TRENDS & ISSUES
in crime and criminal justice

Australian Government
Australian Institute of Criminology

No. 330 February 2007

Internet purchasing: perceptions and experiences of Australian households

Tony Krone and Holly Johnson

There are few reliable national data on the habits and experiences of Australian householders using the internet. In the 2004 International Crime Victimisation Survey (ICVS), the Australian Institute of Criminology (AIC) canvassed a range of issues related to Australian householders and their access to the internet, including whether the internet was used to make purchases, the types of problems experienced in online purchases, and the types of distributed computer problems experienced. The survey provides some basic estimates of householder exposure to online purchasing problems and other credit card abuse. The data indicate that the monetary risk associated with online transactions is lower than for other credit card abuse, and that generally there are fewer problems associated with such transactions, but that problems associated with online transactions are increasing. It is likely that as online transactions increase, the number of victims will also increase, as will associated monetary losses. Educating individuals about the risks, and the need for preventative action, will be challenging for private and public sector agencies.

Toni Makkai
Director

Fraud and internet crime are recognised as important issues for governments and private businesses worldwide. An area of growing concern is the impact of criminal activity on householders who use the internet. Householders use the internet at home for various purposes including work, education, leisure, communication, accessing government services and managing the household. The internet provides the means to perform a variety of specific tasks such as:

- managing banking and financial services
- obtaining information about rights and obligations from government
- researching information
- researching services and products
- communicating generally
- trading in goods and services.

Internet based services offer many advantages to providers and to users. Principal advantages are convenience, speed, accessibility, timeliness and cost effectiveness. Many computer applications were originally designed to deliver these advantages rather than providing high levels of security. The way in which householders use the internet has important implications not just for their own security but also for the security of other users. Security in this context is considered in two ways:

- the system being used by the householder, including the operating system and any applications in use
- the conduct of the online transaction encompassing the person or organisation at the other end of the transaction and the security measures used to protect identity and payment information during the course of the transaction.

ISSN 0817-8542

ISBN 978 1 921185 27 4

GPO Box 2944
Canberra ACT 2601
Australia
Tel: 02 6260 9272
Fax: 02 6260 9293

For a complete list and the full text of the papers in the *Trends & issues in crime and criminal justice* series, visit the AIC website at: http://www.aic.gov.au

Disclaimer:
This research paper does not necessarily reflect the policy position of the Australian Government.

Project no. 0088
Ethics approval no. PO75
Dataset no. 0079

Systems security

Initially favouring functionality over security, the operating systems that support internet applications were developed in ways that made them susceptible to attack or intrusion from other people using the same computer or on other computers communicating across a network. There are three typical ways of attacking other computers over a network. The first is to directly hack into a specifically targeted computer when it is connected to a network. The second is to distribute automated software such as viruses, worms and other malicious software across a network and opportunistically affect computers that are exposed on that network. The third is to use a computer or a series of compromised computers to specifically target another computer, as in a distributed denial of service attack.

There has been a transition from attacks on computers to the compromising of computers so that they can be used to attack other computers. Where a number of computers are compromised and can be remotely controlled by another user, this is referred to as a botnet. Botnets are used to effect a number of criminal actions or precursor actions to support criminal activity. Examples include harvesting of email accounts for spamming, the distribution of spam and the launching of distributed denial of service attacks.

Significant improvements have been made to overcome many of the vulnerabilities within a number of operating systems and software applications. There have been numerous cases reported of hackers exploiting known vulnerabilities. An exploit may have malicious or criminal intent and degrade the functionality of the internet or be used to steal from or defraud other internet users. An important aspect of maintaining the integrity and security of the internet is to ensure that at a minimum, users keep their operating system up to date, use up to date antiviral software and regularly scan their computer for spyware.

Basic guidelines for maintaining systems security

To maintain systems security, users must:

- keep the operating system up to date with all security patches offered by the vendor
- keep application software such as browsers, players and other applications regularly updated
- install and use reliable antiviral software that is regularly updated and used to scan the computer
- install and use reliable anti-spyware software that is regularly updated and used to scan the computer
- install and operate a firewall.

Basic guidelines for maintaining transaction security

To maintain transaction security users must:

- assess the risk of dealing with an unknown vendor and verify that the services are provided by legitimate and reputable companies
- ensure that security and encryption are applied to the transmission of sensitive credit or bank account information
- choose safer payment options that offer some form of consumer protection
- avoid using public facilities such as internet cafes to transmit credit or bank account information online
- avoid using insecure wireless connections to transmit credit or bank account information online.

Transaction security

Apart from the issue of systems security, an internet user may also be vulnerable to exploitation or attack in terms of the security applied in conducting any online transaction. Here the risk is of being deceived by a fraudulent trader, or having valuable personal security and banking details intercepted by a third party or misapplied by the trader.

Whether users will continue to turn to and rely on the internet will depend, at least in part, on their perceptions and experiences of the reliability and safety of online transactions.

The International Crime Victimisation Survey

The Australian component of the ICVS was conducted by the AIC in 2004. The sample consisted of 7,001 households in total: the Australian Government Attorney-General's Department funded a survey of a random national sample of 6,000 respondents, and the Department of Immigration and Multicultural and Indigenous Affairs funded an additional sample of 1,001, selected from recent immigrants from Vietnam and the Middle East. One person 16 years of age or older was selected from each household for an interview. Data were collected using computer-assisted telephone interviewing (CATI). An overall response rate of 53 percent was achieved and households were weighted to represent the Australian population (see Challice & Johnson 2005 for details of the methodology).

