



Australian Government

Department of Communications,
Information Technology and the Arts

TRUST AND GROWTH IN THE ONLINE ENVIRONMENT



TRUST AND GROWTH IN THE ONLINE ENVIRONMENT

November 2005

© Commonwealth of Australia 2005

ISBN 0 642 75330 X

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the Commonwealth available from the Department of Communications, Information Technology and the Arts.

Requests and inquiries concerning reproduction and rights should be addressed to:

Attorney General's Department
Robert Garran Offices
National Circuit
Canberra ACT 2600

or posted at <http://www.ag.gov.au/cca>

Foreword

A growing majority of Australians are enjoying the many benefits arising from the Internet. As the online environment has developed, the Australian Government has been actively raising the awareness of safe and secure online practices.

Building consumer confidence and trust in online services is critical to ensuring that all Australians are able to realise the full benefits of the Internet. Trust and security are identified as major priorities in *Australia's Strategic Framework for the Information Economy 2004–2006* and the Australian Government has initiated a range of activities in the areas of online trust, security, authentication and related issues. Awareness raising of secure and safe online practices is a critical part of this work.

This report, *Trust and growth in the online environment*, presents the results of a survey of the perceptions, experiences and security practices of Australians transacting online. It will make a significant contribution to raising awareness of online trust issues amongst providers and users of online services and will contribute to international research in this area.



Senator the Hon. Helen Coonan

Minister for Communications, Information Technology and the Arts



Table of contents

Foreword	iii
Overview	1
The growth of the online economy	1
Passive versus active Internet users	1
Concerns with transacting or providing information online	2
The online transaction experience	2
Protective measures adopted online	2
Introduction	3
Trust and security.....	3
Towards the development of trust related indicators	6
Australia’s online community and contextual setting	11
Online consumer trust – exploratory measures and findings	17
Survey methodology	17
Definitional issues.....	17
Information on the tables provided in the report	18
Passive and active Internet users.....	18
Active users—multiple activities	20
Concerns	23
Online experiences.....	25
Protective responses.....	27
Why transact online?	32
Endnotes	34

List of Figures

Figure 1	Dimensions of measuring online trust	8
Figure 2	Australians' attitude to technology: technology makes life easier, April 2005 (Nielsen//NetRatings)	12
Figure 3	Online banking (Nielsen//NetRatings)	13
Figure 4	Buying, selling and bill payment (Nielsen//NetRatings)	14
Figure 5	Paying bills online (Nielsen//NetRatings).....	14
Figure 6	Online shopping and bill payment activities by age and location, April 2005 (Nielsen//NetRatings)	15
Figure 7	Home Internet users using broadband technology, Australia (Nielsen//NetRatings).....	15
Figure 8	Impact of broadband on users, April 2005 (Nielsen//NetRatings)	16
Figure 9	What Internet users do online, May 2005 (Sensis)	18
Figure 10	Those who perform a single transaction by type.....	21
Figure 11	Transaction levels by high and low household income ranges	21
Figure 12	Transaction levels by age	22
Figure 13	Security measures undertaken by number of types of transactions performed.....	30

List of Tables

Table 1	Indicative indicators for measuring multi-dimensional aspects of trust.....	9
Table 2	Top 10 online activities, April 2005	12
Table 3	Projected number of Australians in various groups from weighted survey responses.....	17
Table 4	Per cent of passive and active Internet users by household income.....	19
Table 5	Working status of passive and active Internet users.....	20
Table 6	Percentage of active transactors	20
Table 7	Top 10 online concerns	23
Table 8	Top 5 concerns, by transaction level	24
Table 9	Online experiences of active users	26
Table 10	Online experiences by number of transaction types undertaken	26
Table 11	Protective measures undertaken by active users	28
Table 12	Protective measures by number of transaction types undertaken.....	29
Table 13	Single versus multi security measures—active users	30
Table 14	How users ensure online security for those who order, book or pay online	31
Table 15	Why active users transact online.....	32
Table 16	Reasons for transacting online by number of types of transactions undertaken	33

Overview

This report, *Trust and growth in the online environment*, presents the main findings from a recent survey investigating the perceptions and behaviours of online Australians with specific focus on persons choosing to transact online. The report sheds some light on a number of key issues relating to online consumer trust, including:

- the level of adoption of transaction-based activities; banking, bill payment, shopping and the provision of personal information;
- the reasons for transacting online;
- the intensity of online transactions;
- perceptions of the security or risks associated with transacting online; and
- online security practices.

The Sensis survey was a quota sample of 1500 respondents aged 14 years and over, weighted on the basis of 2001 Population Census data to reflect the structure of the general Australian population.

The growth of the online economy

The growing intensity of online activity in Australia is demonstrated by the fact that online Australians viewed 4.2 billion web pages in January 2003. Over a period of two years this figure has doubled to 8.1 billion web pages. While the majority of online activity has been associated with email and information gathering, the Internet is fast becoming a medium for e-commerce.

The patronage of online transaction services such as banking, bill payment, shopping, etc has grown enormously in Australia over the past four years, faster than any other category of online activity; an estimated 17–20 per cent per annum growth since September 2001.

Passive versus active Internet users

Despite the perception that Australians are wary of the Internet, the report found that the overwhelming majority of online Australians now use the Internet for some form of transaction. Just under 12.6 million Australians used the Internet in the 12 months to May 2005, 10 million (over 79 per cent) of these were online transactors (or as termed in this report, active Internet users); undertaking purchases, paying bills, banking or supplying personal information online.

For many users of the Internet, transacting online is about convenience, cost and necessity. Nearly 48 per cent of active Internet users reported convenience as a factor in influencing their decision to transact online, compared to 27 per cent reporting cost of service (cheaper). A further 16 per cent of transactors reported alternatives to the online transaction service not being available and 14 per cent reported factors associated with the location of the online service provider.

Active Internet users are more likely to live in relatively high income households compared to passive Internet users. The survey found that just under 53 per cent of active users were in households with incomes of more than \$55 000 per annum compared to 26 per cent for passive users (those who reported using the Internet in the last 12 months but did not perform any type of online transaction). Nearly 31 per cent of active users resided in households with incomes of more than \$85 000 compared to only seven per cent for passive users. However, possibly reflecting the broad level appeal of online transaction services such as shopping, active Internet users outnumbered passive Internet users across socio-economic variables such as income and labour force status.

Most active Internet users in Australia made use of multiple online transaction services. Just over 80 per cent of active Internet users performed more than one type of transaction online and just over a third completed all types of transactions; single transactors more often (61 per cent) making use of online shopping services.

Concerns with transacting or providing information online

While the majority of Internet users in Australia have chosen to transact online, general security of the Internet was the number one concern identified by both active and passive Internet users, (54 and 55 per cent respectively). Other concerns identified included:

- the potential for fraud (23 and 17 per cent respectively);
- privacy concerns (20 and 17 per cent respectively);
- misuse of personal information (9 and 14 per cent respectively); and
- providing personal information (13 and 9 per cent respectively).

However, perhaps reflective of their experience with transacting online, active Internet users in general, had a lower level of concern than their passive counterparts. Twenty per cent of active Internet users reported having no concerns about transacting or providing information online compared to 15 per cent for passive users. This was further reinforced by the fact that the lowest level of concern was expressed by Internet users engaged in the use of multiple transaction services.

The online transaction experience

The online experience of active Internet users appears to be little different to passive Internet users. When asked about any online security incident or breach, the majority of active users reported either receiving unsolicited material via email or a virus attack (79 and 66 per cent respectively); a common experience for Internet users in general and one not exclusively attributed to transacting online. However, online transactors did report incidences associated with transacting online, albeit at a much lower level than expected:

- 13 per cent of active Internet users reported suffering a breach of privacy;
- 6 per cent reported not receiving an online purchase;
- 5 per cent received sub-standard goods; and
- 4 per cent reported losing money due to online fraud.

Nearly 10 per cent of active transactors reported no incident. With the exception of receiving spam or experiencing a virus attack, the proportion of active Internet users reporting a particular incident remained unchanged for users of multiple transaction services.

Protective measures adopted online

Australians transacting online generally adopted a minimalist approach to securing online transactions. These results were surprising given that the survey showed that the overwhelming majority of transactors had concerns with the security of the Internet:

- 32 per cent of active Internet users reported regularly updating virus or worm protection software;
- 18 per cent looked for sites with 'trustmarks';
- 15 per cent only dealt with well known service providers; and
- only 14 per cent used a firewall service.

The generally low level of responses across the categories indicates that:

- 35 per cent of active Internet users adopted multiple measures to secure online transactions;
- 49 per cent reported a single security measure;
- 7 per cent reported doing nothing; and
- 9 per cent didn't know.

However, the level of protective measures adopted increased significantly for users of multiple transaction services.

These findings and others are explored more fully in the following chapters.

Introduction

The Australian information economy continues to grow strongly, underpinned by a high level of investment in information and communications technology (ICT)¹ and high levels of online participation by governments, businesses, institutions and society generally. The impacts of ICT usage are diverse, contributing to organisational transformation, product and service innovation, innovations in the organisation and distribution of information, and the emergence of an increasingly tech-savvy population that are accepting of an array of fixed and mobile technologies. Key amongst these is the Internet.

The Internet is transforming how Australians undertake day-to-day activities such as communicating, information gathering, transacting, accessing video and audio streaming (including podcasts) as well as a variety of interactive services from online games to education. For the past five years Australia has experienced comparatively high levels of growth in home Internet connectivity resulting in the emergence of a sizeable population of Internet users with a growing level of online experience.

Australians are increasingly active in the use of the Internet and see the opportunities it holds as an information and service resource. In this environment there is a growing recognition that increasing reliance on the Internet has implications for government policy. In order to ensure all Australians are able to realise the full benefits of the information economy, it is critical to build and enhance trust in online information and services. The Australian Government has carried out a range of work in the areas of trust, security, authentication and related issues, pertaining to the online environment. Trust and security are identified as major priorities in *Australia's Strategic Framework for the Information Economy 2004–2006*.

The Department of Communications, Information Technology and the Arts (the Department) has embarked on research into issues associated with building greater consumer trust in the online environment, focusing on the development of trust indicators and surveys. Trust measurement work will bring greater depth to the range of information economy data now available. In focusing on measurement issues such as trust, the Department is seeking to move beyond the established model for measuring Australia's progress in the information economy, i.e. readiness (take up), intensity and

impact. New measures such as the perception of trust and the degree to which trust is an inhibitor or barrier to e-commerce and other online activities are seen as important issues. The Department will also undertake focus group studies to explore trust issues in more detail.

The Department's work also feeds into developments in the OECD, including the OECD's Working Party on Information Security and Privacy (WPISP). As part of its work program to *Build User Trust in the Global Digital Economy*, WPISP identified the need to explore the feasibility and usefulness of improving and developing new indicators to measure trust online.

Trust and security

The Australian Government has carried out a range of work in the online environment in the areas of trust, security, authentication and related issues. One of the four priorities in *Australia's Strategic Framework for the Information Economy 2004–2006* is to ensure the security and inter-operability of Australia's information infrastructure, and support confidence in digital services.

The OECD² has also commented that there is a:

need to develop new indicators in areas that are inherently difficult to measure, because the concepts are yet undefined,

and note that

the issue of trust in online environments is multifaceted and would benefit from a comprehensive framework for empirical analysis.

The issue of trust in online activities is one that shapes how people and organisations use and respond to the online environment on the one hand and how businesses and governments seek to engender trust on the other hand. This is an issue of increasing importance given the growing intensity of online activity in Australia. In January 2005, online Australians viewed an estimated 8.1 billion web pages, up from 5.6 billion in January 2004, 4.2 billion in January 2003 and 2.9 billion in February 2002.³

There are also legal and policy issues associated with aspects of trust, particularly in areas that represent a threat to privacy, wellbeing, e-commerce security, infrastructure security or national security generally.

Some of the threats to trust are already apparent and have resulted in a range of counter measures by organisations such as the Australian High Tech Crime Centre (AHTCC), AusCert and its international affiliates, by software firms, by virus and other malware detection specialists, and by functional units in government. The nature of such attacks and threats is constantly evolving and growing in sophistication, placing an increasing emphasis on detection and countermeasure specialists around the world. It is no longer a matter of simply facing the threat of computer viruses, but increasingly the clever use of trojans, spyware, phishing, and botnets⁴.

At the same time, businesses are aware that in order to succeed in the online world, they must address trust issues as they affect clients, by taking and being seen to have taken appropriate steps to protect the interests of clients. Trust aspects are now often built into strategic business plans, and measures to increase trust are overtly featured in marketing strategies and displayed on websites.

