unsure about the reliability of information they are using to educate themselves and make decisions about online security issues. Many consumers commented on the vested interested of commercial sources. Regardless, since more than 1 in every 3 consumers surveyed indicated a full level of trust in the sources of information they used, and most consumers used commercial sources, the results also highlight the need for many consumers to think more critically about the information they use.

Besides trust, consumers raised concern over the availability (a clutter of sources, Government information sources not well known) and accessibility of information (not written in plain enough language, use of jargon). Further research is needed into investigating the best way to present information about online security to beginning, intermediate and advanced computer users.

Consumer quotes:

*Reliability of information:*

*"It is very difficult to differentiate between the hokes, hysteria and truth. don't blame many for giving up."*

*""It is hard to find genuinely unconflicted information"*

*"Concerned about conflict of interest for commercial security software vendors who need viruses to exist for them to be profitable."*

*"There is still a lot of self serving behaviour undertaken by security companies, in who's best interest it is that you buy particular products…This is unfortunate for ill-informed consumers as they can end up spending money on products they don't need."*

*"Software company's (or retailers) information is subject to salesmanship and sales knowledge... not a clear picture."*
*'All the publicity about these things makes me worry..."*

*"Much is alarmist, and often inaccurate."*

*"There is a lot of scare mongering in the popular press, but not a lot about where to get reliable information."*

*"I've seen many articles that are misleading and in some cases totally wrong because the person writing it was advertising products rather than giving information..."*

*"I have to trust their knowledge, how else could I use the Internet"*

*Accessibility of information:*

*"A clutter of sources - needs more focus to get to what you need."*

*"Most is not written in terms that are easily understood."*

*"I think there should be more said about online security for people who don't understand the internet very well. It should be put in very simple language."*

*"Sometimes confusing because of the use of jargon familiar to the supplier but not the user."*

*"Just send us something simple….not everyone is a walking, talking computer whiz…if I try to read and comprehend all the technicalities of the internet world, I'm exhausted and feel so silly, dumb…its like trying to follow instructions as to how your new mobile phone works…sorry…but we just need to get to the point, straightaway…"*

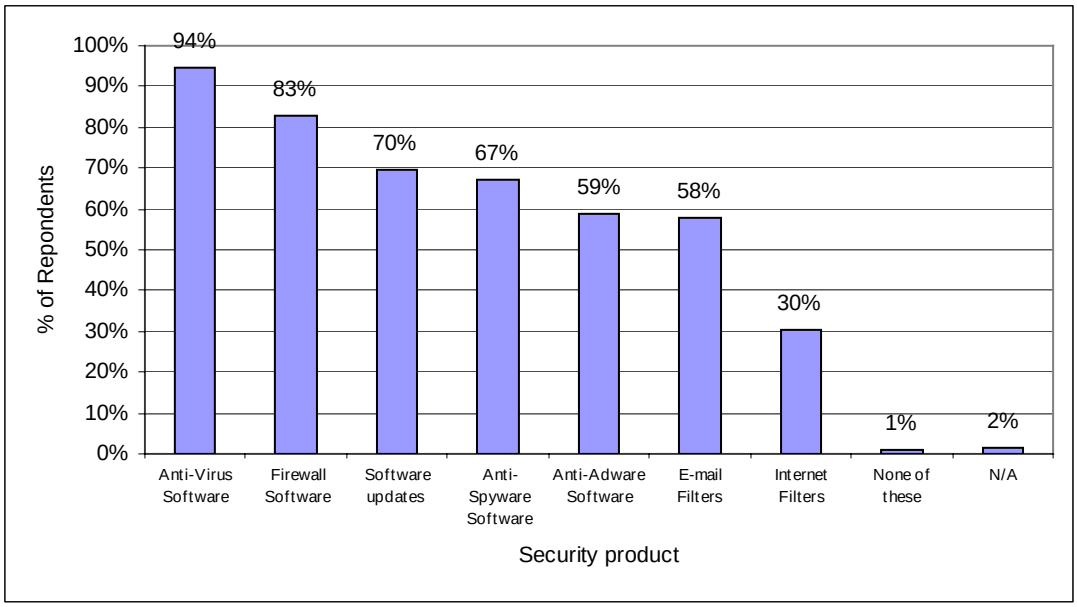
*"Can be difficult to really understand some of the Government stuff."*

*"If Net Alert is a government info site then it needs to be better publicised."*

*"The govt needs to provide more information to the vast majority of 'consumers' about what to look for. The information needs to be better targeted to ensure people at all levels of knowledge can access the appropriate information for their level of understanding."*

## Security Measures

**18. Which of the following security products have you used on a computer you own/lease/rent or on a shared family computer?**

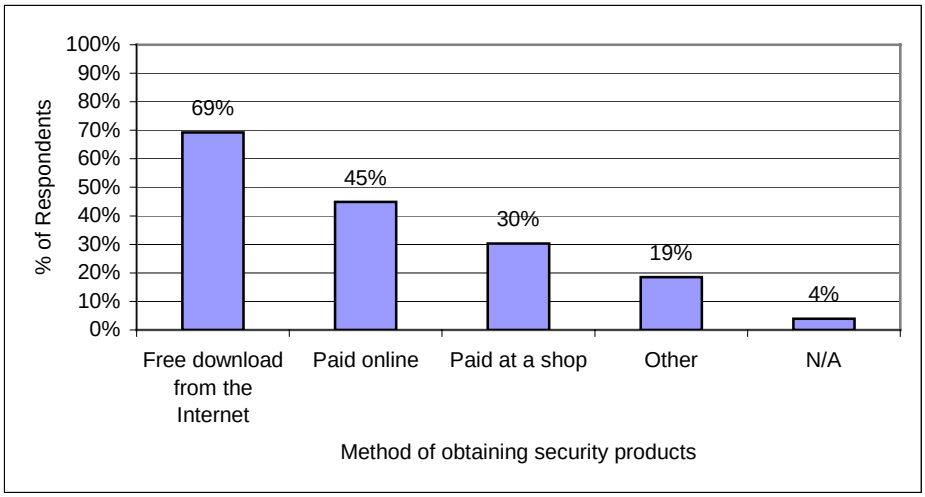



Summary: 94 per cent of consumers surveyed had used anti-virus software on a computer they owned/leased/rented, or on a shared family computer. 83 per cent had used firewall software, 70 per cent had used software updates, 67 per cent had used anti-spyware software, 59 per cent had used anti-adware software, 58 per cent had used e-mail filters, 30 per cent had used Internet filters, 1 per cent did not use any of the products listed and 2 per cent answered N/A.

Comments: The majority of consumers surveyed had used all of the security products we listed, with the exception of Internet filters (which may soon change as a result of the $116.6 million National Filter Scheme[42]). Anti-virus software was nearly universally used, as were firewalls. From comments we received it appears many consumers used more than one version of any particular category of product (two anti-spyware programs running simultaneously, for instance). A potential worry, considering the importance of security patches, is that more than 1 out of every 4 consumers surveyed had not used software updates.

These results may indicate that most consumers are using multiple security products, especially anti-virus and firewall software. This highlights the enormity of the consumer security product market and, potentially, the high degree of importance (or reliance) consumers place on security products.

**19. How did you get the security products you used?**




Summary: 69 per cent of consumers surveyed had downloaded free security products from the Internet, 45 per cent paid online for security products, 30 per cent had paid at a shop, 19 per cent had used other means, and 4 per cent answered N/A.

Comments: Most consumers surveyed obtained security products online, and a strong majority, almost 7 out of every 10, had used free security products. Though a significant proportion of this free software may be accounted for by software updates, the results point to the possibility that many consumers are using free products offered online[43]. This possibility raises the question – what impact on consumers' security will be felt if fewer free products are available in the future? Again, further research needs to investigate the costs consumers are incurring, and are reasonably able to incur, not only as a result of security attacks but also to protect their systems with security products.

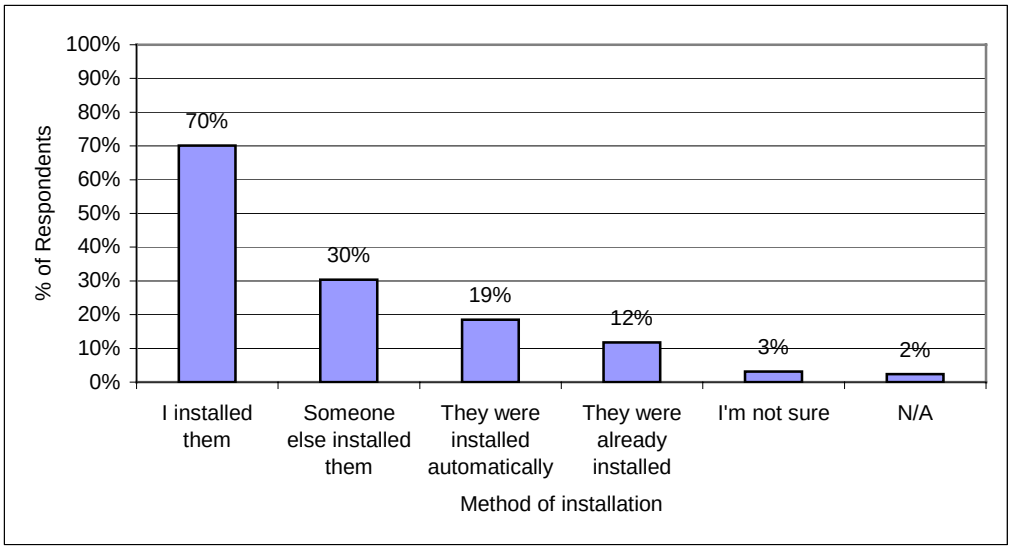
An issue which is touched upon again by these results is the relationship between security measures, especially critical software updates, and a consumers' Internet connection. If many consumers are using the Internet to obtain their security products, and many are using slow or unreliable broadband, they may be facing serious challenges to completing important downloads.

Consumer quotes:

*"There are a variety of free software tools on the net"*

*"Numerous reliable companies…provide freeware that can be downloaded to help protect your PC to provide a reasonable level of protection."*

**20. How were the security products installed?**




Summary: 70 per cent of consumers surveyed had personally installed security products they used, while someone else has installed security products for 30 per cent of consumers surveyed. Security products were automatically installed for 19 per cent of consumers surveyed and already installed for 12 per cent, while 3 per cent were not sure how security products they has used were installed. 2 per cent answered N/A.

Comments: These results highlight that consumers had used a range of methods to install security products. Most had installed products themselves, but for a significant proportion of those surveyed, someone else had installed some of their security products. The later result may indicate that, to varying degrees, some consumers may be relying on someone else to manage their online security. This may also highlight a problem concerning the expiry of security software. If consumers are using software someone else installed or software that was either already installed or automatically installed, they may be confused when they are prompted to renew, leaving them in a potentially pressured situation, or more vulnerable if their protection expires without replacement.

Consumer quotes:

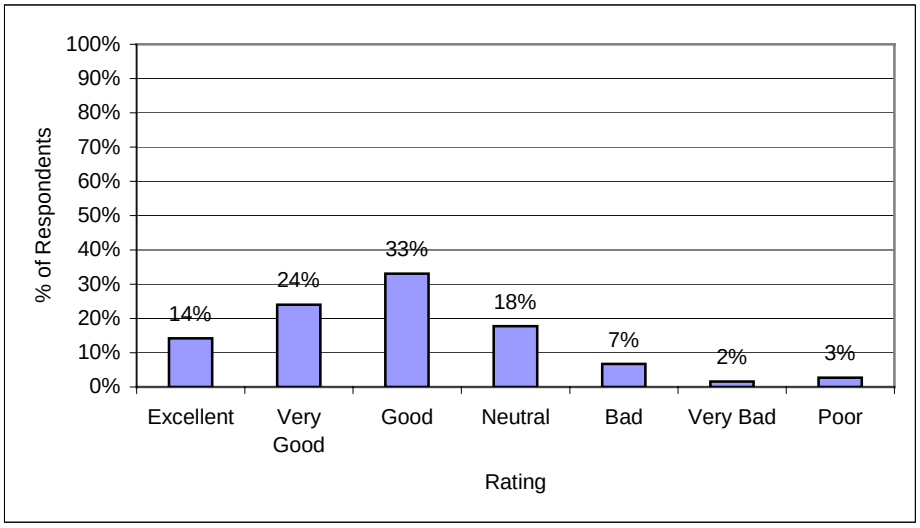
*"I am aware of the threats, but my husband (my personal IT dept) takes care of the anti-threat software and runs it frequently."*

*"Triumph of hope and reliance on a techie who can work remotely on my pc and occasionally visits on a paid basis."*

*"I use a computer technician to assist me with any difficulties and rely on his advice."*

*"I'm not very techo-savvy so I rely heavily on other people who know what it's all about to take care of security precautions for me (at home and at work). If it was up to me to look after security, I would be a lot less confident about using the net for transactions."*

**21. On the whole, how would you rate your understanding of how security products protect you?**




Summary: 14 per cent of consumers surveyed rated their understanding of how security products protected them as "excellent". 24 per cent rated their understanding as "very good", 33 per cent as "good", 18 per cent as "neutral", 7 per cent as "bad", 2 per cent as "very bad" and 3 per cent as "poor".