However, trust concerns go beyond the realm of security incidents. While trust in business relationships is not new, the Internet has added a new dimension to such relationships and has introduced a greater degree of uncertainty in relation to authentication and the use of personal information. Most individuals would presumably have a degree of concern in relation to:

- the use of personal information supplied to business and government organisations;
- the ability of organisations to track and mine information from online sources; and
- in the provision of personal and 'mined' information to third parties.

Other trust concerns exist in relation to order fulfilment, uncertainties about consumer protection, legal rights and the avenues available for redress, especially when adverse situations arise involving overseas parties and jurisdictions.

In many respects, trust and security issues are entangled. While trust is a perception issue and security is a physical/technical issue, trust can be adversely affected by personal experience of a security incident or by knowledge of security incidents that may be reported in the media, including reports from overseas sources.

The effect of trust issues on individuals' and organisations' actual behaviour may result from a number of considerations including:

- levels of awareness of potential threats (or lack of awareness);
- risk assessment considerations;
- needs versus choice evaluations; and
- cost benefit considerations.

Accordingly, lack of trust is not always a barrier to engaging in various activities online, especially when convenience and the time and cost of alternatives, for example, are taken into account.

At an organisational/business level, trust (as a concept) becomes much less a personal attribute and translates more into risk management, efficiency gains and corporate security policy and practice, among other things. However, given that trust, as an attribute, is primarily associated with the human condition, our main focus in this report is on consumer trust issues in relation to Internet usage.

While there is a wide body of literature on trust, there are relatively few statistical references which give a proper perspective on trust related issues that affect Internet users. The majority of Australian studies undertaken to date are either based on focus groups or are focussed on a narrow set of issues. Among these the Australian Privacy Commissioner's 2001 study *Privacy and the Community* is arguably a landmark undertaking focussing on privacy issues. There is also some very interesting work emerging from a number of educational institutions. Swinburne University of Technology undertook a collaborative project in 2002 in conjunction with the University of Adelaide and Network Insight (RMIT), with results reported in *Trust in the Internet—The Key Bottleneck*.

Trust and security issues have been elevated in recent times by three main trends:

1. the dramatic increase in the number of Australians undertaking online transactions such as banking, shopping and bill payment over the last four and half years;
2. the increasing sophistication of security threats and scams; and
3. the shift from dial-up to broadband Internet.⁵

The increasing number of Australians transacting online exposes a wider audience to potential cyber threats. The 'always on' nature of broadband connections makes computers connected in this way more prone to abuse and more open to being utilised for malicious purposes on a wider scale. In the latter context, 'zombie'⁶ computers can be used to launch spam or denial of service attacks in a manner that is difficult to trace back to the real perpetrator. Unprotected broadband systems are also thought to be more prone to spyware and other inconspicuous 'malware' and these agents are likely to represent a much greater threat to the individual.

The lack of appropriate metrics focussing on trust and security issues has recently been given some focus in the OECD as well as by a number of Australian government organisations. The OECD has indicated that:

A fundamental element in enabling the benefits ICT can bring to economic and social development is the confidence users have in platforms, applications and services. Creating an online environment which builds trust amongst the users of ICT networks is an increasing priority for business, industry and governments and has been on the OECD agenda since the late 1990s.... There is a need to be able to use relevant data to assess the effectiveness of public and private initiatives aimed at building trust among users. This is increasingly important as access to, and use of, the Internet continues to grow across the OECD area⁷.

The OECD also makes note of the work presently being undertaken by the AHTCC in conjunction with the Australian Bureau of Statistics (ABS) to develop e-crime statistics, including an AHTCC recommendation for international collaboration regarding the development of standards and data collection methodologies.

The ABS has recently issued a *National Information Development Plan for Crime and Justice Statistics* in which it outlines the need for improved statistical information about fraud and electronic crime (e-crime) including:

- data to assist measurement of the size of the problem;
- offender information; and
- victim information, including economic impacts.

The ABS indicates that a primary information requirement is to estimate the size of fraud and e-crime in terms of economic impacts (including security costs and lost time), number of incidents, number of victims and jurisdiction of origin. A secondary information requirement is to be able to describe the characteristics of incidents including characteristics of offenders and victims.

Because of the growing interest in trust and security statistics and related issues, the Department commenced some exploratory work late in 2004 aimed at developing an analytical framework along with an indicative set of data items focussing on consumer trust of the Internet. In 2005, the Department, in collaboration with Sensis Pty Ltd, fielded a one-off set of trust and security survey questions in the ongoing Sensis Consumer Confidence Survey (a household survey of 1500 private individuals).

Towards the development of trust related indicators

There is a wide body of literature devoted to the trust issue and its definition. Some references go to extreme lengths to define the term and others point out that there is no agreed definition and cite numerous variations. In the Department's development work in this area, the primary interest is in constructing statistical indicators that identify online behaviour modification due to trust issues or signify trust-related barriers. This is somewhat different to measuring trust directly. Indirect measures imply that trust does not become a variable in its own right and accordingly a rigorous definition of trust is not required. In using the term 'trust' in our research, a simple dictionary meaning is implied: confident expectation; reliance in a person or thing without misgiving.

Many of the influences that impact on trust have been mentioned in literature dealing with the definition of trust. In many respects some of this debate arises from conflict between the common meaning of trust and the type of data required to understand how trust is impacted, that is, the analytical framework. For instance, Grandison and Sloman (circa 2000)⁸ examined the various definitions of trust that appear in literature and make a number of observations including that:

1. trust is a complex subject relating to belief in the honesty, truthfulness, competence, reliability, etc of the trusted person or service;
2. there is no consensus in the literature on what trust is, although there is agreement on its importance;
3. the lack of consensus with regard to trust has led authors to use the terms trust, authorisation and authentication interchangeably; and
4. the outcome of a trust decision is based on many things such as the trustor's propensity to trust, and their beliefs and past experiences relating to the trustee.

Chopra and Wallace⁹ comment that research often focuses narrowly on specific aspects of trust, failing to capture its multidimensional nature. They also note that trust literature also lacks clear differentiation among the factors contributing to trust. They indicate

that there is however broad agreement that trust is both a social and psychological phenomenon. The thrust of their conclusions is that trust extends from a generalised expectancy towards others based on one's cumulative experience (the psychological propensity to trust), through to specific interpersonal relationships and broader relational and societal influences that are a reflection of social capital, societal system trust and institutional trust.

With regard to these latter issues, the Department's research¹⁰ into how citizens, organisations and communities use the Internet to build communities, networks and connections concluded that:

- two of the norms pivotal to social capital are trust and reciprocity. The concepts are inherently linked, with reciprocity an underlying element of trust. Together they underpin our daily interactions and facilitate business, government and social exchanges.
- trust is central to the development of social capital in both the face-to-face and virtual realm. Trust in online communication can be enhanced by personal reputation, boundary setting, organisational reputation, ongoing interaction, formal and informal rules and leadership.

This Department research observed that trust is a developmental process. Individual trust is embedded in the personal experience and relations formed over time, and through interaction:

...norms of trust and reciprocity, level of generalised trust and reciprocity is predicted by age, relationship status, the extent to which networks are locally based, ethnicity, health, voluntary activity, tolerance of ethnic diversity, whether to live in an urban or rural area, satisfaction with the safety of one's neighbourhood and level of knowledge of local affairs.¹¹

Furthermore, various kinds of trust can be distinguished; notably *social trust* (i.e. that which is personal and emotional) and *transactional trust* (i.e. that which underlies a business or government transaction).

Transactional trust is far more purpose driven, essentially removed from any one-to-one personal or social interaction. It is generally characterised by dealings between the individual and an organisation, whether government or business, to complete a particular task or transaction. Transactional trust in this respect will vary according to the transaction because an organisation may be trusted to deliver a particular service but not others. The United States' business consultancy, Accenture, proposes that trust in the context of business development:

- is earned over time;
- can be monitored by governments but not established by them;
- is an aggregation of many people's experiences;
- can take years to establish but can be lost in an instant; and
- extends throughout the value chain.

An extensive literature and statistical review showed that trust in online transactions is closely associated with security concerns and levels of uncertainty relating to privacy, authentication, order fulfilment and dispute resolution, etc. In addition, there are many other factors that may contribute to an individual's propensity to transact or supply information online:

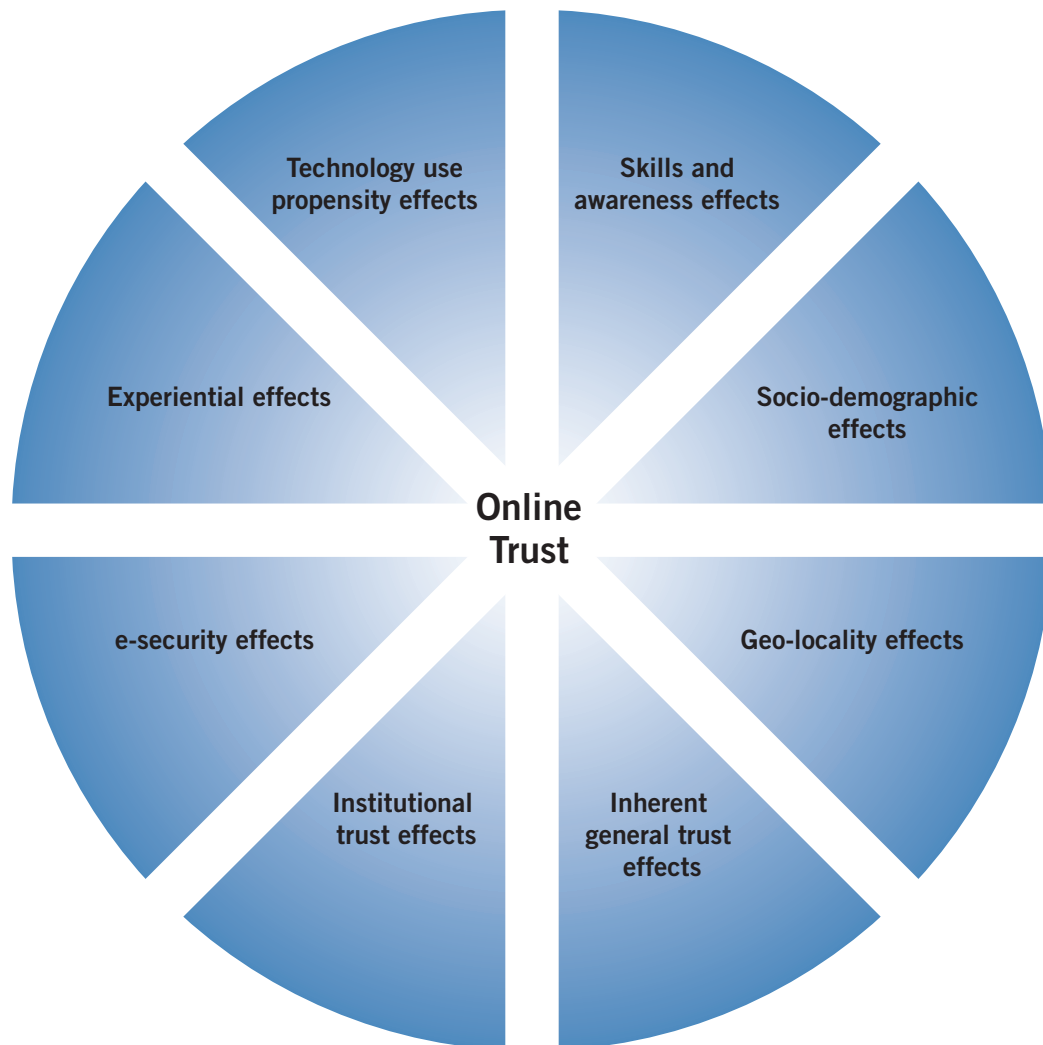
- an individual's inherent level of trust generally;
- their trust in institutions and government agencies;
- their attitude to using modern technologies and their level of experience with; and
- their ability to use computers and online systems.

Some of the concerns and experiences of consumers are reflected in the practices which are adopted to ensure or improve the integrity of transactions. It seems reasonable to suggest that good outcomes will most likely stimulate greater use of online activities while adverse experiences will most likely lead to some combination of modified online behaviour. This might include reduced confidence in the Internet as a trusted channel, reduced trust in particular merchants and organisations, and more elaborate protective measures and practices.

Further to this, there are some less often mentioned details to consider when doing an analysis of trust-related data. Socio-demographic subgroups and broad geographic differences appear to be important value scales in the analysis of trust. This was effectively demonstrated by a 2001 survey undertaken for the Office of the Federal Privacy Commissioner¹². The survey results showed that, 'younger people were less likely to demonstrate assertive privacy-related behaviour as were those with lower levels of education and those in rural areas'. The results also showed that people from lower socio-economic groups tended to register more concern about protecting their privacy. The two findings taken together indicate that while privacy concerns are high for certain segments of the population, these groups were less likely to be proactive in enacting measures to protect their privacy than others.

The multidimensional aspects of trust variously described in the literature highlights that an understanding of how trust in the online economy is shaped, impacted or influenced needs to be explored with a fairly elaborate set of data that covers some or all of the dimensions described in Figure 1.

Figure 1 Dimensions of measuring online trust



A footnote to this figure would be that when seeking to collect data on these dimensions of trust, the use of appropriate data collection methodologies needs to be carefully considered. For instance, *inherent general* and *institutional* trust effects, being associated with the psychological make up of

individuals or interpersonal aspects of trust respectively, are more relevant to consider in focus group studies than in surveys, which are designed to produce aggregated, broad level results representative of the population.

Focus group studies enable more detailed and subtle analysis of factors influencing an individual's perceptions and actions which surveys, due to design limitations and time constraints, cannot accomplish. In seeking to develop indicators designed to collect

data on the various dimensions of trust identified in Figure 1, Table 1 outlines some possible indicative measures that can be incorporated into survey mechanisms and future focus group studies.

Table 1 Indicative indicators for measuring multi-dimensional aspects of trust

Dimension of online Trust	Indicative measures
<i>Socio-demographic effects (including ethnicity)</i>	<ul style="list-style-type: none"> • Age • Gender • Income • Family type • Education level • Indigenous status • Ethnicity (racial heritage) • Type of employment, Occupation (broad)
<i>Broad geographic differences</i>	Differences between attitudes in rural and regional areas re: <ul style="list-style-type: none"> • Inherent trust – smaller versus larger societies • Distances to services – convenience versus security
<i>Inherent general trust</i>	<ul style="list-style-type: none"> • Most people can be trusted* • Cannot be too careful dealing with people* • Will generally trust someone/something until there is a reason to mistrust them/it • Will generally not trust anyone/anything until they/it prove themselves trustworthy • Places a great value on privacy of personal information *Sourced from an ABS survey.
<i>Institutional trust</i>	Willingness to place trust in businesses/organisation depending upon proximity, previous dealings, reputation of entity and physical presence versus virtual <ul style="list-style-type: none"> • Local (council), State or Federal government • Individual departments (eg Family Services, Tax) • Police • Educational institution, health institutions, community services organisations • Legal firm • Retail business • Bank or Credit Union or other financial institution
<i>Experiential factors</i>	<ul style="list-style-type: none"> • Identity theft or other fraud • Breach of privacy from information provided off line • Physical burglary or theft of property • Online fraud; lost money due to online fraud • Breach of privacy from information provided online • Malicious virus or other attack • Purchases sub-standard or not received

Continues over >

Dimension of online Trust	Indicative measures
<i>Propensity to use modern technologies</i>	<ul style="list-style-type: none"> • Mobile phone • Computer (home, work or elsewhere) • ATM, periodically • EFTPOS to purchase, periodically • Phone banking • Internet user status (from home, work, elsewhere) • Home connection is Broadband/Dial-up • Number of years online (<1, 1-5, 5+)
<i>Computer and online skill/ awareness</i>	<ul style="list-style-type: none"> • Computer use, connections and years online etc (see above) • Self assessed skill level (basic, average, advanced) <ul style="list-style-type: none"> - with computers - with Internet
<i>e-security practices</i>	<ul style="list-style-type: none"> • Disable cookies or use anti-cookie software • Use privacy protection, firewall, anti-spyware, anti-SPAM • Regularly update virus/worm protection software • Keep up to date with latest virus threats and hoaxes • Only do financial transaction from work, etc, where there are better security facilities • Stores financial or other sensitive information on computer • Believe they are safe from viruses or hackers

The central focus of any trust survey can be quite varied and may change over time. However, as a government policy agency concerned with promoting and building trust in the information economy our key interests at present could be divided generally between:

- Personal information providers; and
- Transactors.

Beyond this, our main interests would be to:

- take account of trends over time in online activities especially to see if any show a decline;
- take stock of adverse experiences over time;
- understand the type and extent of concerns Internet users have and whether the level of concern is changing over time;

- gain an appreciation of levels of awareness of issues that may potentially impact trust or affect online activities;
- understand the nature and extent of security habits and other protective measures such as are described previously;
- understand the main influences when purchasing online;
- understand the barriers to transacting online (i.e. what prevents transacting online); and
- understand how consumer knowledge and level of understanding of ICT and the online environment impacts on all of the issues listed above.

Australia's online community and contextual setting

In this section, the intention is to present a broad picture of Australia's growing online community as a background to the analysis of data relating to consumer trust in the online environment. This will cover the online activities that users are engaging in, including activities that may be at stake in the event of a significant loss of trust in the online economy.

It is recognised that activities associated with business communications are not covered but are nevertheless very important. In this context, the Internet and World Wide Web are both products of and tools for a new way of doing things, demonstrating the feasibility of achieving significant goals outside of the confines of traditional hierarchical organisations¹³. To the extent that any of these activities are at risk through lack of trust or system security failure, the economic implications may be dire. However, these considerations are not the focus of this report.

Beyond the organisational setting, Australians in general are increasingly recognising the importance of the Internet as a transformative technology, particularly its role in reshaping every day social and economic activities. According to a recent Nielsen survey (shown in Figure 2), approximately 46 per cent of Australians aged 14 years and over believe that technology/computers have made life easier, a view which is more prevalent amongst younger Australians.

According to the survey, 67 per cent of Australians aged 14–17 reported a positive view towards the impact of technology. While the positive impact of technology tailed off with increasing age, generational progression would suggest that technology will have an increasing importance to the vast majority of Australians in the years to come.

The growing number of online Australians provides some insight into the attractiveness of networking technologies such as the Internet. Australia is a highly connected society with over 60 per cent of

households connected to the Internet and in excess of 10 million Australians actively using the Internet on a monthly basis¹⁴. In Australia's business community, 46 per cent of farms and 74 per cent of other businesses (25 per cent of which have a website) now use the Internet for a variety of business purposes, rising to nearly 90 per cent connectivity for businesses with more than four employees¹⁵.

The Internet in Australia now provides for an extensive networked community, a precondition for the rapid development of viable online digital services and content.

The majority of Australians have a reasonably high level of familiarity with the Internet. This familiarity has seen online social and economic activity grow enormously over the last five years. Internet commerce, as measured by the ABS, was estimated to be worth some \$33 billion at June 2004, compared to \$24 billion at June 2003—an increase of 37 per cent over the 12 month period.

However, this is only a limited measure and excludes the benefits that arise from social interaction, general communication and information gathering, as well as the impact of the Internet on organisational productivity.

Australians now undertake an expanding range of activities online. While the Internet quickly became significant for online communication, information gathering and transmission; transaction based activities such as banking and bill payment have grown enormously since late 2001 (Figure 2). More and more Australians recognise the value of these services in terms of time savings, convenience, and the availability of real savings online. Financial activities are now in the top 10 activities as shown in Table 2.

Table 2 Top 10 online activities, April 2005

Activity	%
Electronic mail	84
Searching for product information	59
General surfing	58
Downloading software / files	51
Check account balance	50
Travel information	44
Search for company information	43
Transfer funds between accounts	42
Pay bills online	39
Accessing News & Current Affairs	38

Base = Internet users in the past month
Source: Nielsen Net//Ratings

Figure 2 Australians' attitude to technology: technology makes life easier, April 2005 (Nielsen//NetRatings)

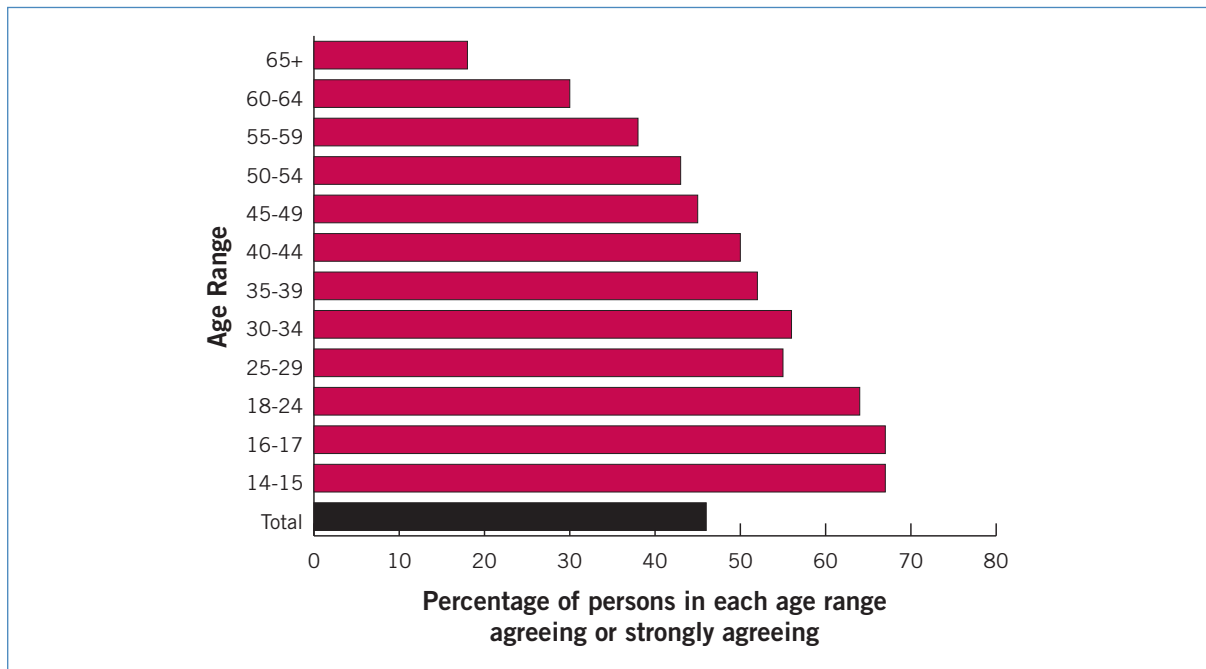
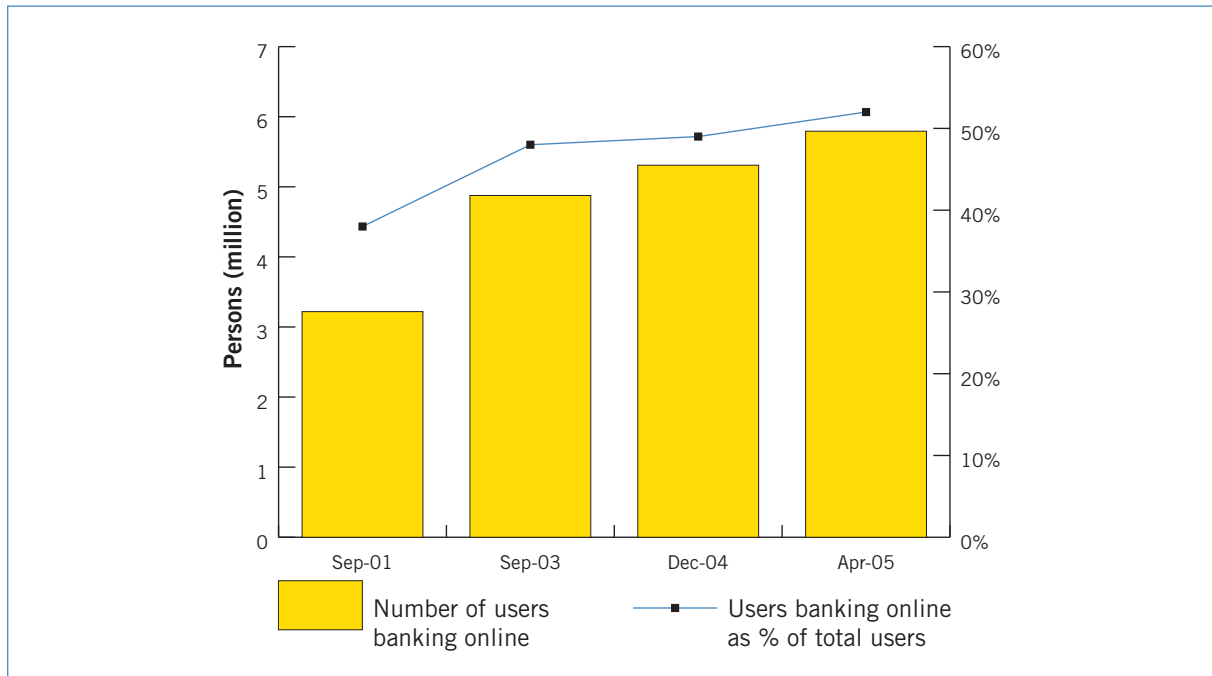


Figure 3 Online banking (Nielsen//NetRatings)



Figures provided by Nielsen//NetRatings (Figure 3) suggest there are just under 5.8 million individuals over the age of 14 years who are banking online (i.e. checking account balances, transferring money between accounts and reviewing loans and mortgages). This represents 52 per cent of all Internet users in this age range. Over the past five years the number of Australians banking online has increased by an average of 18 per cent per annum. The convenience of not having to line up in queues to pay regular bills or to contend with travel issues is also an attractive option for Internet users. Forty per cent of Internet users 14 years and over, now pay bills in this way.