Comments: At first glance, it's an encouraging to see that 70 per cent of consumers surveyed rated their understanding of how security products protect them as good or better. However, upon closer inspection the results do not appear as encouraging. Most importantly, almost 1 in every 3 consumers rated their understanding of how security products protect them as less than good. If this ratio is even roughly equivalent on a larger scale, there is a significant potential for many consumers to become reliant on software prescribed to them, without knowing how it works. Ultimately this may leave consumers dangerously vulnerable to attacks as they evolve – a vulnerability further underscored by the fact that security products are neither universally effective nor immune from attack themselves (see note 16).

Consumer quotes:

*"I am totally uneducated in this and obviously need educating"*

*"I just hope that what has been put into my computer will work...but I'm still a bit worried."*

*"I just rely on my Norton's anti virus software completely"*

*"When I bought my computer I was somewhat aware of these things, so I went to my local computer shop and asked them what to buy in terms of anti-virus software, and bought what they suggested, without going into any further research or discussion than that."*

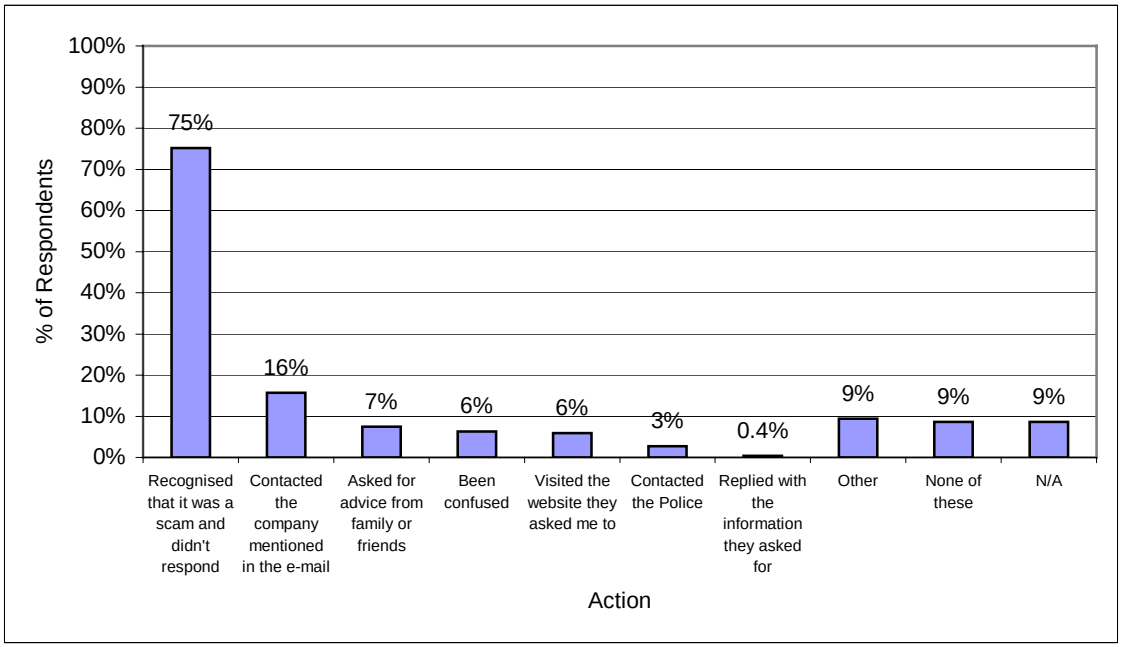
*"You never know whether you have the best…or how effective they are."*

*"The need of buying software that is compatible is a difficult task for an individual to keep up with as the threat changes."*

*"Confusing as determining the best software for home/work use is difficult to understand and to decide on the best mixes to cover the various threats."*

## Security Measures – Spotlight on Phishing, Spam, Adware

**22. Have you done any of the following when you've received a "Phishing" e-mail -- for example an e-mail asking you to visit the website of a company you use (a bank for instance) or asking you to provide personal information?**




Summary: 75 per cent of consumers surveyed had recognised phishing e-mails as a scam and hadn't responded, 16 per cent had contacted the company mentioned in the e-mail, 7 per cent had asked for advice from family and friends, 6 per cent had been confused, 6 per cent had visited the website the e-mails had asked them to, 3 per cent had contacted the Police, and less than 1 per cent had replied with the information the e-mails had asked for. 9 per cent of consumers surveyed had other responses to phishing e-mails, while 9 per cent had not reacted as any of the choices describe and 9 per cent answered N/A.

Comments: Most consumers surveyed recognised phishing e-mails and hadn't respond to them. However, the results do indicate that phishing has the potential to fool significant numbers of consumers. Since phishing is done on such a wide scale, even the slimmest of response rates (even the 1 out of 254 rate in this collection of consumers) may still result in significant consumer losses as a whole. Similarly, even a relatively small percentage of consumers visiting the websites that the phishing e-mails asked them to visit (6 per cent of this collection of consumers), or being confused by phishing e-mails (6 per cent of this collection of consumers) may lead to unwanted experiences or financial loss.

A recent research paper titled, "*Why Phishing Works*" [44] indicated that, "even in the best case scenario, when users expect 'spoofs' to be present and are motivated to discover them, many users cannot distinguish a legitimate website from a spoofed website". The report goes on to say that indicators designed to signal trustworthiness to consumers were not understood (such as browser indicators and certificates) and were easy to spoof, that fully functional and professionally looking

sites can be falsified and that legitimate organisation further confused consumers by hosting secure sites with third parties.

Also noteworthy was that less than 1 out of every 5 had made “proactive” responses such as contacting the company mentioned in the e-mail, asking advice from family, friends, or contacting the police (we overlooked including reporting to or consulting the Australian Competition and Consumer Commission’s ScamWatch website).

Consumer quotes:

*“I'm very computer literate - I'm the person everyone asks about their computer problems, and I was worried by the accuracy of the phishing emails I received - If they looked good to me, I could understand people being taken in by them.”*

*“I wanted to believe I had won that amount of money even though I knew it was 'too good to be true' I automatically responded to their first email - then realised it was most likely a scam and did a thorough 'clean' and computer check. I filled in the 'slam a Cyberscam' form…”*

*“The majority of them ARE SCAMS, yes!!! BUT...BUT...there JUST maybe 1 or 2 that are truly real!!!!”*

*“Look alikes are so professionally presented’*

*“It is difficult for people to know at times if emails are a hoax or genuine.”*

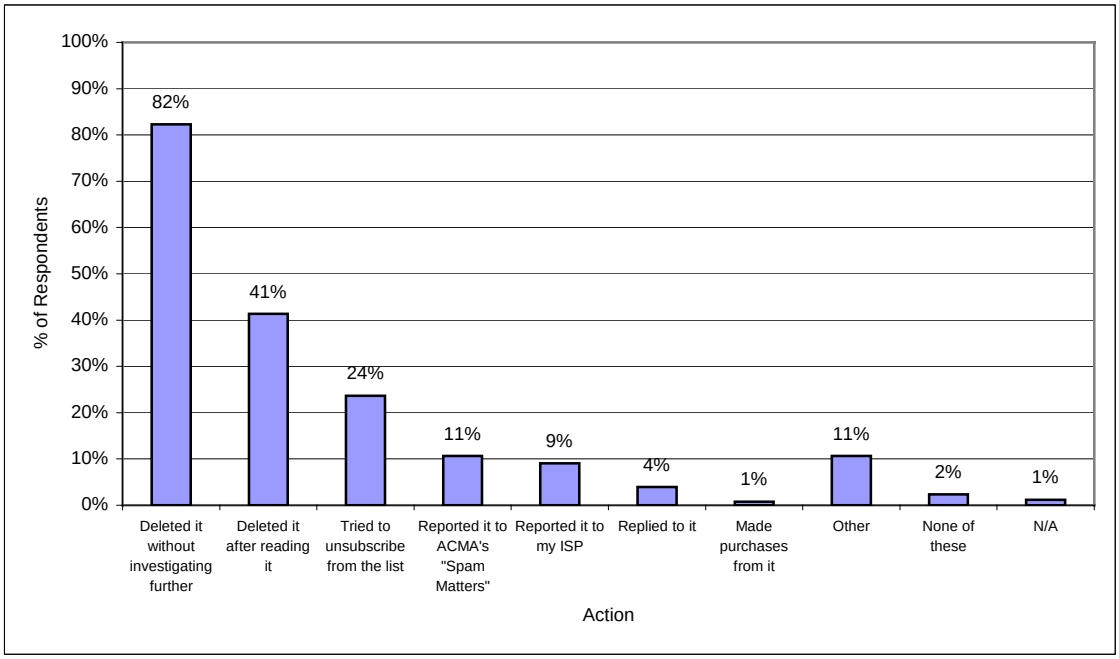
*“I never click to remove myself off a mailing list in a phishing email.”*

*“I told police about rip off, they laughed.”*

*“I always forward phishing emails to my bank when they arrive for them to follow through with in case it is a new threat not yet known.”*

*“Note that banks are always providing advice on phishing.”*

**23. Have you done any of the following when you've received Spam -- for example an e-mail from a source you don't know, trying to sell you something?**




Summary: When receiving Spam, 82 per cent of consumers surveyed had deleted it without investigating further, 41 per cent had deleted it after reading it, 24 per cent had tried to unsubscribe from a mailing list, 11 per cent had reported it to the Australian Communications and Media Authority's "SpamMATTERS" program, 9 per cent had reported it to their ISP (Internet Service Provider), 4 per cent had replied to it, and 1 per cent had made purchases from it. 11 per cent had done something other than the choices listed, 2 per cent had not done any of these actions, while 1 per cent answered N/A.

Comments: Though these results only scratch the surface on consumers' experiences with Spam, we believe that on the whole they show many may be vulnerable to the unwanted effects of Spam (such as time loss, fraud, and other security breaches) despite the *Spam Act* being in place.

An encouraging good sign may be the strong majority of consumers who deleted Spam without investigating it further, which may indicate that many consumers are developing a savvy when it comes to identifying and dealing with Spam. However, deleting e-mails without investigating them does run the risk of accidentally deleting legitimate mail.

Another encouraging sign is that 1 in every 10 consumers surveyed had reported Spam to the Government through the Australian Communications and Media Authority's (ACMA) SpamMATTERS program for further investigation, despite it only being launched a few months before the survey was conducted (a few consumers did complain that it wasn't available for MAC users).

Most worrying, however, were the results that indicated that some consumers may be replying to Spam (4 per cent), making purchases from Spam (1 per cent) or tyring to unsubscribe from Spam (24 per cent). Though it is unclear whether these

purchases or responses brought about positive or negative experiences for consumers, even a small percentage of consumers being scammed or opening themselves up to more Spam or malware may have a far reaching impact as a whole. In the case of attempting to unsubscribe, the effectiveness or danger in doing so may depend on how legitimate the business sending the mail is or if they are a company subject to the Australian Spam Act.

Another concern is that, though a significant proportion of consumers surveyed had deleted Spam after reading it, there is a time cost involved in doing so and a greater chance of being scammed or attacked by malicious code/programs.