Sixty per cent of the online population 14 years and over (6.6 million persons) currently do some form of buying, selling or bill payment online as indicated in Figures 4 and 5). While growth in the number of online shoppers and bill payers has slowed to just over 4.4 per cent in the period December 2004 to April 2005, the average annual growth since September 2001 has been 20.2 per cent. These are very substantial figures and warrant particular attention in relation to trust and security issues.

Across all age ranges, home is the predominant location for engaging in online shopping and bill payment activities as is depicted in Figure 6.

This is useful information when considering the type of policy or remedial responses that may be required in the face of increasing threat levels of various kinds.

Over the last four years, Australians have also upgraded their home Internet connections, increasingly turning to broadband services, predominantly DSL or cable, a development which is largely being fuelled by the desire to undertake existing online activities more efficiently and the attractiveness of declining price structures for broadband services. Fifty seven per cent of home Internet users are now estimated to be using home broadband services (Figure 7).

As seen in Figure 8, the predominant impact of broadband on online usage patterns has been to greatly improve the efficiency of Internet use. Specifically, home broadband is enabling users to carry out existing online activity such as browsing, downloading and sending files and e-commerce more efficiently without the time delays associated with dial-up access. However, broadband also brings its own set of risks and security issues. Along with the tendency to download more which in itself increases the chance of malware infection, the 'always on' nature of broadband systems means that they are potentially permanently visible to malicious network agents. Dial-up connections on the other hand, do not have a static IP address and are visible for shorter periods of time.

Figure 4 Buying, selling and bill payment (Nielsen//NetRatings)

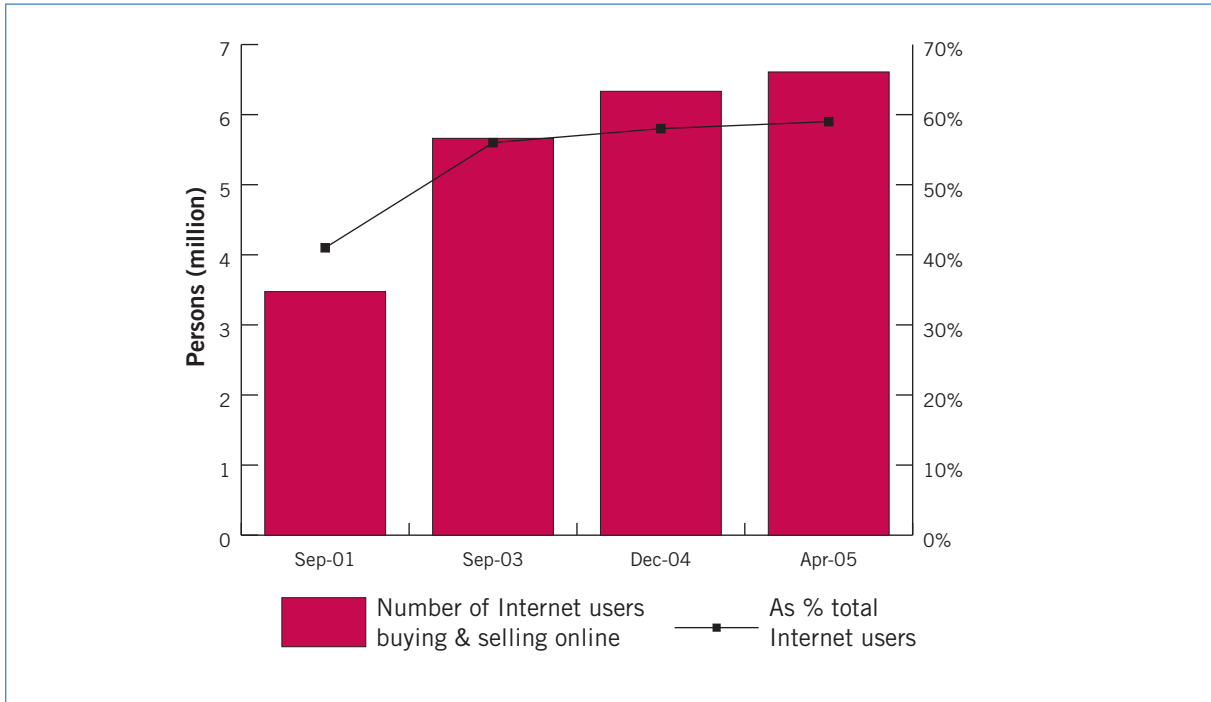


Figure 5 Paying bills online (Nielsen//NetRatings)

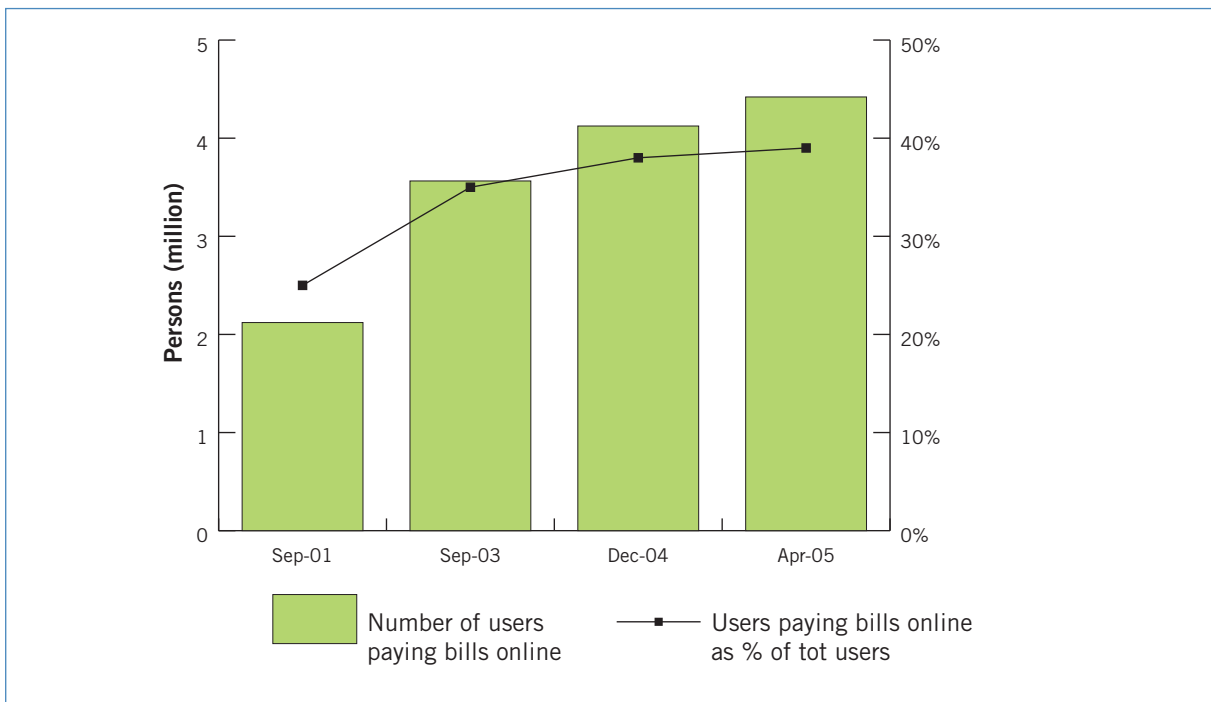


Figure 6 Online shopping and bill payment activities by age and location, April 2005 (Nielsen/NetRatings)

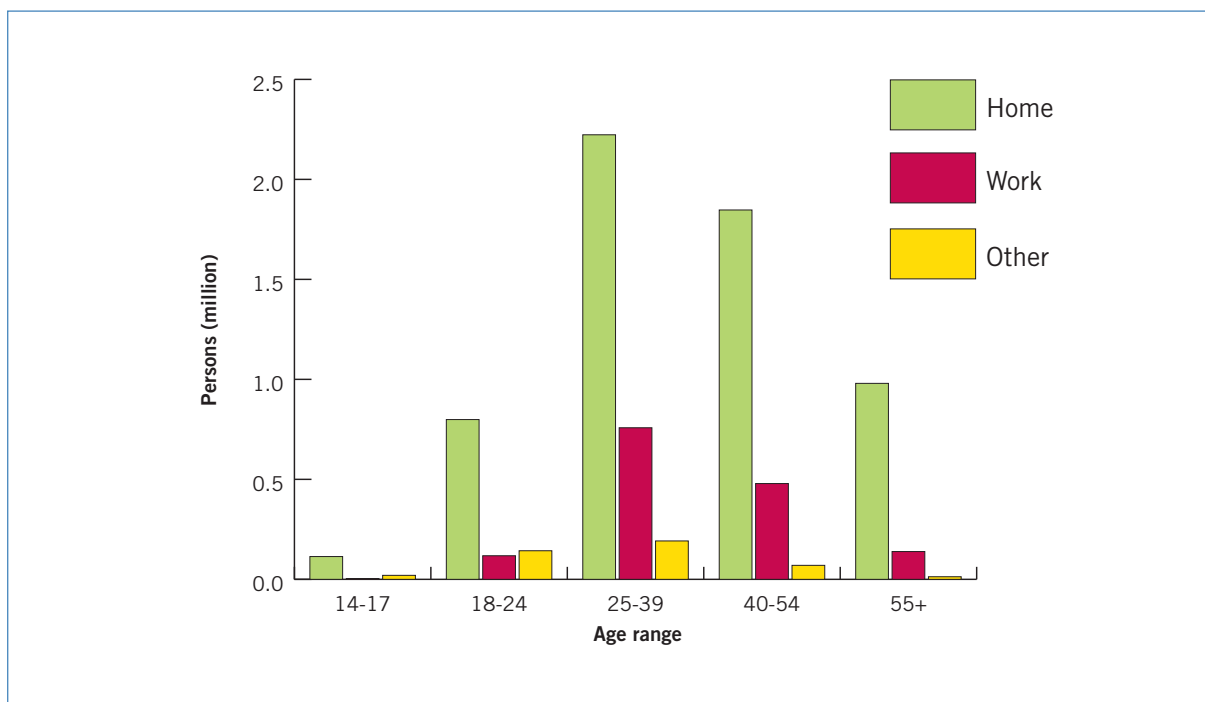


Figure 7 Home Internet users using broadband technology, Australia (Nielsen/NetRatings)

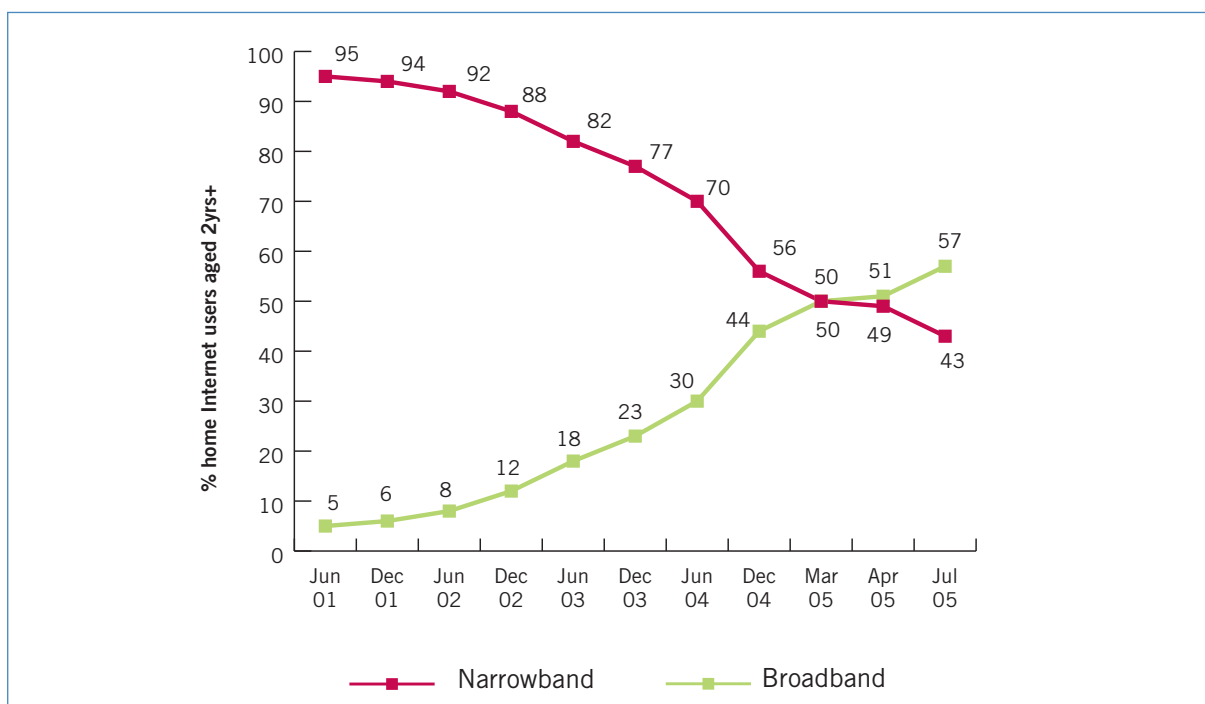
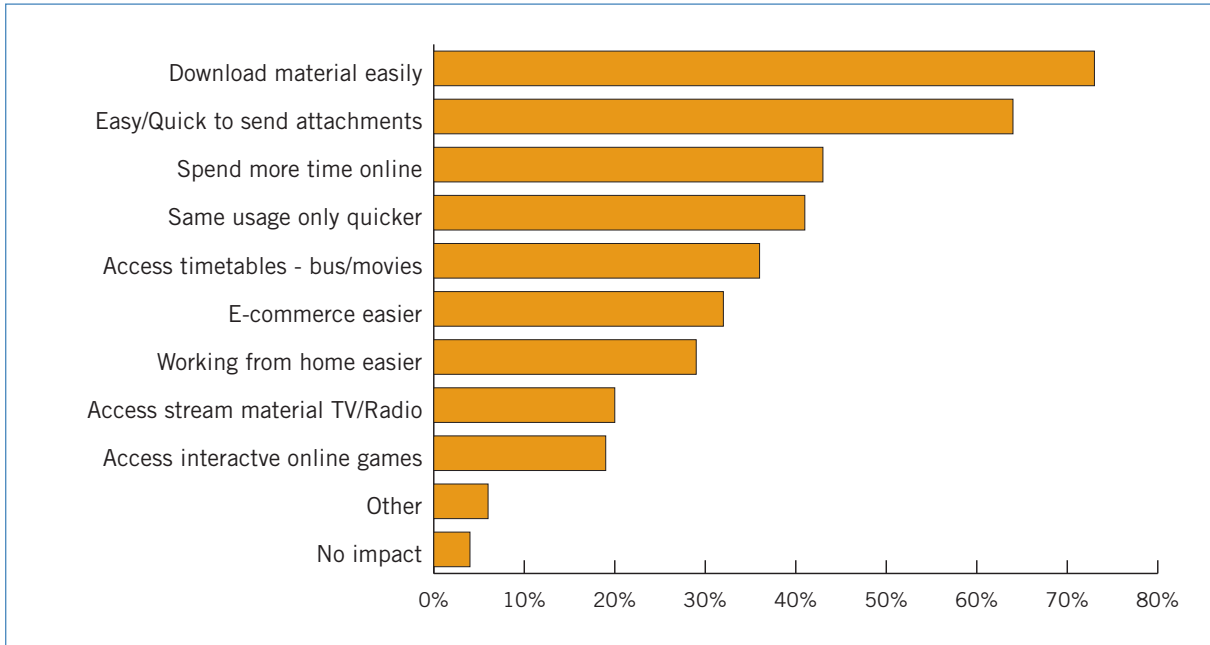


Figure 8 Impact of broadband on users, April 2005 (Nielsen//NetRatings)



The preceding data shows that Australia has a large constituent of active and regular online transactors. This provides a significant base to explore the issue of

trust and to evaluate the potential impacts of threats to future confidence in the Australian online economy.

Online consumer trust—exploratory measures and findings

Survey methodology

In this section, consumer data collected by Sensis Pty Ltd in May 2005 as a supplement to its Consumer Report¹⁶ is presented. Internet users in the survey are those who used the Internet in the 12 months to May 2005.

Table 3 Projected number of Australians in various groups from weighted survey responses

Category	Number '000
Number of online Australians	12 575.8
Passive Internet users	2 587.8
Active Internet users	9 988.0
Those who perform a single online transaction	1 928.0
Those who perform multiple transactions	8 060.0
Those who perform 2 types of transactions	2 110.0
Those who perform 3 types of transactions	3 235.3
Those who perform 4 types of transactions	2 714.7

The Sensis survey was a quota sample of 1500 respondents 14 years and over, weighted on the basis of 2001 Population Census data to reflect the structure of the general Australian population. Table 3 shows how the weighted survey responses translate to the Australian population for a number of categories.

A set of exploratory questions was fielded on the issue of trust and security. The survey yielded some interesting results and will be a useful basis for the development of any similar survey in the future.

The survey provides estimates of the total Australian population 14 years and over and identifies the proportion that used the Internet in the past 12 months. Internet users were asked what they did online using six response categories:

1. Ordered goods and services
2. Made bookings
3. Paid for purchases or bills with credit card or other means
4. Undertaken banking online
5. Supplied personal information online
6. None of the above

All Internet users were then asked about their online concerns in a single multiple choice question. Those who responded to items 1 to 5 above were then taken through a further series of questions covering:

- Internet experiences;
- Concerns with transacting online;
- How they sought to ensure online security; and
- Why they chose to transact or provide information online.

Respondents to the Sensis Consumer survey were also asked to provide a range of demographic information to assist analysis.

Definitional issues

A few terms have been developed to describe particular sub-sets in this paper. 'Active users' refers to those who have transacted online. 'Passive users' refers to the group who are connected to the Internet but not engaging in online transactions.

For the purposes of this survey 'virus and other attacks' include viruses, worms and trojans and a range of other malware with spyware separated from this group. It is possible that differences in the individual's interpretation may have resulted in skewed results for these experiences, i.e. over reporting of 'yes' responses for 'experienced a virus attack or other' and under-reporting for 'Spyware'.

However, since this paper is exploring issues relating to trust and consumer perception, it is important to know whether consumers believe they have experienced these online threats. These form a group of malicious threats that consumers do not want on their computers.

Information on the tables provided in the report

The following section contains tables showing the per cent of respondents answering 'yes' to a number of questions within the categories listed above. Some questions received a low number of 'yes' responses and therefore are likely to have a standard error of more than 25 per cent, and in some cases, of more than 50 per cent. Therefore, percentages of less than 10 per cent in the following table should be used with caution.

Passive and active Internet users

Internet users engage in a wide variety of online activities. For the purposes of this research our interest was in establishing the relative proportions of Internet users that engaged in 'active' versus 'passive' activities insofar as their activities related to trust.

'Passive' Internet users were classified as those people who did not engage in online ordering or booking, did not make online payments and did not do banking online nor provide personal information online. In Figure 9, passive users are counted against the category 'none of the above'. 'Active' users were the set of Internet users who engaged in one or more of the e-commerce related activities or who supplied their personal details online for related or other purposes (the other five categories in Figure 9).

As can be seen in Figure 9, the vast majority of Internet users were in the 'active' category. Just under 21 per cent of Internet users were passive.

Figure 9 What Internet users do online, May 2005 (Sensis)

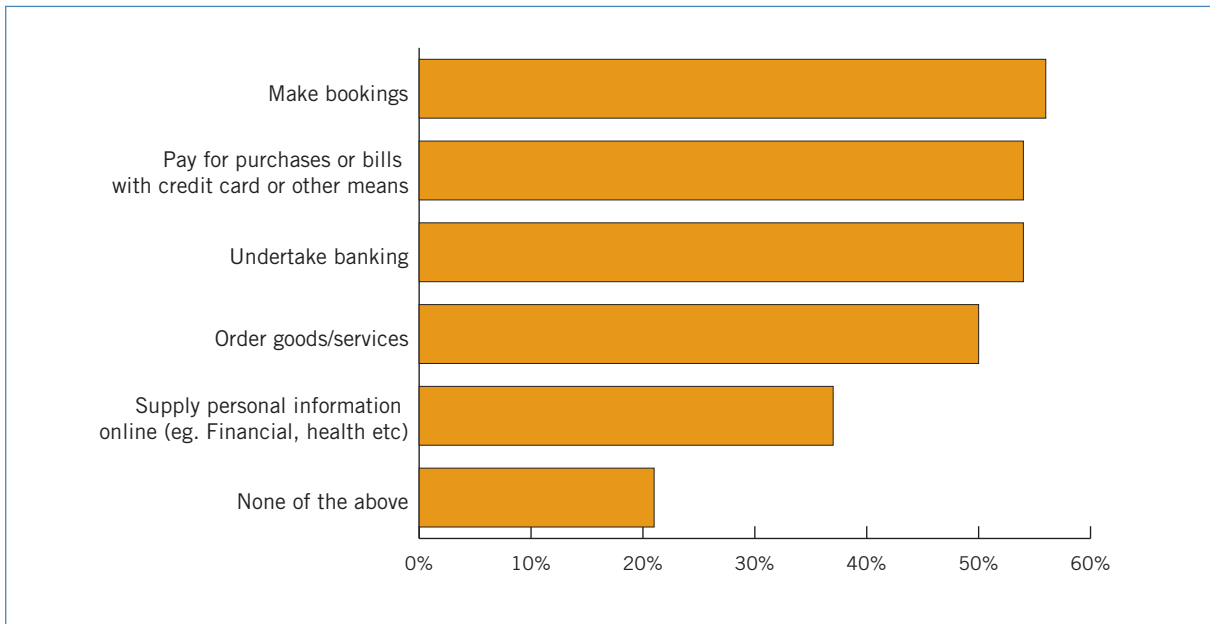


Table 4 Per cent of passive and active Internet users by household income

Household Income	PASSIVE %	ACTIVE %
Up to \$25 000	24.9	7.0
\$25 001–\$35 000	9.5	5.5
\$35 001–\$45 000	5.7	8.7
\$45 001–\$55 000	4.5	10.9
\$55 001–\$65 000	8.1	7.9
\$65 001–\$75 000	8.6	7.9
\$75 001–\$85 000	1.9	6.2
\$85 001–\$100 000	2.5	9.1
\$100 001+	4.9	21.4
Refused	14.4	10.7
Don't know	15.1	4.8
Total	100.0	100.0

Table 4 shows both passive and active users grouped by household income. (Personal income was not available.) The distribution of passive users is skewed towards lower household incomes, whereas the distribution of active users is skewed in the opposite direction. For instance, just over 34 per cent of passive users were from households with an income below \$35 000 whereas more than 30 per cent of active users were from households with incomes over \$85 000.

A number of factors may influence this outcome including:

- persons from low income households being less willing to take risks with what they have;
- having less lifestyle-influenced need to transact online;
- less means such as access to a credit card to shop online; or
- less disposable income.

For these people the staples of life tend not to be transacted over the Internet.

Table 5 Working status of passive and active Internet users

Working Status	PASSIVE %	ACTIVE %
Working full-time	32.9	54.3
Working part-time	24.3	21.2
Unemployed, seeking work	6.2	3.9
Looking after the home	7.8	6.8
Studying full-time	19.7	11.5
Studying part-time	2.6	1.5
Retired	19.0	7.6
Total	100.0	100.0

A distribution of passive and active Internet users by working status is shown in Table 5 and reveals that the largest proportion of both groups were made up of full- and part-time workers; 57 per cent and 76 per cent respectively. However, across all labour force groupings, active Internet users outnumbered passive Internet users. Full-time workers were six times more likely to be active than passive users, whilst persons in part-time employment and those looking after the home were three times more likely to be active Internet users. The unemployed and persons studying full- or part-time were twice as likely to be active Internet users, compared to one and a half for retirees.

Active users—multiple activities

The survey results showed that there is considerable overlap in the set of activities engaged in by active users. That is, most active users tended to perform more than one of the four categories of transactions. While the amount and frequency of online transactions performed by individuals was not captured in this survey, broad level information about transaction types allows for some distinctions to be made between those who performed only one kind of online transaction, and those who performed many.

The four transaction categories considered below are:

- ordering or booking;
- online payments;
- online banking; and
- supplying personal information.

Because of their similarity, the ordered goods and services category was combined with the bookings category.

Table 6 shows that just over 80 per cent of active transactors performed more than one type of transaction and just over a third completed all types of transactions. Less than 20 per cent of active transactors performed only one type of transaction and Figure 10 shows the breakdown of transactions for this group.