Another area of concern is the low proportion of consumers surveyed who had reported Spam to their ISP. As later results show, many consumers surveyed would like ISPs to take more responsibility protecting them from security threats. Spam seems like a logical area in which ISPs can be mandated to provide more assistance, such as free e-mail filtering services.

Consumer quotes:

*"I just wish SPAM could be stopped."*

*"Often the send[er] of the email has the name of someone I genuinely correspond with, and I have to think twice when I first see the email…"*

*"From now on if I don't recognise an email address, I delete it straight away. I can usually tell from the subject or the sender's address that it is Spam"*

*"I know that there's a Spam Act so I know the difference between Spam emails that I can stop and I can't do anything about - I unsubscribe from the ones covered by our Spam act."*

*"It makes no difference flinging it into the Spam world of never, never...they're still there the next time round."*

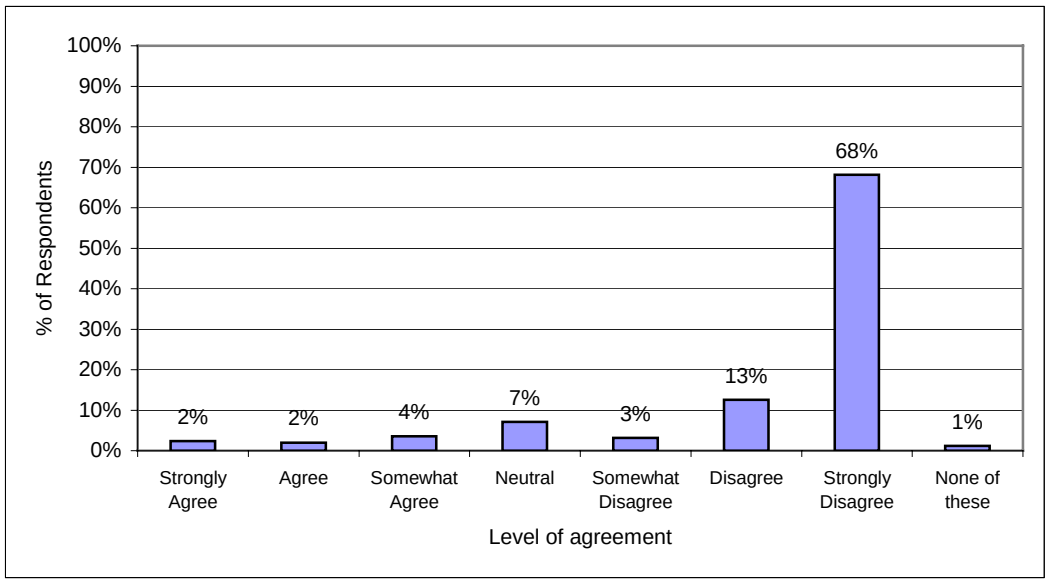
*"I report every single Spam to the US FTC, SpamCop and the ACMA. I report every phishing attempt to US CERT and the Australian bank if I can find a reporting address. I report pump-n-dump Spam to the US SEC. If you think I'll do anything I can to hurt spammers and scammers, you're right!"*

*"I believe that Australian Spam is now being tracked and possibly prosecuted but what of the stuff from overseas"*

*"I actively report spammers to the hosts of reverse block lists…so that they are prevented from doing further damage… After all, if the signal to noise ratio becomes as bad for the spammers as it is for their victims, it might just become unprofitable enough that they give up.*

*"ACMA should handle Spam for MAC OS users."*

**24. "Adware" includes programs that can be downloaded to your computer or run in the background to your Internet browsing, often without you knowing, to serve you with advertising. They can also collect information on your Internet usage to provide "targeted" advertising. Do you agree with the use of "Adware"?**




Summary: 2 per cent of consumers surveyed "strongly agree" with the use of adware, 2 per cent "agreed", 4 per cent "somewhat agreed", 7 per cent answered "neutral", 3 per cent "somewhat disagreed", 13 per cent "disagreed", 68 per cent "strongly disagreed", and 1 per cent answered "none of these".

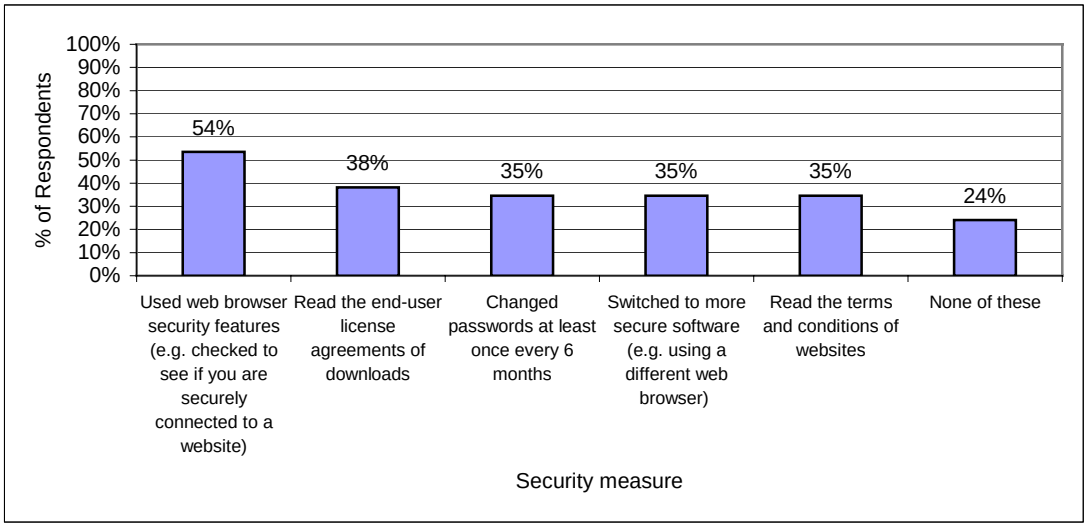
Comments: A large majority of consumers surveyed did not agree with the use of adware, most strongly. On the whole, there is much unknown about adware – in our survey more than 1 in every 3 consumers surveyed either did not fully understand adware, had never heard of it or weren't sure if they'd heard of it (see Q. 12). While some types of adware have the potential to provide benefit to consumers' experiences online (some cookies, for example, can help remember a users' settings on a website), there is much potential for adware to adversely affect consumers. The latter is especially relevant considering the grey area between spyware and adware. Privacy is one of many concerns in this area, with threats even coming from large, well-known companies[45].

It seems to be the case that there is a clash between consumers' needs and commercial wants – consumers expect free or inexpensive content online but often commercial profit is a prerequisite for the content. Furthermore, commercial entities may not want consumers to know about the methods they're using to track habits and serve advertising. In the least, to ensure consumers are adequately protected, there must be full disclosure of the use of adware, and consumers must give their informed consent to its use. We are recommending that informed consumer consent be the central principle of the Adware guidelines being developed by the Internet Industry Association and Australian Direct Marketing Association (see Note 23).

Consumer quotes:

> *"I am against any form of tracking information by other people. If I wanted that information to be given I would provide it to them myself."*
>
> *"The merger of malware and adware is a terrible blurring of boundaries, and I am scared that spy and virus software companies are not really able to be completely frank with me because of litigation pressure from marginals."*
>
> *"I am very concerned about businesses here and overseas in effect acting like viruses or spyware, adding things to my computer without asking, but claiming to be legitimate, because they have no respect for me and are likely to be a serious cause of trouble on my computer."*

**25. Have you regularly taken any of the following security measures while online for personal use?**




Summary: 54 per cent of consumers surveyed had used web security features (e.g. checked to see if they were securely connected to a website) while online for personal use, 38 per cent had read the end-user license agreement of downloads, 35 per cent of consumers had changed passwords at least once every 6 months, 35 per cent had switched to more secure software (e.g. has used a different web browser), 35 per cent had read the terms and conditions of websites, while 24 per cent of consumers surveyed had taken none of these measures.

Comments: These results lend support to the view that many consumers may not be proactive about their security beyond employing security products. We collected this list of recommended measures from various government, NGO and industry sources on online security. Only a slim majority of consumers had regularly used web security browser features. Beyond this, no measure was taken regularly by a majority of consumers we surveyed, and approximately 1 in every 4 had not taken any of the measures we listed. In the case of changing passwords, many comments alluded to the complexity of managing multiple passwords.

Consumer quotes:

*"With so many numbers and passwords to remember a new one means remembering what is the current code and in a one not used often it can get a bit confusing."*

*"Far too messy to change many passwords every six months"*

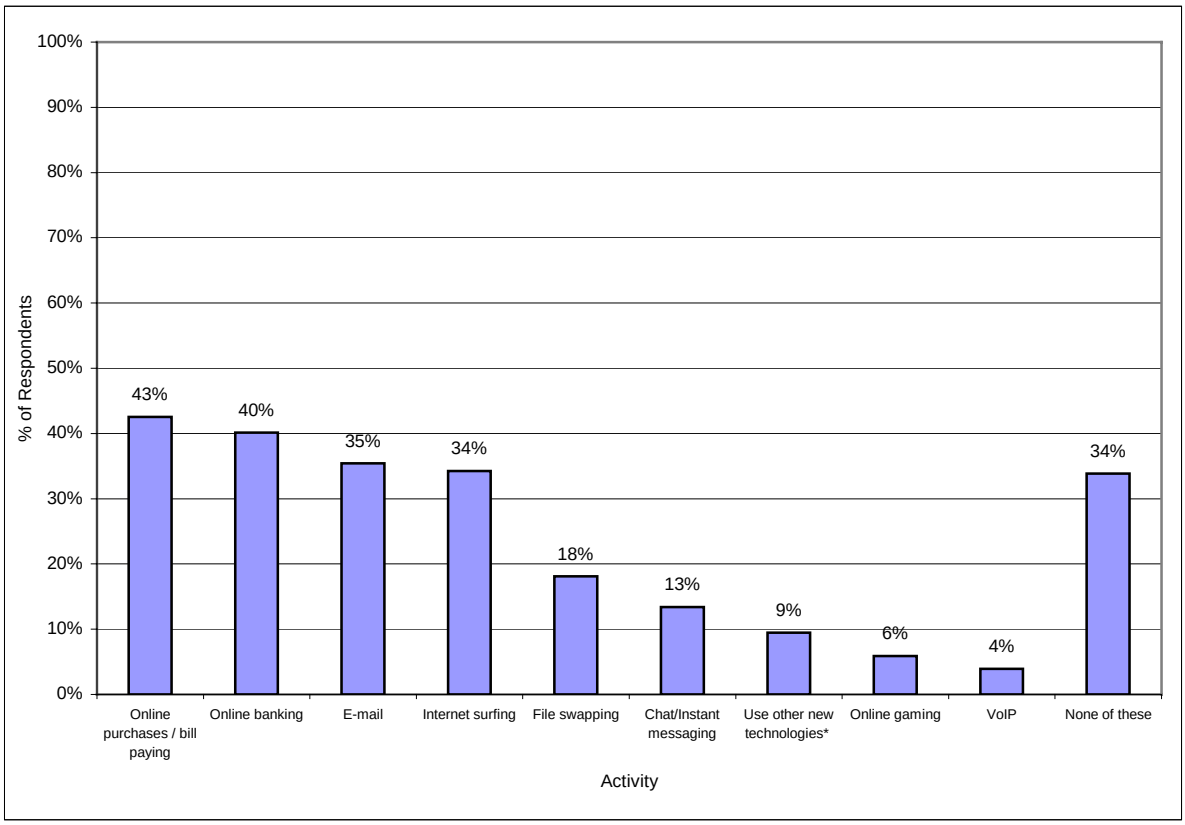
*"If a password is compromised it has to be changed immediately, but since one does not know when it has been compromised, 6 months would be to long as well. So change it daily? not really."*

*"Too many ways in a sites terms and conditions absolving themselves of responsibility"*

*"I have also "Googled" information found on suspect emails, and search for information on free software (ratings, forums, etc) before downloading/installing."*

## In the Future

**26. Have online security concerns or experiences stopped or changed the way you do any of the following?**




* A different type of Internet connection or new types of mobile phones for example

Summary: 43 per cent of consumers surveyed had stopped or changed the way they used online purchases or bill paying as a result of online security concerns or experiences, 40 per cent had stopped of changed the way they used online banking, 35 per cent e-mail, 34 per cent Internet surfing, 18 per cent file swapping, and 13 per cent chatting or instant messaging. 9 per cent had stopped or changed the way they used new technologies (such as a different type of Internet connection or new types of mobile phones) as a result of online security concerns or experiences, 6 per cent had stopped or changed the what they used online gaming, and 4 per cent VoIP. 34 per cent of consumers surveyed had not stoped or changed the way they did any of these activities as a result of security concerns or experiences.