Table 6 Percentage of active transactors

Number of transaction types performed	Active Transactors %
1	19
2	21
3	32
4	27
Total	100

Figure 10 Those who perform a single transaction by type

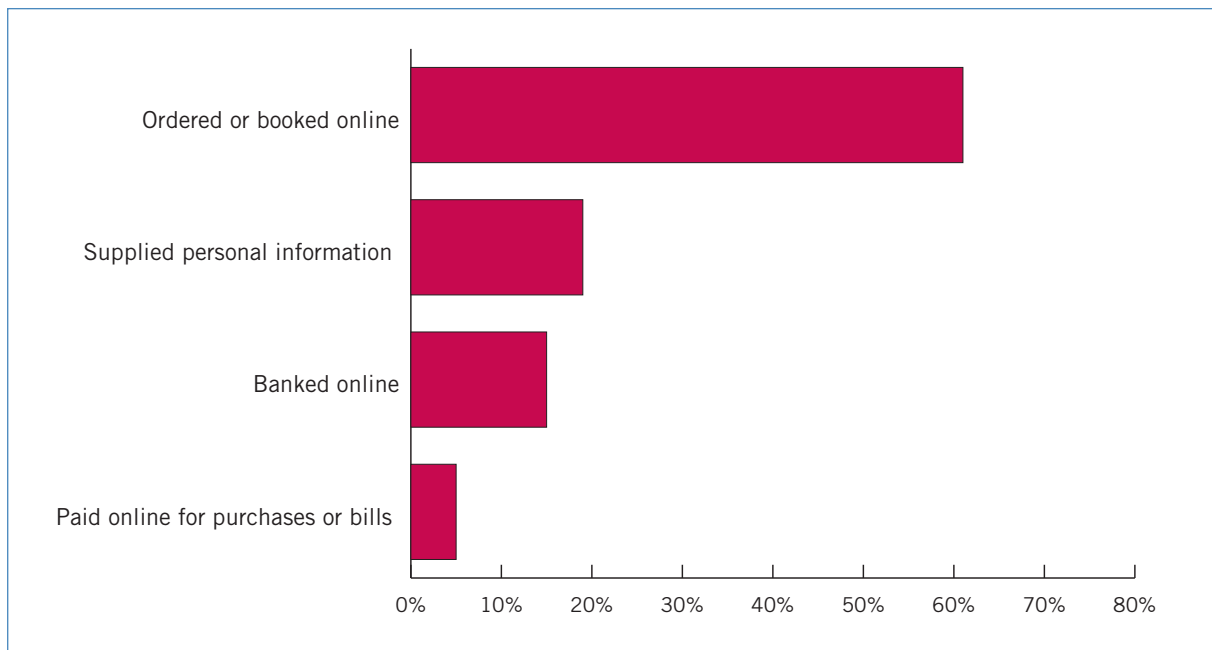


Figure 11 Transaction levels by high and low household income ranges

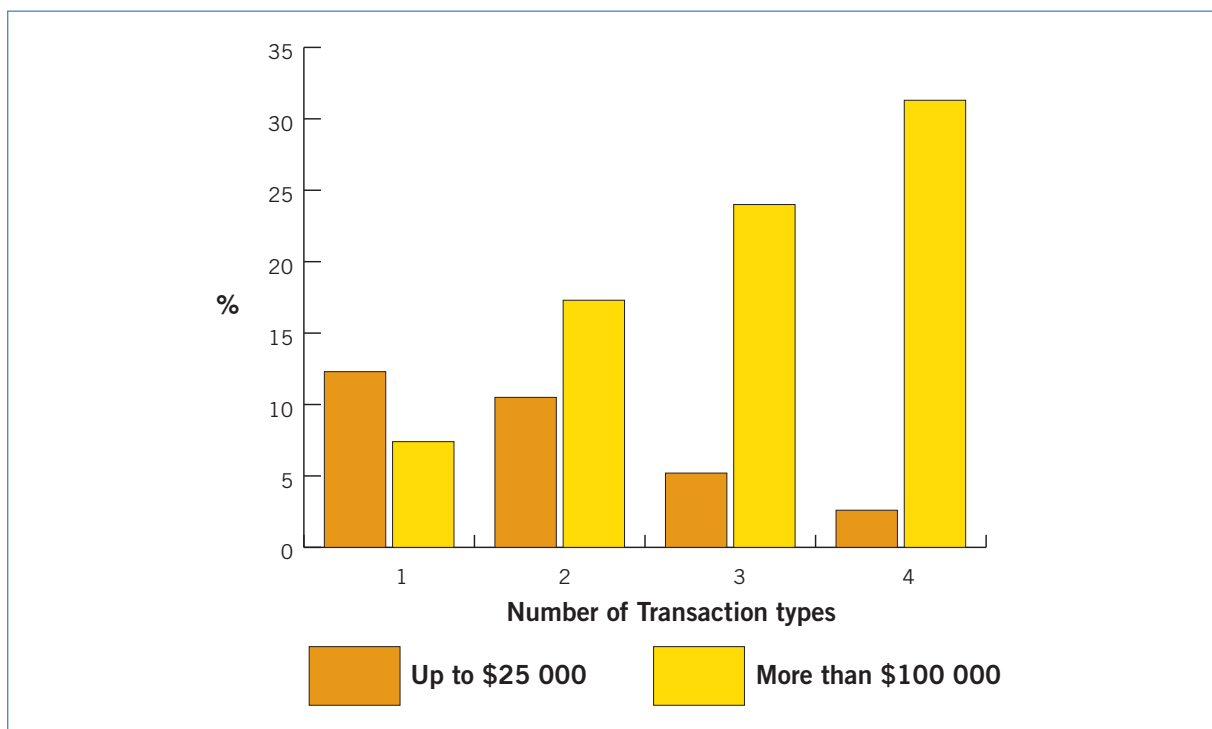
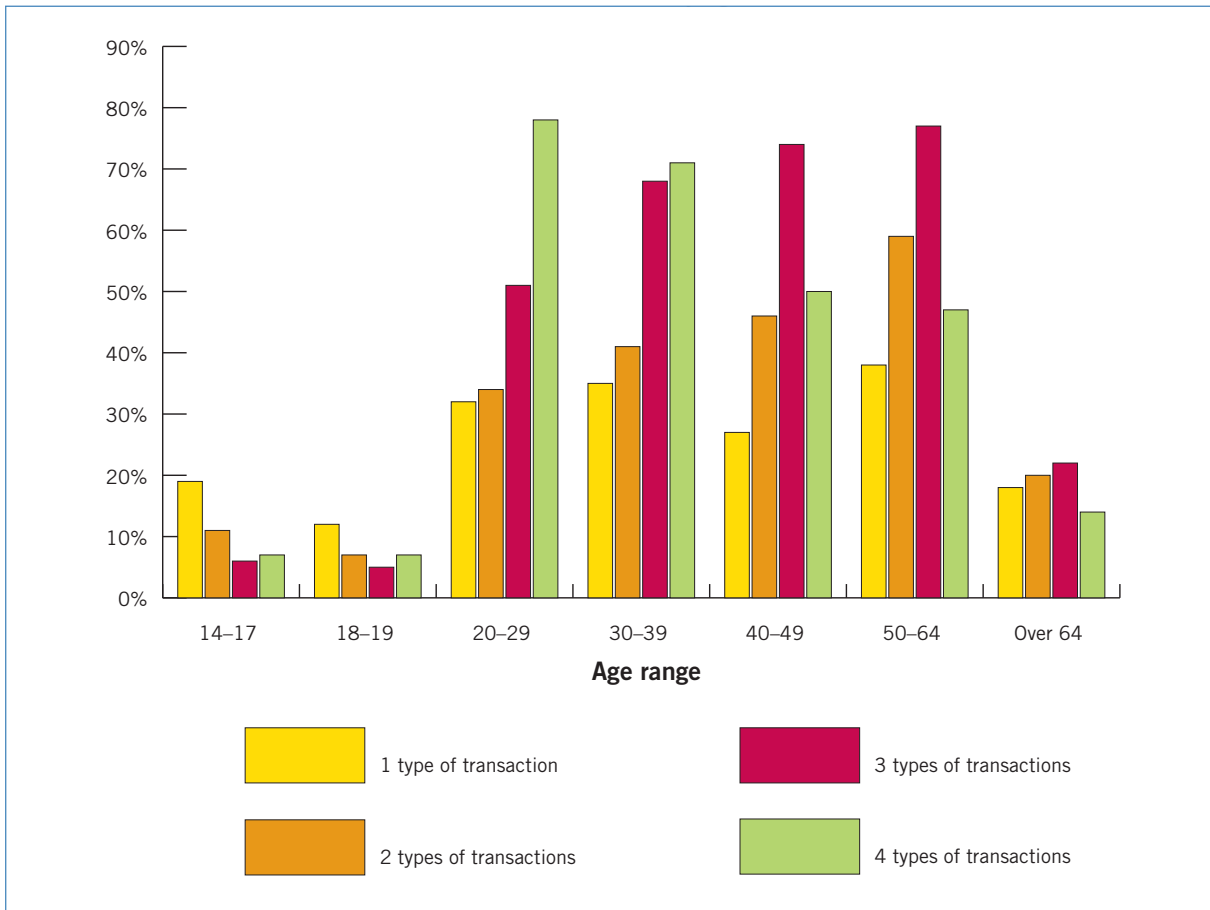


Figure 12 Transaction levels by age



The overwhelming majority of single transactors were people who ordered goods and services or booked online. Just under 20 per cent only supplied personal information online, followed by online banking (15 per cent) and making online payments (5 per cent).

Figure 11 illustrates the relationship between the number of transactions performed and household income. The level of household income appears to be a major determinant of whether a person is a multiple transactor. There was a strong relationship between household incomes of over \$100 000 and the occurrence of multiple types of transactions, but quite a low relationship among individuals who resided in a household with an income of less than \$25 000. This would suggest that ‘income rich but

time poor’ individuals are the most likely group to be multiple transactors—a proposition that is supported by other findings in this report. There were no clear trends apparent for other income levels.

There is also a relationship between age and the tendency to be a multiple transactor (Figure 12). The relationship is strongest for individuals within the 20–39 age range. Those aged 14–17 years mostly performed only one type of transaction. For those aged over 64, there was an inverse relationship with performing multiple types of transactions. That is, individuals in this group were more likely to be a single transactor and progressively less likely to engage in two, three or four types of transactions. Similarly, from age 20 onwards, the probability of engaging in all four types of transactions declined with age.

Concerns

Security of the Internet was the number one concern for both passive and active Internet users, although 20 per cent of active users and 15 per cent of passive users reported no concern (see Table 7).

The potential for fraud was the second greatest concern for both groups and seems not to be closely associated with hacking or virus concerns, both of which rated as a much lower concern. While these concern levels are reasonably high, statistics in the next section show that the incidence of online fraud was much lower. The concern may therefore largely be a result of users' general awareness of fraud related issues, especially those that receive press coverage including from overseas sources. There are also numerous Internet sites (including security firms, government and financial institutions) that draw attention to fraud related activities such as phishing

and similar scams. A slightly greater proportion of passive Internet users identified the potential for fraud as a concern and this perhaps demonstrates a constraining effect that comes with a greater awareness of fraudulent online activities.

Privacy concerns were the next most prevalent concerns for both groups (with possible misuse of personal information and actual provision of personal information being closely related). A slightly higher proportion of passive users were concerned with privacy and providing personal information than were active users. On the other hand, concern about the misuse of personal information rated slightly higher among active users, which implies that there is an element of misgiving accompanying the provision of such information.

Table 7 Top 10 online concerns

Internet users	PASSIVE %	ACTIVE %
Security of the Internet	54	55
None	15	20
Potential for fraud involving theft of funds/credit cards	23	17
Privacy concerns	20	17
Misuse of personal information	9	14
Providing personal information	13	9
Open to computer hackers	3	2
Lack of confidence in using services	3	1
Open to viruses	1	1
Uncertainty relating to consumer protection, rights	1	1

Table 8 Top 5 concerns, by transaction level¹⁷

	Number of types of transactions undertaken			
	1	2	3	4
Security of the Internet	51.9	62.9	58.5	48.3
Privacy concerns	15.4	17.3	17.3	18.2
Potential for fraud involving theft of funds/credit cards	15.7	17.2	19.7	13.8
Misuse of personal information	20.4	14.3	12.5	11.5
Providing personal information	7.9	7.9	11.0	9.9
None	21.8	12.8	19.4	24.0

Looking at trends among single and multiple transactors (Table 8), a large number of those in each of the transactor groups were concerned with security of the Internet, ranging from just under half to almost 63 per cent of respondents. However, the most avid users (who perform all four types of transactions) appear to be less concerned with the security of the Internet and the misuse of personal information.

When cross referenced with security measures undertaken (see Protective measures, page 33 in this report), this very avid group was more inclined to perform at least single, if not multiple security measures. A significant number of the individuals in this group may therefore be less concerned on account of the protective measures they adopt. At the same time, there may also be a significant number of individuals in the group whose concern levels have been lowered through uneventful usage or who may have some disregard for the potential dangers for a variety of other reasons.

In relation to personal information, the greatest concern with misuse of personal information was shown by those who performed only a single type of transaction, which reduced as more transaction types are undertaken. This would suggest that concerns of this type may initially be a disincentive to transacting online, diminishing with greater exposure to online transactions. The concerns of online Australians towards transacting online are also mirrored in international research.