Comments: These results indicate that security concerns and experiences may be significantly affecting consumers' behaviour online, even preventing them from accessing and enjoying the full range of services and content available to them. Specifically, consumers may be changing their use of online purchasing services, online bill-paying services, and online banking the most. Projected to a larger base of consumers, one can see the potentially large affect this change in behaviour can have on consumers (and potentially the economy) in a society in which more and more important information and services are pushed online and into new technologies.

Finally, 34 per cent of consumers we surveyed had not changed the way they did any of the activities we listed as a result of online security concerns or experiences. Are they not changing their behaviour because they are confident of their protection online or because they are unaware of the threats that they may face?

Consumer quotes:

*"Because I am afraid of identity theft I don't buy online and only have a small amount in a visa card"*

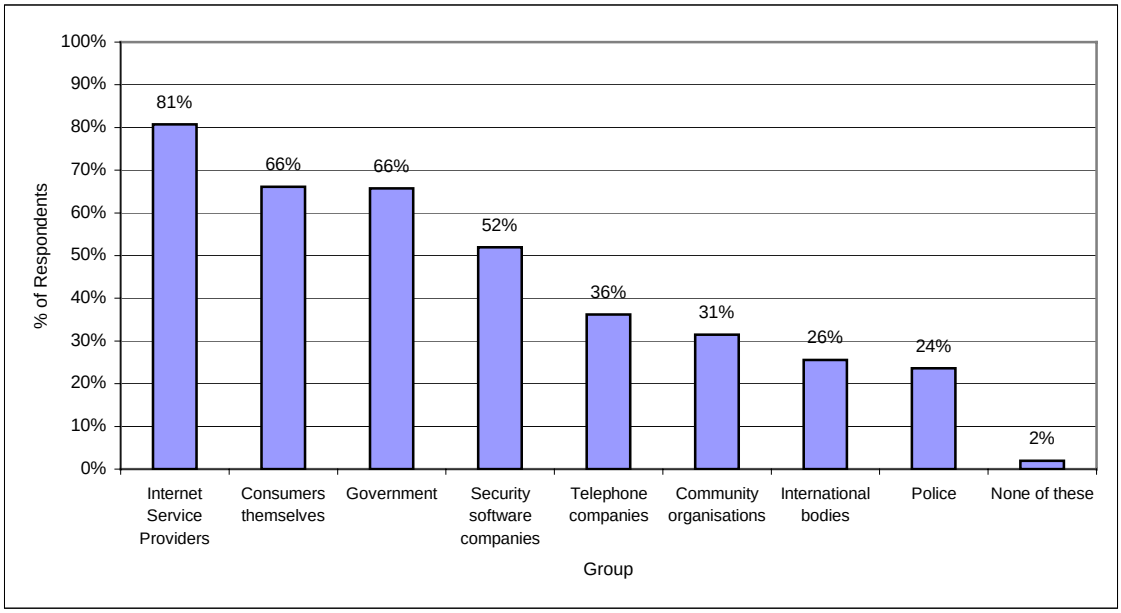
*"I'm not confident  using online banking because I'm in two minds as to how safe it really is."*

*"I do not trust online banking as I feel Australia hasn't taken Online Security seriously enough. I feel that very little has been done to protect me from online security threats."*

*"I worked in the finance industry and aware of the high amount of internet fraud - so therefore I do not do any banking, bill paying or shopping on line"*

**27, 28. Which of the following groups do you think should take more responsibility to provide better security online for consumers?**

**Share any comments you have on what should be done to better address online security issues for Australian consumers.**




Summary: 81 per cent of consumers surveyed thought Internet Service Providers should take more responsibility to provide better security online for consumers, 66 per cent thought consumers themselves should, 66 per cent Government, 52 per cent security software companies, 36 per cent telephone companies, 31 per cent community organisations, 26 per cent international bodies, 24 per cent police and 2 per cent thought none of these should take more responsibility to provide better security online for consumers.

Comments: More than 4 out of every 5 consumers we surveyed wanted ISPs to take more responsibility to provide better online security for consumers. 2 out of every 3 consumers surveyed named their fellow consumers and Government.

Written comments shed further light onto what consumers may have in mind for each group. For ISPs, some suggested mandated, free filtering of Spam and phishing. For consumers, some suggested that individuals should be more responsible for addressing their own online security. At a Government level, some suggested a tougher stance on online security – more legislation, tougher sanctions, and better enforcement. Some wrote that Government should hold companies responsible for the software they release and some consumers suggested a central reporting body for security attacks. In the least, Government legislation, sanctions, enforcement and reporting processes must be constantly evaluated and developed to ensure that basic consumer rights are adequately being met in the online world. For instance, it is unclear how well bodies such as the Australian High Tech Crime Centre, AusCERT (the national Computer Emergency Response Team for Australia), of NetAlert are among consumers, or how prepared police forces are to lay charges[46].

Concerning industry, many consumers commented on the need for commercial companies to be proactive in protecting their customers and ensuring their products are secure. Finally, across all of these groups, many consumers made it clear that education is of the utmost importance. Some suggested more direct distribution of information as a priority.

Consumer quotes:

***Consumers on Consumers:***

*"Consumers should be proactive about their own online security."*

*"I think the key issue is that protection is a day-by-day responsibility. Definitely not a case of fit-and-forget."*

*"Too many do not care enough about security while their PCs are happy bots-bots."*

*"It is ultimately the consumer who must take responsibility for being properly informed about the market they are in."*

*"It's frustrating when you get viruses from other computer uses that have not kept up to date with security."*

*"Newcomers to the internet advised to use commonsense at all times the same as if someone called at your front door or contacted you by telephone"*

***On ISPs:***

*"I believe server providers could be more diligent in stopping Spam, phishing emails as they come into their servers. The technology is there and consumers should not wear the brunt of all the responsibility. The cost of access to the internet and emails is still quite high compared with overseas and whilst this is so the ISP's still have a responsibility to do more to make surfing the net and accessing emails a safer experience for consumers."*

*"I think that internet providers need to have far more friendly reporting mechanisms for Spam…I though that providers were trying to make their servers more secure. doesn't seem so."*

*"There are many technical measures which ISPs can put in place which will minimize or eradicate Spam (at least within Australia).. Making ISPs share some of the responsibility for Spam sent from their networks, e.g. through the imposition of fines for not implementing easy to manage technical steps might also be effective."*

*"ISPs need to offer more protection as a standard - after all, most offer increased protection for a fee!!"*

*"Is it possible for the Govt to make it so Internet providers have to automatically scan and warn of these. I have to pay an extra $4 a month to have this done."*

***On Government:***

*"Self regulation does not work, there needs to be very heavy penalties for those that flaunt the laws in regard to internet security."*

*"Phishing, Spam or Adware should not be tolerated at any level in this country."*

*"I personally believe that persons creating virus's, spyware etc are the scum of the earth. If found they should be prosecuted and jailed for life."*

*"Police need to arrest the scammers"*

*"Prosecute virus writers with large sentences."*

*"…companies producing shawdy software with low quality or non-existent security should be made responsible and accountable, just as any company would be in other sectors of the economy. Currently, shawdy software manufacturers are getting away with blue murder on the Internet."*

*"You pay hundreds of $ and have no chance to make a SW vendor liable."*

*"A Central reporting body for such matters and easy access and contact would be helpful."*

*"I filled in the 'slam a Cyberscam' form but also wished there was a database or something so I could check these 'phishers' online!!"*

*"Change the legislative regime to better ensure that software vendors are forced to accept liability for their insecure products.'*

*"Keep government bodies well out of it"*

***On Commercial Companies:***

*"The responsibility to provide better online security should be with the operating system & software vendors. i.e. don't release software & products with security flaws in the first place."*

*"Banks need to do more to protect customers"*

*"Inexpensive software that will give as much protection that is possible against all the issues mentioned above."*

*"Most people are let down by the resellers of computer systems who do not adequately explain the risks with insecure operating systems and software eg windows XP, internet explorer - these systems require significant effort to avoid even the common problems."*

***On Consumer Education & Awareness:***

*"Ultimately though, the most effective countermeasures are better educated consumers…"*

*"Education campaign to inform consumers of the risks and what can be done to protect themselves."*

*"An understanding of the underlying protocols, even to a basic degree, can greatly help one understand why security awareness is necessary and what measures can be taken to improve security."*

*"It would be advantageous if computer points of sale encouraged or assisted people in the use of spyware, antivirus, firewalls etc and had brochures with simple explanations of use and need when a computer system is purchased."*

*"It should be a basic part of the school curriculum, in the same way that we warn people about other threats to society and individuals."*

*"Everybody should get a simple non-jargon pack of information about what to do sent to their computer."*

*"Ensure people are more aware when purchasing a computer and/or connecting to the Internet."*

*"'Dummies guide' to security could be offered with computer purchase, as in a brochure (hard copy)."*

*"Provide up to date - and refresher training in libraries for individuals - you don't have access to updates when retired/unemployed etc"*

*"Sadly, as cyber-space is so full of undesirables on the make who prey on the unwary and uninformed, perhaps information contained within normal snail mail Telco accounts and information brochures would be helpful as well as safer."*

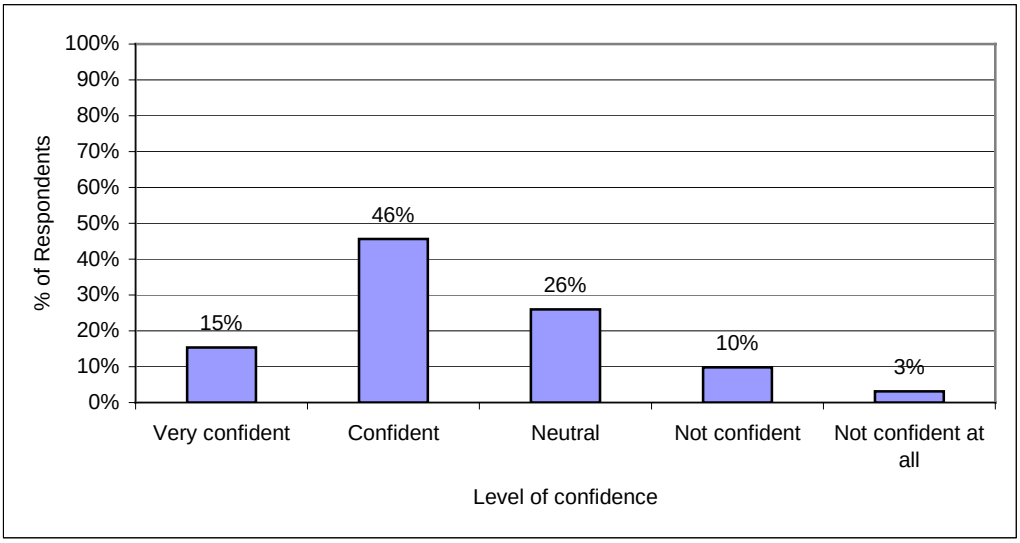
*"Australians are generally unaware at to who they should report illegal activity to: AFP, Police, A.G., Broadcasting Authority, etc."*

*"More media education for everyday consumers"*

*"Awareness needs to increase and a good way to raise awareness is to raise the profile - get the media involved, get politicians talking about it."*

*"A lot of good advice is hidden in the technical sections of the media, instead of being put where everybody can see it"*

**29. On the whole, after this survey, how confident are you that you can effectively protect a computer you own/lease/rent, or a shared family computer from online security threats?**

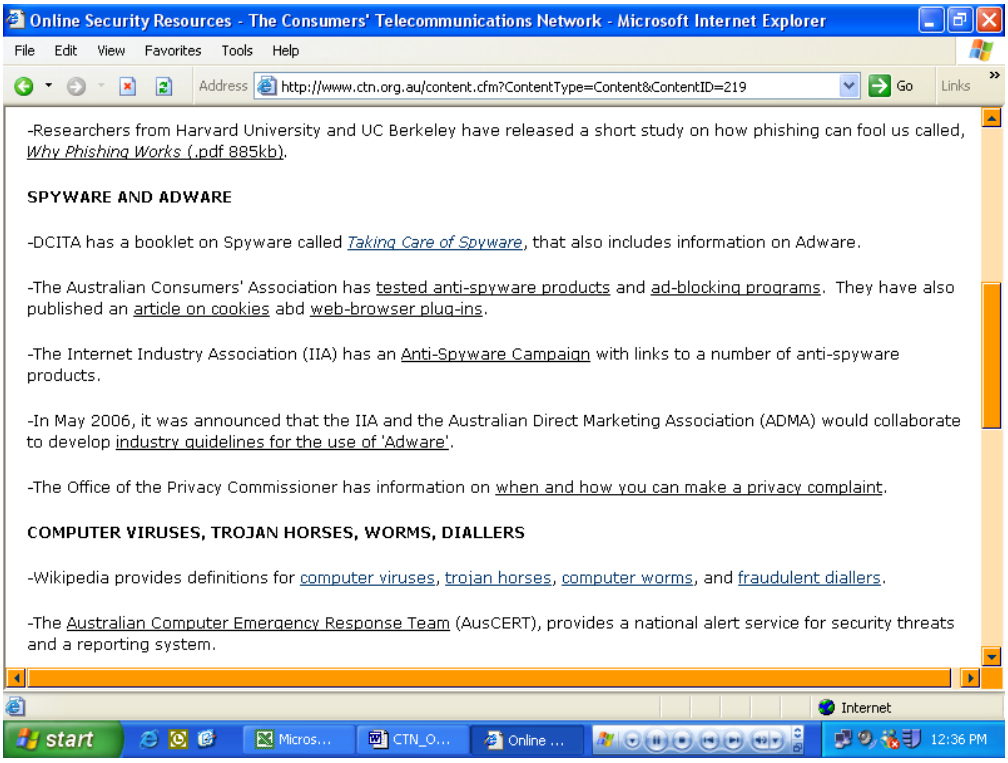


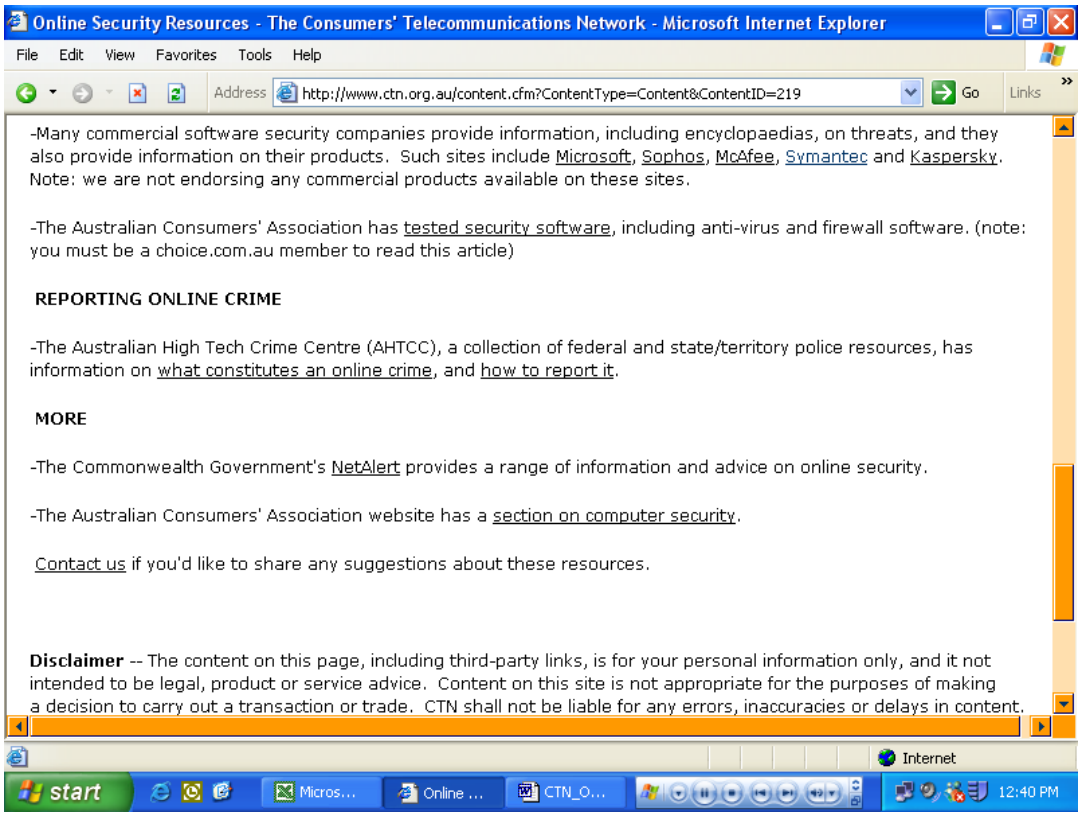

Summary: 15 per cent of consumers surveyed were 'very confident' they could effectively protect a computer they owned/leased/rented, or a shared family computer from online security threats. 46 per cent were 'confident', 26 per cent were 'neutral', 10 per cent were 'not confident' and 3 per cent were 'not confident at all'.

Comments: These results can be interpreted a number of different ways. Approximately 3 out every 5 consumers felt confident or very confident that they could effectively protect a personal computer from online security threats, which may not be reason for concern. Conversely, 2 out of every 5 consumers were less than confident, and confidence may not be a direct indicator of the ability or action taken to protect a computer.

# Appendix

Screen captures of CTN's Online Security Resources. Retrieved 21 August 2006 from <http://www.ctn.org.au/content.cfm?ContentType=Content&ContentID=219>:


Online Security Resources - The Consumers' Telecommunications Network - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://www.ctn.org.au/content.cfm?ContentType=Content&ContentID=219
Go
Links
-Many commercial software security companies provide information, including encyclopaedias, on threats, and they also provide information on their products. Such sites include Microsoft, Sophos, McAfee, Symantec and Kaspersky. Note: we are not endorsing any commercial products available on these sites.
-The Australian Consumers' Association has tested security software, including anti-virus and firewall software. (note: you must be a choice.com.au member to read this article)
REPORTING ONLINE CRIME
-The Australian High Tech Crime Centre (AHTCC), a collection of federal and state/territory police resources, has information on what constitutes an online crime, and how to report it.
MORE
-The Commonwealth Government's NetAlert provides a range of information and advice on online security.
-The Australian Consumers' Association website has a section on computer security.
Contact us if you'd like to share any suggestions about these resources.
Disclaimer -- The content on this page, including third-party links, is for your personal information only, and it not intended to be legal, product or service advice. Content on this site is not appropriate for the purposes of making a decision to carry out a transaction or trade. CTN shall not be liable for any errors, inaccuracies or delays in content.
Internet
start
Micros...
Online ...
CTN_O...
12:40 PM

# Notes and References

[1] **Spyware**

**"**Spyware is software that is installed on a computing device and takes information from it without the consent or knowledge of the user and gives that information to a third party. Spyware is an intelligence gathering tool—it is used to literally spy on people and collect information about them. People who install spyware may be targeting information such as banking and credit card details or other sensitive, commercial or private information." (p.3)

–Department of Communication, Information Technology and the Arts 2005, *Taking Care of Spyware*, Department of Communication, Information Technology and the Arts, Canberra. Available at: http://www.dcita.gov.au/ie/publications/2005/september/taking_care_of_spyware.

[2] **Computer Viruses**

"…a computer virus is a self-replicating computer program that spreads by inserting copies of itself into other executable code or documents…the insertion of a virus into the program is termed as an "infection", and the infected file, or executable code that is not part of a file, is called a "host""

–Wikipedia, "Computer Virus", *Wikipedia*, viewed 8 August 2006, <http://en.wikipedia.org/wiki/Computer_virus>.

[3] **Trojan Horses**

"Trojan horse is a malicious program that is disguised as or embedded within legitimate software. The term is derived from the classical myth of the Trojan Horse. They may look useful or interesting (or at the very least harmless) to an unsuspecting user, but are actually harmful when executed."

–Wikipedia, "Trojan horse (computing)", *Wiipedia*, viewed 8 August 2006, <http://en.wikipedia.org/wiki/Trojan_Horse_%28Computing%29#Definition>.

[4] **Worms**

"A computer worm is a self-replicating computer program similar to a computer virus…a worm is self-contained and does not need to be part of another program to propagate itself. They are often designed to exploit the file transmission capabilities found on many computers."

–Wikipedia, "Computer worm", *Wikipedia*, viewed 8 August 2006, <http://en.wikipedia.org/wiki/Computer_worms>.

[5] **Fraudulent Diallers**

**"**Dialers are necessary to connect to the internet (at least for non-broadband connections), but some dialers are designed to connect to premium-rate numbers. The providers of such dialers often search for security holes…on the user's computer and use them to change the computer to dial up through their number, pocketing the additional money for themselves. Alternatively, some dialers inform the user what it is that they are doing, with the promise of special content, accessible only via the special number."

–Wikipedia, 'Diallers – Fraudulent diallers", *Wikipedia*, 8 August 2006 <http://en.wikipedia.org/wiki/Dialler#Fraudulent_dialers>.

[6] **"Zombie" or "Botnet" computers**

"Zombie computers are machines that have been compromised by hackers to enable their use in cyber crimes and pose an imminent threat to both commercial and private users. Once compromised hackers have full access to a system and can use the computer to gather personal information or attack other networks."

–NetAlert, "Tackling Zombie Computers and Cyber Crime", *NetAlert*, viewed 14 August 2006, < http://www.netalert.net.au/02663-Tackling-Zombie-Computers-and-Cyber-Crime.asp>.

"Australia's communications regulator is fighting back against so called "zombie" computers that help to propagate internet crimes without their owners' knowledge…Zombies are compromised PCs used by hackers to form remotely controlled networks called botnets. Each botnet can consist of tens of thousands of machines and can thus pose serious threats. According to ACMA, zombies can also use internet bandwidth that broadband customers have paid for."

–Sydney Morning Herald, “Government hunts down zombies”, Sydney Morning Herald, viewed 7 November 2005, <http://www.smh.com.au/articles/2005/11/07/1131211986029.html>.

[7] **Adware**

“There is no universally accepted definition of 'Adware'. However, it is generally understood to refer to software which can: • deliver information and advertising to users; • provide information to website owners about user preferences; • help target advertising to meet a user's likely interests; and • personalise the user's online experience.”

–Coonan, H. 2006, *Industry development welcomed for online best practice guidelines* , Senator the Hon. Helen Coonan, Minister for Communications, Information Technology and the Arts, Canberra, 22 May 2006.

“Adware is software installed on a computer to deliver advertisements or other content which encourages you to purchase goods or services. It is often installed through downloading free software. With your permission, some adware may also collect information such as your web-surfing habits so that advertisements can be better targeted towards your interests.”

–Department of Communication, Information Technology and the Arts 2005, *Taking Care of Spyware*, Department of Communication, Information Technology and the Arts, Canberra. Available at: http://www.dcita.gov.au/ie/publications/2005/september/taking_care_of_spyware.

[8] **Spam**

“Spam is the common term for electronic 'junk mail' – unwanted messages sent to a person's email account or mobile phone. Spam now makes up more than 60 per cent of all email traffic, and its negative effects have become significant and far-reaching…On 10 April 2004, Australia’s anti-Spam legislation – the Spam Act 2003 came into effect. The Spam Act identifies Spam as 'unsolicited commercial electronic messages'. The Act covers email, instant messaging, SMS and MMS (text and image-based mobile phone messaging) of a commercial nature. It does not cover faxes, internet pop-ups or voice telemarketing.”

–Australian Communications and Media Authority , “What is Spam?”, *Australian Communications and Media Authority*, viewed 8 August 2006, <http://www.acma.gov.au/ACMAINTER.65636:STANDARD::pc=PC_2907>.