A survey conducted by Ipsos Insights in August 2005¹⁸ of 1000 American individuals concluded that phishing and hacker tactics were having an impact on online banking. Their results indicated that:

- 83 per cent of survey respondents who conduct their personal banking online reported concerns over protecting their personal information from theft;
- 73 per cent of people said theft of personal information is a deterrent for them to use online banking; and
- survey respondents were equally concerned about banks selling their personal information to a third party, with 72 per cent of respondents citing the issue as extremely or very important.

While the Ipsos survey gave no suggestion that the 39 per cent of Americans using online banking was diminishing, it did suggest that take up had flattened out and that participation may be higher were it not for such concerns.

Research conducted by EUROSTAT¹⁹ found whilst buying over the Internet is generally perceived as relatively safe, among those who had never bought via the Internet, 42 per cent mentioned security concerns and worries about giving credit card details over the Internet. While such concerns appear to be an inhibitor to online shopping, in many European countries there is a strong preference to shop in person and to be able to see the goods. There also appears to be significant variability between countries in that concerns about security and providing credit card details online varied from 10 per cent of Latvian online shoppers up to 70 per cent of those in Finland, and the Portuguese were more concerned about providing personal details online (52 per cent) than were the Danes (5.4 per cent).

Concerns about security and the possible misuse of personal information have been identified as the main inhibitors of online commerce for some time. So there is really nothing new in the Department/Sensis or other findings. For instance, Harris Interactive made similar observation on the basis of data collected in 2000²⁰. What is lacking in the Australian context (and presumably for other countries) is any substantial proof that the situation has changed significantly over time, although it is clear that such concerns are long-standing and persist.

The inference for online traders is that in order to entice a greater proportion of the Internet community to online shopping channels, they must continue to provide and promote security and privacy aspects in their online dealings with consumers. At the same time, the lack of rigorous statistics on threats, incidents and trends may also serve to give voice to a body of information that is unscientific, emotively reported or which mainly serves the interests of its authors.

Online experiences

From the material above it is clear that there are high levels of concern about Internet security and the potential for fraud involving theft along with medium level concerns about privacy and information misuse. These types of concerns can be based on actual experience or on an individual's knowledge and awareness including knowledge gained from media reports and other online sources.

From the information in Table 9, it is reasonable to conclude that concerns about Internet security seemed to be largely associated with real experiences

of viruses and other malware. Some 66 per cent of active users had experienced such attacks. These types of agents are frequently delivered in unsolicited emails and as can be seen, there is a very high incidence of users receiving unsolicited emails.

Concerns about online fraud involving theft were indicated by just under 17 per cent of the active group. However, less than 4 per cent of the group reported they had actually 'lost money due to online fraud'. While the concern seems to outweigh the experience, the non-trivial nature of the statistic itself may be of concern to the wider audience. It would be useful to be able to track this over time, and if possible, to determine the size of the loss and the circumstances (i.e. how many were phished or how many were defrauded in other ways).

At the same time, the observation needs to be tempered with an appreciation of comparable experiences in the physical world. Figures published by the Australian Competition and Consumer Commission in its 2003–04 annual report suggest that complaints and enquiries about an 'online trader or e-commerce' represented 14.5 per cent of business related complaints that year. This represents a one percentage point increase over the previous year. It also indicated that of the top 10 possible contraventions of the Trade Practices Act 'accepting payment non-supply' accounted for three per cent.

Spyware has been implicated in online theft and is receiving considerable attention in the press and by analysts. However, in this survey less than one per cent of active users had any apparent experience of spyware. The fact that this statistic is exceptionally small may be of concern in itself, as some researchers believe that most people are unaware that their computers contain spyware.

Privacy concerns were mentioned by 17 per cent of active users. In the light of statistics showing that 13 per cent had actually experienced a breach of privacy (left open to the respondent to define), the level of concern appears to be justified.

The survey also found that less than six per cent of active users had not received the goods they purchased online and just over five per cent claim that the goods they received were sub-standard. Some of these experiences will be instances of intentional fraud. These experiences would no doubt have an impact on trust with particular vendors, but not necessarily the Internet as a channel for services.

Table 9 Online experiences of active users

Experiences	ACTIVE USERS %
Received unsolicited material via email	79.3
Experienced a virus or other attack	66.2
Suffered a breach of privacy	13.2
None of the experiences identified here	9.8
Not received online purchases	5.6
Received sub-standard goods	5.1
Lost money due to online fraud	3.7
Get porn ads	1.4
Get a lot of spam	1.4
Get advertisements/pop up ads	1.3
Line drop outs	1.1
Takes too long/too slow	0.7
Spyware	0.4
Hacking	0.3

Table 10 Online experiences by number of transaction types undertaken

Online experiences	Number of different types of transactions undertaken %			
	1	2	3	4
Received unsolicited material via email	62.9	81.1	81.3	87.0
Experienced a virus or other attack	52.7	69.6	65.6	73.8
Suffered a breach of privacy	8.6	10.9	18.1	12.2
None of the experiences identified here	21.1	6.9	10.2	3.6
Not received online purchases	3.0	6.1	5.2	7.4
Received sub-standard goods	3.7	5.0	3.3	8.4
Lost money due to online fraud	4.1	5.3	1.9	4.4
Get porn ads	3.4	0.8	1.2	0.8
Get a lot of spam	0.9	2.6	1.5	0.6
Get advertisements/pop up ads	2.2	1.4	0.4	1.6
Line drop outs	0.2	0.8	1.4	1.7
Takes too long/too slow	0.2	1.7	0.4	0.5
Spyware	0.0	1.3	0.2	0.1
Hacking	0.1	0.0	0.5	0.5

Looking at the trends between single and multiple transactors (Table 10), generally those who performed multiple online transactions reported more online experiences. The most pronounced difference can be seen in the categories 'received unsolicited material' and 'experienced a virus or other attack'. Almost nine out of 10 people who performed all types of transactions had received unsolicited mail and seven out of 10 people had experienced a virus or other attack. Both of these categories were at least 20 percentage points higher than those for single transactors. For those who had lost money due to online fraud there was no significant difference between single and multiple users, perhaps indicative of increased measures taken to ensure online security by those in the latter category.

Spam is the main delivery mechanism for viruses, Trojans, spyware, phishing scams and other intrusions. However, while the vast majority of spam can be traced to IP addresses in the United States, South Korea and China (36, 25 and 10 per cent respectively) according to Sophos²¹, this does not necessarily mean that the real perpetrators are residents of those countries.

In relation to global spam and phishing volumes, an article published in Techworld²² provides a useful summary.

The amount of spam made up of phishing emails is lower than one would assume from the recent publicity on the topic. Symantec puts the absolute number of phishing emails at around 4.5 million per day (33 million per week), which equates to fractions of a per cent of the total spam volume. CipherTrust puts the percentage as high as one per cent, while OnlyMyE-mail.com puts the figure at just over half of one per cent.

Regardless of the real volumes of spam and phishing related emails, etc, their continuing existence serves to undermine trust in Internet based communications. The evidence of this is demonstrated in the preceding discussion of the concerns that Internet users have. At the same time, there is evidence that users are becoming more aware and discerning in how they deal with unsolicited communications and this is discussed under the next heading.

Protective responses

Results from the May 2005 Sensis Consumer Confidence survey show that active users in Australia adopted a broad range of practices to minimise risk when using computers and the Internet (Table 11).

Given the high incidence of attacks—virus, Trojans, spyware, phishing, scams and other intrusions—it is encouraging to note that virus protection software is at the top of the list shown in Table 11. However, it is perhaps disconcerting that the numbers are not considerably higher for this and other related items. For instance, in addition to only 32 per cent indicating the use of anti-virus software, only 14 per cent reported against firewall software or services, and a meagre six per cent reported the use of spyware protection software. In comparison, Eurostat report that more than a quarter of Internet users have installed a firewall in Denmark, Germany, Hungary, the UK and Iceland²³.

Similarly, given the high incidence of unsolicited email reported earlier and concerns about privacy etc, a very low proportion of active users reported against the use of privacy protection software (three per cent), anti-SPAM software (2.4 per cent) and anti-cookie software (less than one per cent). ABS statistics indicate that in the March quarter 2005, 76 per cent of ISPs were offering spam-filtering software and the majority of these services were free. The take up of such services appears therefore to be quite low.

There also appears to be relatively little concern among this group of Internet users of storing financial and other sensitive information on their computers. Only 3.5 per cent were definite about avoiding this.

On a more positive note, the figures suggest that a significant number of active Internet users are discerning about whom they deal with and their dealings are definitely not restricted to Australian websites. Table 11 shows that just over 18 per cent looked for sites with trustmarks or certificates and privacy and security policy statements, just over 15 per cent preferred to only deal with well known organisations, and more than six per cent reported they 'use only secure sites/sites I know/trust'.

Table 11 Protective measures undertaken by active users

Protective measures	ACTIVE USERS %
Regularly update virus/worm protection software	32.4
Look for sites with trustmarks/certificates, privacy and security policy statements	18.1
Only deal with well known organisations online	15.2
Use firewall software or service	14.0
Don't know	7.6
Do nothing	6.9
Regularly change passwords	6.7
Use only secure sites/sites I know/trust	6.4
Use spyware detection/protection software	6.2
Only do financial transactions from sites such as work etc where there are better facilities	4.8
Limit the value of online transactions	4.2
Don't store financial information or other personally sensitive information on the computer used to access the Internet	3.5
Keep up to date with the latest virus threats and hoaxes	3.2
Don't spend on line	3.1
Use privacy protection software (e.g. Evidence Eliminator, Window Washer, etc)	3.0
Use anti-SPAM software	2.4
Limited credit amount	1.5
Use anti-cookie software	0.7
Access Australian sites only	0.5

Table 12 Protective measures by number of transaction types undertaken

Protective measures	Transaction levels %				
	1	2	3	4	Total
Regularly update virus/worm protection software	23.3	25.6	34.7	41.4	32.4
Look for sites with trustmarks/certificates, privacy and security policy statements	9.8	15.8	15.3	29.3	18.1
Only deal with well known organisations online	5.3	14.0	17.3	20.6	15.2
Use firewall software or service	7.3	14.1	12.1	20.8	13.9
Don't know	20.4	6.9	4.9	2.2	7.6
Do nothing	10.9	12.7	4.4	2.7	6.9
Regularly change passwords	4.4	7.9	6.4	7.8	6.7
Use only secure sites/sites I know/trust	4.4	2.9	7.0	9.7	6.4
Use spyware detection/protection software	3.6	3.2	9.2	6.8	6.2
Only do financial transactions from sites such as work etc where there are better facilities	1.7	4.9	6.4	5.1	4.8
Limit the value of online transactions	9.0	4.1	3.7	1.5	4.2
Don't store financial or other personal information	3.4	3.4	3.1	4.2	3.5
Keep up to date with the latest virus threats and hoaxes	1.1	3.9	4.5	2.6	3.2

Regarding single versus multiple transactors, an increasing percentage of those who performed a range of transactions online also carried out appropriate protective measures (Table 12). For instance, those who performed four types of transactions were twice as likely as single transactors to regularly update virus/worm software (41 per cent compared to 23 per cent) and three times more likely to look for sites with trustmarks, privacy and security statements, etc. This suggests that many of the more intensive transactors are conscious of the need to adopt responsible practices, and they appear to have the knowledge and the means to put in place appropriate measures. For those who performed only one type of transaction, the categories receiving the most responses were:

- regularly updated their virus/worm protection (23 per cent);
- didn't know (20 per cent); or
- did nothing (11 per cent).

This might suggest that less intensive transactors are less concerned about protective behaviour, may lack experience or may be less aware about security measures.

Table 13 shows that of the active users, almost 50 per cent performed a single security or protective measure, 35 per cent performed multiple measures and more than 15 per cent did not know or had no security or protective measure.

There appears to be a correlation between security or protective measures undertaken and the number of types of transactions performed online. Figure 13 shows that the proportion of online transactors that adopted multiple protective measures (more than two) increased with the number of types of transactions performed online and conversely, the proportion with no protective measures diminished.

Table 13 Single versus multi security measures—active users

Number of security measures	%
No security measures or don't know	16
Single security measure	49
Multiple security measures	35
Total	100

Having mentioned experience as a possible driver of better online habits, it seems reasonable to test this hypothesis. Does a bad online experience modify behaviour? As indicated earlier, Pew has noted changes in the online habits of American Internet users in the face of increasing levels of intrusion, fraud and other unsatisfactory experiences.

To test what the Sensis data reveals, a more detailed look at the subgroup that had suffered the worst online experiences was carried out (i.e. those who had lost money, not received purchases or had received sub-standard purchases). The population for this analysis was restricted to persons who had ordered, booked or paid online. It should be noted, however, that the survey did not seek to explicitly identify behaviours resulting from negatives experiences with an online transaction service.