[9] **Phishing**

“An early form of computer hacking was used to gain illicit access to people's phone accounts and use them for illegal or expensive calls. This was called "phreaking", using the first two letters of the word "phone". It became fairly common hacker practice to replace the letter "f" with "ph" when talking about online or phone-based activities. "Phishing" is a technique used to gain personal information for purposes of identity theft, using fraudulent e-mail messages that appear to come from legitimate businesses, most commonly banks. These authentic-looking messages are designed to lure recipients into divulging personal data such as account numbers and passwords and credit card numbers.

–Department of Communication, Information Technology and the Arts, “*Phishing – don’t take the bait! – Fact Sheet*”, Department of Communication, Information Technology and the Arts, Canberra. Viewed 8 August 2006, <http://www.dcita.gov.au/ie/publications/2004/may/phishing_-_dont_take_the_bait!_-_fact_sheet>.

[10] **Potential for financial Loss from online security attacks**

“From January-September 2005, the National Fraud Information Centre in the USA reported that consumer victims of Internet scams lost an average of US$2,033, an increase of US$1,138 over the figure for 2004… In 2002 it found that Australia was ranked third highest country from which Internet fraud complaints were made, behind the United States and Canada. In 2001, Australia was ranked seventh on the list of countries from which Internet fraud perpetrators operated.”

–Australasian Consumer Fraud Taskforce, “Fraud and Corporate Crime”, *Australasian Consumer Fraud Taskforce*, viewed 10 October 2006, < http://www.aic.gov.au/research/fraud/acft/>.

“While the sampling method is limited and the results cannot be used to estimate the overall nature, extent and cost of computer crime in Australia, the Annual Computer Crime and Security Survey is an important source of information about trends among those surveyed…Thirty-five percent of respondents in the 2005 report indicated that they experienced an attack compared to 67 percent in the 2002 report. There was a rise in the estimated cost of attacks from $5.78 million in the 2002 report to $16.85 million in the 2005 report…Key findings in the 2005 report

are that financially motivated attacks are increasingly prevalent and more sophisticated, and that the ways in which offenders target vulnerabilities in operating systems and application software are not easily addressed."

–Australian Bureau of Criminology, "Computer Crime trends [CFI no.99]", *Australian Bureau of Criminology*, viewed 10 October 2006, < http://www.aic.gov.au/publications/cfi/cfi099.html>.

"Seventy percent of malicious software being circulated is linked to various types of cybercrime, a study by security firms Panda Software showed Thursday…The survey confirms a shift from several years ago, when malicious software was often aimed at garnering attention or exposing security flaws."

–Sydney Morning Herald, "Theft the motive for 70 per cent of malware', *Sydney Morning Herald* , viewed 5 May 2006, <http://www.smh.com.au/articles/2006/05/05/1146335896653.html>.

"In another example of "ransomware," a new Trojan horse threatens to delete files unless the victim pays up, security experts have warned…This is the second example of malicious software that seeks to extort money in as many months…"Our concern is that this may be the beginning of a growing trend of malware designed to extort money," Cluley [Sophos] said."

–ZDNet, "Trojan Horse: Your money or your files", *ZDNet*, viewed 1 May, 2006, < http://www.zdnet.com.au/news/security/soa/Trojan_Horse_Your_money_or_your_files/0,2000061744,39254746,00.htm>.

[11] **Internet usage in Australia**

"Just under 12.6 million Australians used the Internet in the 12 months to May 2005, 10 million…of these were online transactors"

–Department of Communication, Information Technology and the Arts 2005, "Trust and Growth in the Online Environment", *Department of Communication, Information Technology and the Arts, Canberra*. See: <http://www.dcita.gov.au/ie/benchmarking/trustandgrowth>

"The take up of broadband services has passed three million connections, according to the latest Australian Competition and Consumer Commission *Snapshot of Broadband Deployment…*"

–Australian Competition and Consumer Commission, "More than 3 million broadband services connected: ACCC", Australian Competition and Consumer Commission, news release, 23 June 2006, http://www.accc.gov.au/content/index.phtml/itemId/744386

According to November 2000 Australian Bureau of Statistics figures, 50 per cent of all adults over 18 years of age in Australia accessed the Internet (32 per cent at home). In the 12 months to November 2000, 10% of all adults in Australia purchased or ordered goods and services for private use via the Internet, and in the 3 months to November 2000,13% of all adults used the Internet to pay bills or transfer funds.

Australian Bureau of Statistics 2001, *8147.0 - Use of the Internet by Householders, Australia, Nov 2000*, Australian Bureau of Statistics, Canberra. See: <http://www.abs.gov.au/ausstats/abs@.nsf/e8ae5488b598839cca25682000131612/ae8e67619446db22ca2568a9001393f8!OpenDocument>.

[12] **Consumer concern over online security**

Security issues relating to Spam, Phishing, and viruses were the main topic of interest of a sample of over 500 Australian Seniors Computer Clubs' members surveyed in 2006.

–Australian Seniors Computer Clubs Association – Bosler, N, *Seniors' Teleommunications Issues: Their Interests and Concerns*", Australian Seniors Computer Clubs Association, 2006. See www.seniorcomputing.org.

"Only two percent of home Internet users believe the Net is safe, according to a new survey commissioned by security vendor Symantec. The survey, querying 518 people, also found that close to half of all respondents believed their banking and personal details are not safe either."

–iTnews.com.au, "Aussie consumers fearful of Net security", *iTnews.com.au*, viewed 15 March 2006, < http://www.itnews.com.au/newsstory.aspx?CIaNID=30863&r=hstory>.

[13] **Popular platforms, programs and services vulnerable to security threats**

"A new study has revealed that a staggering 83% of adults who visit social networking sites expose themselves to malicious hackers and identity thieves…The study revealed that extraordinarily high percentages of visitors to social networking sites, such as MySpace and FaceBook, are engaging in high risk security practices, which expose them to identity theft, fraud, spyware and viruses."

–Beer, S. , "Social networking sites an open door to hackers", *ITWire*, viewed 5 October 2006, <http://www.itwire.com.au/content/view/6064/53/>.

"On 8 August Microsoft released a bumper collection of security patches for 23 separate flaws in Windows and programs in the Office software suite. One of the problems identified in the August update was deemed so serious that the US Department of Homeland Security (DHS) issued a warning urging users to download the patch and apply it as soon as possible. The DHS has a role in securing America's critical infrastructure which includes the internet."

–BBC News, "Hackers target latest Windows fix", *BBC News*, viewed 17 August 2006, < http://news.bbc.co.uk/2/hi/technology/4797949.stm>.

"Microsoft has patched almost as many critical vulnerabilities in the first 8 months of 2006 as it did in 2004 and 2005 combined, security researchers said Wednesday…Thus far this year, there have been 51 security bulletins and 98 patches, 64 of which were deemed critical.'

–iTnews.com.au, "Microsoft breaks patch records", *iTnews.com.au*, viewed 14 August 2006, <http://www.itnews.com.au/newsstory.aspx?CIaNID=35778&eid=1&edate=20060811>.

"One in 600 profile pages on social networks host some form of malware, a new study has found.… Traffic to social networking sites – such as MySpace and Bebo – thought to be popular with teens, accounted for one per cent of all Web use in the workplace..."

–iTnews.com.au, "Social networks riddled with malware", *iTnews.com.au*, viewed 14 August 2006, <http://www.itnews.com.au/newsstory.aspx?CIaNID=35799&eid=3&edate=20060811>.

"Malware writers have developed worms capable of attacking all major instant messaging (IM) networks across both PC and Mac platforms, security experts warned today."

–iTnews.com.au, "'Evolved' worms target all IM networks", *iTnews.com.au*, viewed 14 August 2006, <http://www.itnews.com.au/newsstory.aspx?CIaNID=35798&eid=3&edate=20060811>.

"Apple Computer issued on Tuesday updates for its Mac OS X operating system to fix 26 security flaws."

–ZDNet, "Apple fixes 26 Mac OS flaws", *ZDNet*, viewed 3 August 2006, <http://www.zdnet.com.au/news/security/soa/Apple_fixes_26_Mac_OS_flaws/0,2000061744,39265286,00.htm>.

"Scammers are using bots to create bogus Ebay accounts that boast trustworthy profiles in a new scheme to rip off buyers, a security company said Monday."

–iTnews.com.au, "New bot-powered Ebay scam uncovered", *iTnews.com.au*, viewed 1 August 2006, <http://www.itnews.com.au/newsstory.aspx?CIaNID=35456&eid=1&edate=20060801>.

**"**Newly disclosed, unpatched flaws in three browsers could make the Web a more dangerous place to surf, security experts have warned. Security researchers published details on the bugs in Microsoft's Internet Explorer, Apple Computer's Safari and Mozilla's Firefox to security mailing lists over the weekend."

–ZDNet, "Bugs bite into popular browsers", ZDNet, viewed 26 April 2006, <http://www.zdnet.com.au/news/security/soa/Bugs_bite_into_popular_browsers/0,2000061744,39252931,00.htm>.

"A hole in Microsoft Excel has been identified that could allow attackers to take control of a computer, a security group said on Thursday."

–ZDNet, "Excel hit by another security hole", *ZDNet*, viewed 10 July 2006, <http://www.zdnet.com.au/news/security/soa/Excel_hit_by_another_security_hole/0,2000061744,39262848,00.htm>.

"…SurfControl has discovered a new blended email/internet security threat, with a fake Google banner. The email claims to be from 'Team Google' launching a new 'Google Pharmacy' service. It directs users to a pharmaceutical site for purchasing medicines. However the website harbours two malicious trojans."

–iTnews.com.au, "Cyber crims fake Google pharmacy", *iTnews.com.au*, viewed 8 June 2006, <http://www.itnews.com.au/newsstory.aspx?CIaNID=33481&eid=3&edate=20060608>.

"British website bbc.co.uk has this week become the bait for a new phishing campaign aimed at stealing sensitive security data from computer users by exploiting an Internet Explorer flaw."

–Sydney Mornign Herald, "BBC News delivers security threats", *Sydney Morning Herald*, viewed April 3 2006, <http://www.smh.com.au/articles/2006/04/03/1143916454970.html>.

**[14] New services and technologies affected by security threats**

"In a third and final report on Windows Vista, Symantec examined the security of the operating system core and found some vulnerabilities."

–ZDNet Australia, "Symantec picks away at Vista's core", *ZDNet Australia*, viewed 10 August 2006, <http://www.zdnet.com.au/news/security/soa/Symantec_picks_away_at_Vista_s_core/0,2000061744,39266028,00.htm>.

"Some computers with wireless internet capabilities are vulnerable to attacks that could expose passwords, bank account details and other sensitive information even if the machines aren't actually online…"

–Sydney Morning Herald, "Hacker exposes security flaw in wireless computers", *Sydney Morning Herarld*, viewed 3 August 2006, <http://www.smh.com.au/news/wireless--broadband/hacker-exposes-security-flaw-in-wireless-computers/2006/08/03/1154198254214.html>.

"The Australian Tax Office confirmed yesterday that 178 taxpayers had unwittingly revealed their tax file numbers while lodging tax returns online…"

–Sydney Morning Hearald, "Identity theft virus infects 10,000 computers", *Syndey Morning Herald*, viewed 3 August 2006, "http://www.smh.com.au/news/security/identity-theft-virus-infects-10000-computers/2006/08/03/1154198244503.html>.

"Online scammers have found a new way of tricking computer users into handing over their secure banking details, this time by using internet telephone networks."

–Sydney Morning Herald, "VoIP new target for financial fraudsters", *Sydney Morning Herald*, viewed 19 July 2006. <http://www.smh.com.au/news/security/voip-new-target-for-financial-fraudsters/2006/07/19/1153166440371.html>.

"The first real mobile phone virus, which was found in the wild and could replicate on its own, was discovered almost two years ago… At AusCERT, Hyppönen [Finnish anti-virus firm F-Secure]…explained that malware aimed at mobile phones is close to evolving into something that could make cybercriminals lots of money."

–Zdnet, "First mobile phone virus nears 2nd birthday", *ZDNet Australia*, viewed 30 May 2006, < http://www.zdnet.com.au/news/security/soa/First_mobile_phone_virus_nears_2nd_birthday/0,2000061744,39257470,00.htm>.

"VoIP provider Skype rolled out an update on Friday to quash a bug that can let attackers send a file to a recipient without his or her consent, and potentially obtain access to the computer and its data."

–iTnews.com.au, "Skype sick with bad bug, must be patched", *iTnews.com.au*, viewed 22 May 2006, <http://www.itnews.com.au/newsstory.aspx?CIaNID=32816&eid=1&edate=20060522>.

"Over-hyped security threats have made companies unnecessarily hesitant to roll out new technologies, such as Internet telephony and wireless networks, a research firm said this week."

– iTnews.com.au, "Gartner IDs 'over-hyped' security threats", *iTnews.com.au*, viewed 9 August 2005, < http://www.itnews.com.au/newsstory.aspx?CIaNID=19068>.

**[15] Security products affected by security threats or ineffective against them**

"Consumer versions of McAfee Inc.'s leading software for securing PCs are susceptible to a flaw that can expose passwords and other sensitive information stored on personal computers, researchers have said. The vulnerability affects many of McAfee's most popular consumer products…"

–Sydney Morning Herald, "McAfee security programs may expose data, researchers say", *Sydney Morning Herald*, viewed 1 August 2006, <http://www.smh.com.au/news/breaking-news/mcafee-security-programs-may-expose-data-researchers-say/2006/08/01/1154198118746.html>.

"The most popular antivirus applications on the market are rendered useless by around 80 percent of new malware, according to AusCERT…the general manager of the Australian Computer Emergency Response Team (AusCERT)…told the audience that popular desktop antivirus applications "don't work"..."So if you are running these pieces of software, eight out of 10 pieces of malicious code are going to get in," said Ingram."

–ZDNet, “Eighty percent of new malware defeats antivirus”, *ZDNet*, viewed 19 July 2006,<http://www.zdnet.com.au/news/security/soa/Eighty_percent_of_new_malware_defeats_antivirus/0,2000061744,39263949,00.htm>.

“Symantec Corp.'s leading antivirus software, which protects some of the world's largest corporations and U.S. government agencies, suffers from a flaw that lets hackers seize control of computers to steal sensitive data, delete files or implant malicious programs, researchers said on Thursday.”

–Sydney Morning Herald, “Flaw found in anti-virus program”, *Sydney Morning Herald*, viewed 26 May 2006, <http://www.smh.com.au/news/security/flaw-found-in-antivirus-program/2006/05/26/1148524847847.html>.

“According to the results of the AusCERT 2006 computer crime survey, even though 98 percent of companies used an antivirus product, almost half of them experienced a virus infection over the past year.”

–Zdnet, “Antivirus software 'is being defeated'”, *ZDNet*, viewed 23 May 2006, <http://www.zdnet.com.au/news/security/soa/Antivirus_software_is_being_defeated_/0,2000061744,39257227, 00.htm>.

“In the ultimate slap in the face, the world's largest anti-virus vendor Symantec has had its identity spoofed by a virus purveyor. A high risk malicious email, which appears to be a Symantec virus advisory, but actually is an e-mail that contains a payload that disables anti-virus updates, was discovered by another internet security services provider.”

–iTWire, “Symantec gets spoofed by virus purveyor”, *iTWire*, viewed 19 April 2006, <http://www.itwire.com.au/content/view/3955/53/>.

**[16] Constantly evolving security threats**

“Educating users to recognise potential phishing scams may no longer be an effective tool because recent attacks are so sophisticated that fraudulent sites were virtually indistinguishable from the original, according to MessageLabs.”

–Kotadia, M., “Education no longer enough to combat phishing?”, *ZDNet Australia*, viewed 20 September 2006, <http://www.zdnet.com.au/news/security/soa/Education_no_longer_enough_to_combat_phishing_/0,130061744,339271203,00.htm>.

“As security technologies have matured to address the types of flaws typically exploited by traditional attacks, attackers have shifted their focus to new attack vectors. Further, as technological solutions are proving increasingly more effective, attackers are reverting to older, non-technical means of compromise, such as social engineering, in order to launch successful attacks.1 Attackers are thus shifting attack activity away from network infrastructures and operating system services toward attacks that focus on the end user as the weakest link in the security chain.”

–Symantec, “Symantec Internet Security Threat Report – Trends Janaury 06 – June 06”, Volume X, September 2006. See: < http://www.symantec.com/specprog/threatreport/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf>.

“In three years phishing has transformed from an unknown threat into a multi-million dollar industry; in the next stage of their evolution, phishers will be able to avoid sending spam and bypass anti-phishing tools by hijacking small parts of 'trusted' Web sites.”

–ZDNet Australia, “Web 2.0 makes phishing spam obsolete”, ZDNet Australia, viewed 12 September 2006, <http://www.zdnet.com.au/blogs/securifythis/soa/Web_2_0_makes_phishing_spam_obsolete/0,139033343,339270982,00.htm>.

“In the never-ending cat-and-mouse game between hackers and those charged with stopping them, it's pretty clear who's winning--and it's not the cat. Speaking at the Black Hat conference in Las Vegas last week, Kevin Mandia, president of Mandiant…[a] security consultancy, said attackers are using increasingly sophisticated methods to evade detection and make life difficult for security incident response teams.”

–iTwire.com.au, “Hacker sophistication outpacing forensics”, *iTwire,com.au*, viewed 10 August 2006, <http://www.itnews.com.au/newsstory.aspx?CIaNID=35748&eid=3&edate=20060810>.

**[17] Consumer research on Internet auctions**

See: Moustakas, N 2006, “Online auctions: user protection and liability issues”, *Communications Law Centre*, Melbourne. Available at: http://www.comslaw.org.au/auction/

[18] **Confusing security terminology**

"Anti virus vendors historically pick a name for each piece of malware that they detect. As different vendors assign different names, end users can get confused when malware outbreaks are covered in the media."

–iTnews.com.au, "Security sector rethinks common virus names", *iTnews.com.au*, viewed 21 July 2006, <http://www.itnews.com.au/newsstory.aspx?CIaNID=35099&eid=1&edate=20060721>.

[19] **Size of the Internet security market**

"The global Internet security market is estimated to be about $27.7 billion in 2005 and is expected to rise at an average annual growth rate (AAGR) of 16.0%, reaching $58 billion by 2010."

–BCC Research, "SAS012 Internet Security", *BCC Research*, viewed 20 September 2006, <http://www.bccresearch.com/sas/SAS012A.asp>.

[20] **Spam Act 2003 and Government's international efforts on Spam**

For draft of legislation see:
http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/current/bytitle/7C84FF3ED0D0FC13CA256FE70083B9A1?OpenDocument&mostrecent=1

See also DCITA Spam website: http://www.dcita.gov.au/ie/spam_home

See also: "A Perth-based company has been fined $5.5 million for sending millions of unsolicited emails, with a judge labelling the spam annoying, costly to combat, and a threat to the internet. It is the first time an Australian company has been fined under the the federal government's spam laws, introduced in April 2004."

Sydney Morning Herald, "Hefty fine for spammer who sent 75m emails", *Sydney Morning Herald*, viewed 28 October 2006, < http://www.smh.com.au/news/security/hefty-fine-for-spammer/2006/10/29/1162056871608.html>.

See also DCITA International action on Spam: "Spam is a global problem that requires a global solution. International cooperation is a vital part of the Australian multi-layered approach to Spam. Since the introduction of the Spam Act, the Australian Government has established a number of international anti-Spam information sharing and enforcement arrangements with other governments and agencies."

Department of Communications, Information Technology and the Arts, "Spam International", *Department of Communications, Information Technology and the Arts*, viewed 4 September 2006, <http://www.dcita.gov.au/ie/spam_home/spam_international>.

[21] **ACMA's SpamMATTERS system**

**"**ACMA has implemented the SpamMATTERS reporting and forensic analysis system to help fight Spam. A SpamMATTERS reporting 'button' is available for download and installation into the Microsoft Outlook and Outlook Express email programs. Once installed, users can simultaneously delete their Spam and report it to ACMA with one click of their mouse. Spam reported using the button is forensically intact and contains the information that ACMA needs to track down spammers and take action against them. "

–Australian Communications and Media Authority (ACMA), "SpamMATTERS – ACMA's spam reporting system", *ACMA*, viewed 17 August 2006, <http://www.acma.gov.au/ACMAINTER.196832:STANDARD::pc=PC_100097>. [Note: you can download SpamMatters at this site].

**"**In the three months since ACMA officially launched the SpamMATTERS spam reporting 'button', there have been more than seven million reports of spam from the general public. Since the launch on 30 May 2006, more than 102,000 individual submitters have reported spam using the button."

– Australian Communications and Media Authority (ACMA), "SpamMATTERS takes off", *ACMAsphere*, Issue 12, September 2006. See:

< http://www.acma.gov.au/ACMAINTER.852114:STANDARD::pc=PC_100794#6>.

[22] Coonan, Sen Hon H, 2005, *Outcome of spyware review announced*, media release, Senator the Hon. Helen Coonan, Minister for Communications, Information Technology and the Arts, Canberra, 22 March. <http://www.minister.dcita.gov.au/media/media_releases/outcome_of_spyware_review_announced>.

See also: Government Spyware review <http://www.dcita.gov.au/__data/assets/pdf_file/24939/Outcome_of_Review_of_the_Legislative_Framework_on_Spyware.pdf>

See also: DCITA Spyware website <http://www.dcita.gov.au/ie/spyware>.

[23] **Development of Adware Guidelines**

"The Minister for Communications, Information Technology and the Arts, Senator Helen Coonan, today welcomed the Australian Direct Marketing Association (ADMA) and the Internet Industry Association's (IIA) proposed collaboration to develop industry guidelines for the online marketers and website operators use of 'Adware'. "I am encouraged to see industry taking a lead in the development of best practice guidelines in this area," Senator Coonan said. "Consumers are unclear on some aspects of how these technologies are used. The work of ADMA and the IIA is a useful contribution to removing this uncertainty in the minds of Australian businesses and consumers."

> –Coonan, H., 2006, *Industry development welcomed for online best practice guidelines*, media release, Senator the Hon. Helen Coonan, Minister for Communications, Information Technology and the Arts, Canberra, 22 May.

[24] See: <http://www.scamwatch.gov.au/>

[25] See: <http://www.auscert.org.au>

[26] See: <http://www.ahtcc.gov.au/>

[27] See: <http://www.netalert.net.au>

[28] **Launch of www.staysmartonline.gov.au**

"The Minister for Communications, Information Technology and the Arts, Senator Helen Coonan, today launched National E-Security Awareness Week, 23–27 October 2006, to encourage Internet users to 'stay smart online'. "The Internet is increasingly part of our home and business lives, from banking and shopping, to communicating with family and friends," Senator Coonan said. "We all need to think about security when we set up our computers and in our behaviour when online. National E-Security Awareness Week has activities and useful information about online security, for businesses and home users of all ages. "As part of National E-Security Awareness Week, I am delighted to launch a new website *www.staysmartonline.gov.au*, for Internet users. It has simple advice on how to secure computers, transact and interact safely online. "

> –Coonan, H., 2006, *Launch of collaborative online security initiative*, media release, Senator the Hon. Helen Coonan, Minister for Communications, Information Technology and the Arts, Canberra, 23 October.

[29] Department of Communication, Information Technology and the Arts (DCITA) 2005, *Trust and Growth in the Online Environment*, Department of Communication, Information Technology and the Arts, Canberra. Available at: http://www.dcita.gov.au/ie/benchmarking/trustandgrowth

[30] Department of Communication, Information Technology and the Arts (DCITA) 2006, *Trust and Growth in the Online Environment*, Department of Communication, Information Technology and the Arts, Canberra, prepared by the Centre for International Economics, and Edgar, Dunn & Company, June. Available at: http://www.dcita.gov.au/__data/assets/pdf_file/40522/Exploration_of_Future_Electronic_Payments_Markets.pdf

[31] **8 Basic Consumer Rights**

As adopted by the United Nations Assembly on 9 April 1985: The right to safety, The right to be informed, The right to choose, The right to be heard, The right to satisfaction of basic needs, The right to redress, The right to consumer education, and The right to a healthy environment.
See: < http://www.fairtrading.qld.gov.au/oft/oftweb.nsf/web+pages/ABDDDDD88B517CA84A256B410081D4C2?OpenDocument > and <http://www.un.org/documents/ga/res/39/a39r248.htm>.