Table 14 shows how this sub-group sought to ensure their online security in comparison to the balance of users who ordered, booked or paid online (i.e. online shoppers and bill payers).

Figure 13 Security measures undertaken by number of types of transactions performed

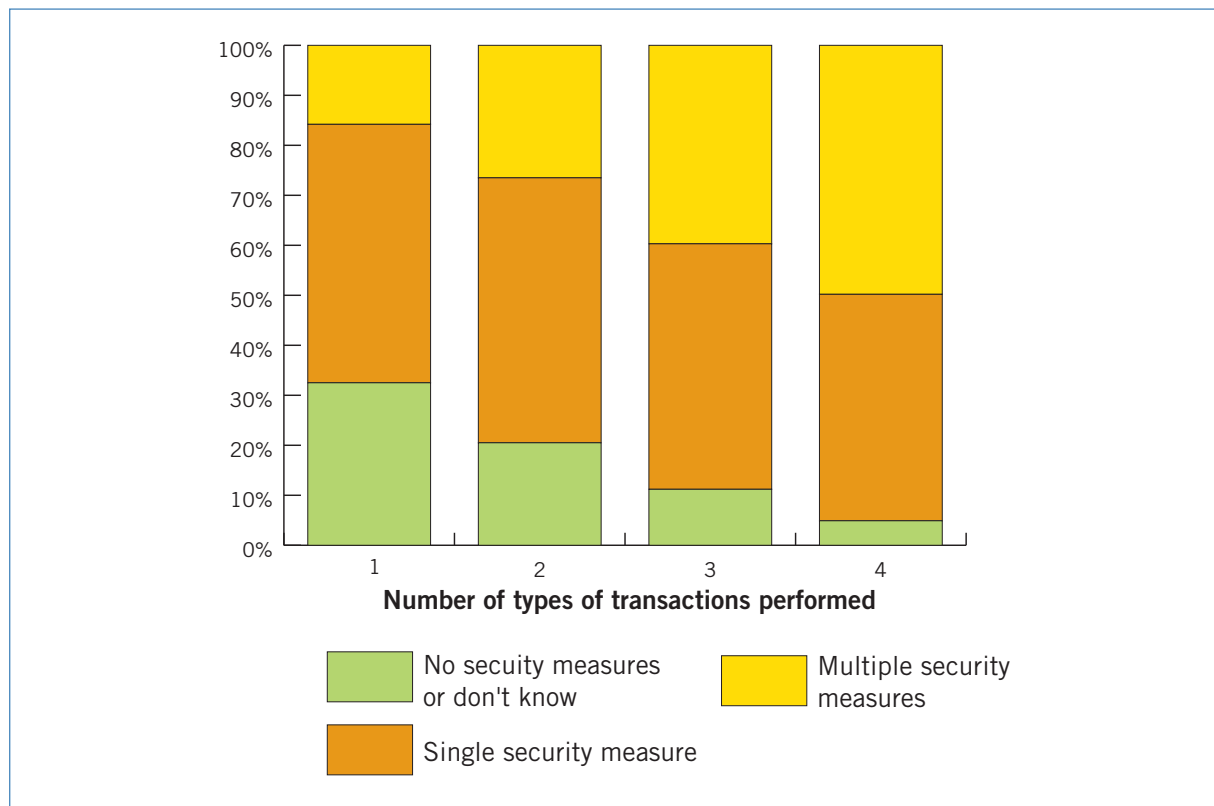


Table 14 How users ensure online security for those who order, book or pay online

Security measures	Lost money, substandard goods or not received goods?	
	NO %	YES %
Regularly update virus/worm protection software	33.3	31.2
Look for sites with trustmarks/certificates, privacy and security policy statements	17.8	27.8
Only deal with well known organisations online	15.2	21.9
Use firewall software or service	13.0	26.6
Regularly change passwords	7.0	3.1
Do nothing	6.6	1.8
Use only secure sites/sites I know/trust	6.6	5.8
Don't know	6.3	7.5
Use spyware detection/protection software	6.1	7.7
Only do financial transactions from sites such as work etc where there are better facilities	5.0	4.7
Limit the value of online transactions	4.8	2.6
Don't store financial information or other personally sensitive information on the computer used to access the Internet	4.3	0.0
Don't spend on line	3.4	1.3
Keep up to date with the latest virus threats and hoaxes	3.3	3.6
Use privacy protection	3.1	3.4
Use anti-SPAM software	2.1	4.9
Limited credit amount	1.8	0.3
Use anti-cookie software	0.8	0.2
Access Australian sites only	0.6	0.0
Passwords	0.4	0.1

The sub-group who had either lost money, received substandard purchases or had not received their purchases at all, showed a considerably higher propensity to seek out sites with trustmarks/certificates or privacy and security policy statements (28 per cent of the subgroup compared to 18 per cent of the larger complement). The subgroup also had a slightly higher proportion of individuals who only deal with well known organisations (22 per cent compared to 15 per cent).

These differences could suggest that bad online purchasing experiences lead to more selective and discerning buying habits, noting that in general, less than one third appear to have consciously adopted these selective buying habits. The data also suggests

that one in eight online shoppers and bill payers have had an unfavourable outcome at some time.

The other major difference that appears in the statistics relates to the use of firewall security software or services. The subgroup that had experienced a poor outcome was twice as likely to use firewalls (more than 26 per cent compared to 13 per cent). However as a general comment, the proportion of online shoppers and bill payers who appeared to be taking proper steps to protect themselves from spyware and other malicious agents is in the minority. While this may seem alarming, it may also suggest that there is a good deal of trust in the Internet as a purchasing channel (including by those whose trust stems from naivety). This suggestion is also supported by the high

number of Internet users who are engaging in such activities (more than nine million based on Sensis data estimates).

In the light of the concerns and experiences discussed earlier, there are many questions that arise about changes in the habits and practices of Internet users. For example, in a recent Pew Internet & American Life Project spyware report²⁴, Pew indicated that 91 per cent of Internet users had made at least one change in their online behaviour to avoid unwanted software programs. Among the changes that Pew identified are the following:

- 81 per cent of Internet users say they have stopped opening email attachments unless they are sure these documents are safe;
- 48 per cent of Internet users say they have stopped visiting particular Web sites that they fear might deposit unwanted programs on their computers;
- 25 per cent of Internet users say they have stopped downloading music or video files from peer-to-peer networks to avoid getting unwanted software programs on their computers; and
- 18 per cent of Internet users say they have started using a different Web browser to avoid software intrusions.

Gartner²⁵ has also noted a change in Internet user behaviour in the face of increasing phishing attacks and disclosures about unauthorised access to sensitive personal data. In a survey of 5000 United States adults, Gartner found that most online consumers no longer open email from companies or individuals they do not know from prior experience. They also indicate that three out of four online shoppers are now more cautious about where they buy goods online and that one in three are now buying fewer items than they otherwise would because of security concerns.

Although the Sensis survey of Australians does not reflect the magnitude of the United States findings, these statistics do reflect a definite trend for online shoppers to patronise the more secure and well known shopping sites.

In relation to the handling of unsolicited email, the Sensis survey does not contain comparable measures. However, survey questions that draw attention to such changes in online behaviour would be a very desirable inclusion in any future Australian research.

This leads to the final question: 'Why is the Internet an attractive medium for purchasing or paying bills?'

Why transact online?

Table 15 Why active users transact online

	%
More convenient/easier	47.9
Cheaper	27.1
Couldn't transact any other way	16.4
Overseas or interstate purchase	14.4
Don't buy on line	9.0
It is quicker/saves time	5.3
Outside normal office hours	4.8
Better variety of product offered	3.0
Able to see prices and products/ gives information	3.0
Just to try it out/looks like fun	1.4
Better deals on the net	0.6

The most frequently cited reasons for using online activities were related to convenience and relative cheapness (Table 15). In addition, some services are only available online (such as eBay) and this largely accounts for the responses to 'couldn't transact any other way'. A further advantage is the ability to select easily from interstate or overseas sources.

The subset of users who ordered, booked or paid online showed no significant differences when compared to active users overall.

With respect to multiple transactors (Table 16), survey results show that a far greater proportion of those who performed more than two types of transactions online did so because they found it to be convenient and easier, and responses to this answer were almost double that of the single transactor group. Relative cheapness and the ability to purchase from interstate and overseas sources also showed an upward trend as the number of transaction types increased. An inverse relationship is evident for those who 'don't buy online'. Single transactors were the least likely to buy online: 28 per cent reported that they don't buy online.

Table 16 Reasons for transacting online by number of types of transactions undertaken

Why transact online?	Transactional levels %			
	1	2	3	4
More convenient/easier	27.8	46.0	55.1	54.8
Cheaper	18.8	25.8	29.7	30.9
Couldn't transact any other way	16.3	17.3	13.8	18.8
Overseas or interstate purchase	8.3	14.7	14.2	18.7
Don't buy on line	28.1	9.1	4.6	0.6
It is quicker/saves time	3.1	7.8	2.5	8.3
Outside normal office hours	0.6	5.3	6.4	5.4
Better variety of product offered	1.0	3.4	3.5	3.6
Able to see prices and products/gives information	2.7	3.3	3.9	1.9
Just to try it out/looks like fun	2.3	0.6	1.5	1.1
Better deals on the net	0.7	0.0	1.0	0.6

As a concluding remark, the relative size of the active group in combination with earlier data showing that shopping and bill paying activities are growing, suggests that the convenience and other advantages of using the Internet appear to vastly outweigh any of the concerns and bad online experiences.

While less than one in 25 Australian 'active' Internet users claimed to have lost money online and slightly more than one in 20 claimed to have not received purchases or received substandard purchases, these experience do not appear to have had an impact on the general level of online shopping and bill payment.

Endnotes

- 1 The Organisation for Economic Co-operation and Development (OECD) in 2000 reported that 23 per cent of 'non-residential fixed capital formation' in Australia was ICT related; the 3rd highest in the OECD.
- 2 Policy relevant indicators and empirical analysis for the information society: a discussion of WPIIS outputs and ideas for future work, Working Party on Indicators for the Information Society; Committee for Information, Computer and Communications Policy; Directorate for Science, Technology and Industry, OECD, April 2004. [DSTI/ICCP/IIS(2004)1]
- 3 Nielsen//NetRatings
- 4 www.security.ia.net.au
- 5 www.dcita.gov.au/ie/publications/2004/january/current_state_of_play_-_december_2003/e-service_capability_and_online_activities#broadband
- 6 A zombie computer (abbreviated zombie) is a computer attached to the Internet that has been compromised by a hacker, a computer virus, or a trojan horse, and performs malicious tasks of one sort or another, under the direction of the hacker. See en.wikipedia.org/wiki/Zombie_computer
- 7 Scoping study for the measurement of trust in the online environment, Working Party on Indicators for the Information Society; Committee for Information, Computer and Communications Policy; Directorate for Science, Technology and Industry, OECD, April 2005 [DSTI/ICCP/IIS(2005)1]
- 8 A Survey of Trust in Internet Applications, Tyrone Grandison and Morris Sloman, Imperial College
- 9 Trust in Electronic Environments, Chopra and Wallace—presented at the International Conference on System Sciences 2003
- 10 The Role of ICT in Building Communities and Social Capital, DCITA 2005
- 11 Stone and Hughes 2002 cited in DCITA (9), p.32
- 12 Privacy and the Community, 2001 www.privacy.gov.au/publications/rcommunity.pdf
- 13 *Learning to Innovate—Re-perceiving the global information society*, January 2005 Information Society Commission www.isc.ie/downloads/34843_InfoSoc.pdf
- 14 www.dcita.gov.au/ie/benchmarking
- 15 ABS *Business Use of Information Technology, 2003–04* and *Farm Use of Information Technology 2002–03*
- 16 www.about.sensis.com.au/knowledge/research.php
- 17 Categories falling below the top 5 are not included because the low level of responses for these categories results in a standard error of more than 25 per cent, and in some cases, of more than 50 per cent.
- 18 www.ipsos-na.com/news/pressrelease.cfm?id=2765
- 19 Internet use in Europe; Security and trust, EUROSTAT, 2005
- 20 www.bbbonline.org/UnderstandingPrivacy/library/harrissummary.pdf
- 21 www.sophos.com/spaminfo/articles/dirtydozen05.html
- 22 www.techworld.com/infosec/features/index.cfm?featureID=1372
- 23 Internet use in Europe; Security and trust, EUROSTAT, 2005
- 24 www.pewInternet.org/pdfs/PIP_Spyware_Report_July_05.pdf

DEPARTMENT OF COMMUNICATIONS, INFORMATION TECHNOLOGY AND THE ARTS
www.dcita.gov.au