[32] According to June 2005 Australian Bureau of Statistics figures, 26 per cent of the Australian population was 0-19 years of age, 14 per cent were 20-29, 15 per cent were 30-39, 15 per cent were 40-49, 13 per cent were 50-59, 8 per cent were 60-69, and 9 per cent were 70 and over.

Australian Bureau of Statistics 2005, *3235.0.55.001 – Population by Age and Sex, Australia – Electronic Delivery, Jun 2005*, viewed 25 July 2006, <http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/3235.0.55.001Main+Features1Jun%202005?OpenDocument>.

[33] According to November 2000 Australian Bureau of Statistics figures, 74 per cent of the Australian population between 18 and 24 accessed the Internet in the 12 months to November 2000.

Australian Bureau of Statistics 2001, *8147.0 - Use of the Internet by Householders, Australia, Nov 2000*, Australian Bureau of Statistics, Canberra. See: <http://www.abs.gov.au/ausstats/abs@.nsf/e8ae5488b598839cca25682000131612/ae8e67619446db22ca2568a9001393f8!OpenDocument>.

[34] According to June 2005 Australian Bureau of Statistics figures, 50.26 per cent of the Australian population was female, and 49.74 per cent was male.

Australian Bureau of Statistics 2005, "3235.0.55.001 – Population by Age and Sex, Australia – Electronic Delivery, Jun 2005", viewed 25 July 2006, <http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/3235.0.55.001Main+Features1Jun%202005?OpenDocument>.

[35] According to December 2005 Australian Bureau of Statistic figures, 33 per cent of Australians live in NSW, 25 per cent in VIC, 20 per cent in QLD, 10 per cent in WA, 8 per cent in SA, 2 per cent in the ACT, 2 per cent in TAS and 1 per cent in the NT.

Australian Bureau of Statistics 2005, "3101.0 - Australian Demographic Statistics, Dec 2005", viewed 25 July 2006, <http://www.abs.gov.au/ausstats/abs@.nsf/0e5fa1cc95cd093c4a2568110007852b/6949409dc8b8fb92ca256bc60001b3d1!OpenDocument>.

[36] According to 2004 Australian Bureau of Statistics figures, 65 per cent of Australians lived in "major urban areas', 22 per cent in 'other urban' areas, and 12.9 per cent in 'bounded localities' or 'rural balances'.

Australian Bureau of Statistics 2004, *Census of Population and Housing – 2032.0 Australia in Profile – A regional Analysis 2001*, *Australian Bureau of Statistics*, Australian Bureau of Statistics, Canberra. See: <http://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/2032.02001?OpenDocument>.

[37] **Importance of software patches**

"In the first six months of 2006, 80% of vulnerabilities were considered easily exploitable, up from 79%."

–Symantec, "Symantec Internet Security Threat Report – Trends Janaury 06 – June 06", Volume X, September 2006. See: < http://www.symantec.com/specprog/threatreport/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf>.

"The study…analyzed the security performance of commonly-used computer platforms against Internet attacks in the wild when running on the default security settings designated by vendors. The study revealed that…[t]he regular Windows XP Service Pack 1 system without a third-party firewall was the most vulnerable, and was successfully compromised by an attack within four minutes of first plugging into the Internet… "The majority of home PCs are running some form of Windows-based platform and it is important for them to know that the moment they connect to the Internet, they are almost immediately under some form of Internet attack," said Marcus Colombano, partner at Avantgarde and co-investigator of this experiment."

–Avantgarde, "Automated "Bots" Overtake PCs Without Firewalls Within 4 Minutes", Media Release, viewed 31 August 2006, < http://www.avantgarde.com/ttln113004.html>.

[38] **Size of software patches**

Microsoft's Service Pack 2 update was over 79 Megabytes.
See: <http://www.microsoft.com/windowsxp/sp2/default.mspx>

[39] **Choice of operating systems and software**

"Security vendor Symantec has accused Microsoft of abusing its monopoly in deciding which security products can run on its upcoming operating system. Symantec said Microsoft, which started selling its own security products in May, is deliberately withholding information needed to develop products that work on Windows Vista."

> –Sydney Morning Herald, "Microsoft accused of abuse of power", *Sydney Morning Herald*, viewed 28 September 2006, <http://www.smh.com.au/news/security/microsoft-accused-of-of-abuse-of-power/2006/09/28/1159337262813.html>.

"Due to Microsoft's extensive licensing agreements with many computer vendors, Windows presently comes pre-installed on most computers as a bundled OEM version, making it the default choice for most of the market. For some consumers, Windows is the only valid option for a computing environment, or it is mandated by their workplace; additionally, an unfamiliarity with other operating systems results in a lack of desire to switch to other operating systems. Finally, the large base of proprietary software available exclusively for the Windows family of operating systems has become a large reason for the popularity of Windows, at least partly because many users do ot realize that there are free, open source, and portable alternatives available."

> –Wikipedia, "Microsoft Windows", *Wikipedia*, viewed 31 August 2006, <http://en.wikipedia.org/wiki/Microsoft_Windows>.

"Microsoft has been hit with yet another antitrust claim, this time from a partner that alleges that the software vendor abused its market dominance to extract exorbitant fees from OEMs, distributors and resellers for its operating system licenses…Tangent alleged further that Microsoft entered into restrictive agreements with OEMs and system builders, limiting or eliminating their ability to feature non-Microsoft products. Tangent builds configured-to-order desktops, notebooks and servers for educational institutions, government agencies and enterprises, using Microsoft Operating Systems."

> –Hazard, J., "Tangent Suit Claims Microsoft Soaked Partners" , *E-Week Channel Insider*, viewed 31 August 2006, <http://www.thechannelinsider.com/article/Tangent+Suit+Claims+Microsoft+Soaked+Partners/171923_1.aspx>.

[40] **Rootkits**

**"**A rootkit is a set of software tools intended to conceal running processes, files or system data, thereby helping an intruder to maintain access to a system whilst avoiding detection. Rootkits are known to exist for a variety of operating systems such as Linux, Solaris and versions of Microsoft Windows. Rootkits often modify parts of the operating system or install themselves as drivers or kernel modules."

> –Wikipedia, "Rootkit", *Wikipedia*, viewed 31 August 2006, < http://en.wikipedia.org/wiki/Rootkit>.

[41] **Government action on diallers**

"Telstra terminated all contracts it previously held with providers of Internet diallers using 190 numbers on 25 August 2003. As a result, Internet diallers are no longer available on 190 numbers and Telstra no longer acts as a billing agent for these services. Further, the major service providers have voluntarily barred direct dial access to a number of overseas countries associated with Internet dialler services and share information about these services under a protocol developed by the Australian Communications Industry Forum (ACIF), thereby enhancing the effectiveness of the barring measures. The result is that complaints to the Telecommunications Industry Ombudsman (TIO) about Internet diallers have fallen to historically low levels….In August 2005, the Minister wrote to the CEOs of each major service provider to make it clear that the Government expects the industry to develop an effective registered code of practice dealing with consumer credit management issues without delay, or more direct action would be considered by the Government. In response, ACIF released a draft revised Credit Management code in October 2005…"

> –Department of Communications, Information Technology and the Arts, "Internet Dumping and Internet Diallers – Frequently Asked Questions", *Department of Communications, Information Technology and the Arts*, viewed 31 August 2006, <http://www.dcita.gov.au/tel/faqs/consumer_rights_and_benefits/faq_-_internet_dumping_and_internet_dialler_software#3>.

[42] **National Filter Scheme**

"The Government will create a National Filter Scheme to provide every Australian family with a free Internet filter as part of a $116.6 million comprehensive package of measures to crack down on the scourge of Internet pornography, the Minister for Communications, Information Technology and the Arts, Senator Helen Coonan, announced today.

The National Filter Scheme is the centrepiece of the Australian Government's Protecting Families Online package. Protecting Families Online will also include measures to provide Australian libraries with free filters so computer corners at libraries across Australia will become child-friendly zones."

–Coonan, H., 2006, *$116.6 fo Protect Australian Families Online*, media release, Senator the Hon. Helen Coonan, Minister for Communications, Information Technology and the Arts, Canberra, 21 June.

**[43] Free v Paid security products**

"Microsoft gives away a security firewall with its latest operating system. Many high-speed Internet service providers offer free anti-virus protection for subscribers. And several websites distribute free toolbars to warn of web scams. AOL even recently made a package of basic security tools — anti-virus, anti-spyware and firewall programs — available for free to anyone, not just paying subscribers. Despite all the free protection, primarily for Windows computers, leading security vendors are moving forward with plans to start selling their annual slate of security products this (northern hemisphere) autumn. Why bother, when so much is available elsewhere at no cost?"

–Sydney Morning Herald, "Securing your PC: free v paid", *Sydney Morning Herald*, viewed 18 September 2006, < http://www.smh.com.au/news/security/securing-your-pc-free-v-paid/2006/09/18/1158431614729.html>.

**[44] Research on how phishing can fool consumers**

Dhamija, R, Tygar, J.D., Hearst, M., "How Phishing Works", research paper, Harvard, UC Berkeley, viewed 4 April, 2006., <http://people.deas.harvard.edu/~rachna/papers/why_phishing_works.pdf>.

See also: ZDNet Australia, "The secret of phishers' success", *ZDNet Australia*, viewed 4 April 2006, <http://www.zdnet.com.au/news/security/soa/The_secret_of_phishers_success/0,2000061744,39249547,00.htm>.

**[45] Privacy and Adware**

"Advertisers want to know all about our online habits but some of the information gathering goes too far, writes Claire Doble…Electronic Frontiers Australia, among other civil liberties groups, warns that "profiling" is a big concern. "The issue is when organisations are collecting information without the consent of the individual and using it for purposes the individual hasn't consented to," says its executive director, Irene Graham."

–Doble, C., "Every click you make, they'll be watching you", *Sydney Morning Herald*, viewed 30 September 2006, < http://www.smh.com.au/news/biztech/every-click-you-make-theyll-be-watching/2006/09/26/1159036543260.html>.

"Eight of the top ten reported security risks were adware programs…Three of the top ten new security risks are what Symantec calls "misleading applications."

–Symantec, "Symantec Internet Security Threat Report – Trends Janaury 06 – June 06", Volume X, September 2006. See: < http://www.symantec.com/specprog/threatreport/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf>.

"Millions of Windows users may unwittingly be test subjects for an unfinished Microsoft antipiracy tool. The software maker has been delivering a pre-release version of Windows Genuine Advantage Notifications software to PCs as a "high priority" item in the built-in update feature in Windows…But some security experts are troubled by Microsoft's decision to deliver pre-release software to millions of Windows users without clearly notifying them. People may not realise they are participating in a trial and have in essence become unsuspecting guinea pigs, they said…Indeed, most consumers won't know what to do when Automatic Updates offers them the piracy tool and thus will simply accept it, said Michael Silver, a Gartner analyst."

–ZDNet Australia, "Microsoft draws fire for stealth test program", *ZDNet Australia*, viewed 14 June 2006,<http://www.zdnet.com.au/news/security/soa/Microsoft_draws_fire_for_stealth_test_program/0,2000061744,39259767,00.htm>.

**[46] Police enforcement of computer crimes**

"Flawed police protocols and holes in the official crime database have contributed to widespread under-reporting of e-crimes, according to new research. Many Victorian police - including members of the major fraud squad - have not read the 2003 Computer Offences Act, Melbourne University doctorate student Shane McKenzie has found. Also, several of the act's offences are not coded into the Victoria Police Law Enforcement Assistance Program (LEAP) database , so charges for these offences cannot be pursued. Mr McKenzie presented results from his PhD research on the investigation of electronic crime last week. He interviewed 42 police and private investigators and

was given access to LEAP database records on 3529 cleared e-crime incidents from 1999 to 2004. More than half of the e-crimes were classified as deception, and another quarter were crimes of harassment. However, it is hard to find a sympathetic ear when reporting e-crimes, Mr McKenzie says."

–Sydney Morning Herald, "E-crims slipping through the net", *Sydney Morning Herald*, viewed 8 August 2006, < http://www.smh.com.au/news/security/ecrims-slipping-through-the-net/2006/08/07/1154802814943.html>. *Note, there is a correction to this story given at the website listed.