The primary objective of the ICVS is to provide estimates of the prevalence of selected violent and property crimes, the percentage reported to the police, and respondents' perceptions of crime and the criminal justice system. A special module of questions was added to the Australian component of the 2004 ICVS to produce estimates of internet purchasing, modes of payment, the prevalence of problems experienced with online and offline purchasing using credit or bank cards, estimates of associated loss, and reporting behaviour. Questions were also asked about the extent to which householders were exposed to computer problems commonly distributed across the internet. A five-year reporting framework for questions regarding crime victimisation is used for the ICVS generally and this was applied to obtain estimates of online and offline purchasing problems. Survey interviews were conducted between August and November 2004. Estimates were produced of internet and other credit card related problems within the five years prior to the survey (since 1999), as well as in the previous complete calendar year (2003).

Internet related crime is an under-studied field and a dedicated survey is needed to fully explore this area. In the absence of a dedicated survey and because of a lack of reliable data on householder experiences of problems when using the net, the opportunity was taken to add a short section to the ICVS. Inevitably this approach involved an element of compromise. The relevant section of the survey instrument was constrained to fit within the larger aims of the ICVS and should be considered a pilot study on a topic that warrants further exploration. It is important to undertake further research in relation to both householder and industry use of the internet to develop a more complete picture of the risks associated with its growing use. For example, a major issue for investigation is the use of the internet by householders to conduct online banking.

Internet access and internet purchasing

Australians are increasingly embracing the use of information and communications technologies in the home. According to the Australian Bureau of Statistics (ABS), the proportion of Australian households with access to a computer rose from 61 percent in 2002 to 66 percent in 2003. The proportion of households with access to the internet rose from 16 percent in 1998 to 46 percent in 2002 and 53 percent in 2003 (ABS 2004). The proportion of adults who accessed the internet from any location was slightly higher: 41 percent in 1999 and 58 percent in 2002 (ABS 2004). The ICVS indicated that 70 percent of households had access to the internet at some point over the five-year period from 1999 to 2004 (Figure 1). Respondents to the ICVS were asked if anyone in the household had purchased anything over the internet by giving credit card or bank account details online within the previous five years. Forty-three percent of all households had made an online purchase in this way. This represents 61 percent of households with internet access.

The amount of data transferred over the internet is staggering. ABS figures show that in March 2004 there were 4.48 million household ISP subscribers downloading 4.74 terabytes of data in that month alone (ABS 2004). One terabyte is the equivalent of 1,024 gigabytes and the entire print collection of the US Library of Congress is estimated to be the equivalent of about 10 terabytes (Lyman & Varian 2003).

Reasons for not making purchases online

Respondents who had internet access but indicated that no internet purchase had been made by anyone in their household in the previous five years were asked why. The primary reason was a concern about the security of providing credit card details over the internet (63%). About one in five said they preferred to shop in person. One in 10 hadn't seen anything they wanted to buy and about one in 10 reported that they lacked a credit card needed to make an internet purchase, or that they were not confident enough with computer technology. Two percent cited other reasons (Figure 2).

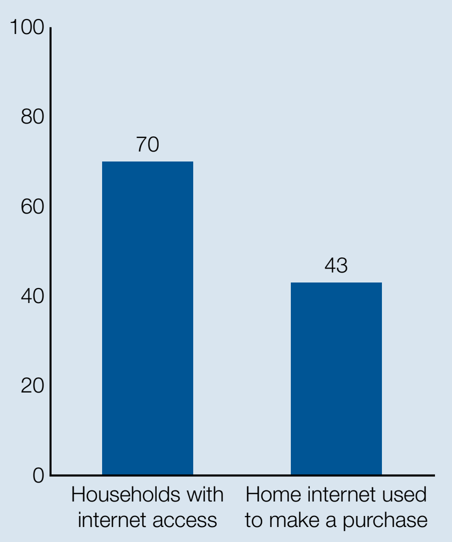
Mode of payment

Among those households who made a purchase online, the most common form of payment was by giving credit card or bank account details online. Sixty-one percent of households making an internet purchase used these methods alone. Eleven percent of households made an internet purchase by paying in other ways, such as by paying an invoice on receipt of goods. A further 28 percent of households had used both online payments and other methods to make internet purchases (Figure 3).

Problems with online purchases

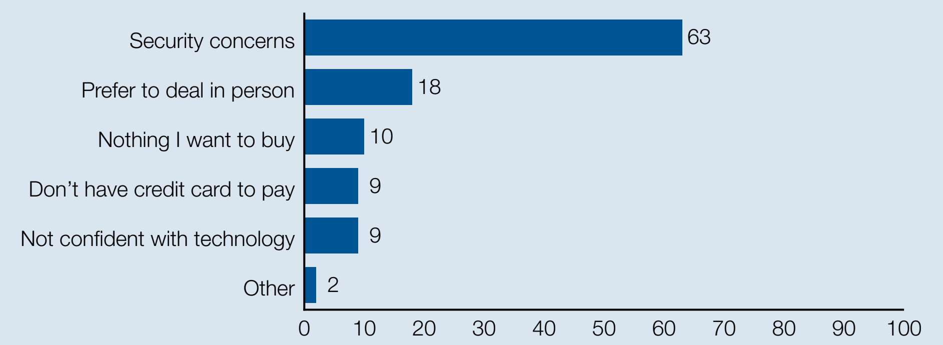
A total of 11 percent of households that made internet purchases by giving credit card or bank details online experienced problems. Internet

Figure 1: Internet access and purchasing, over the past 5 years (percent)



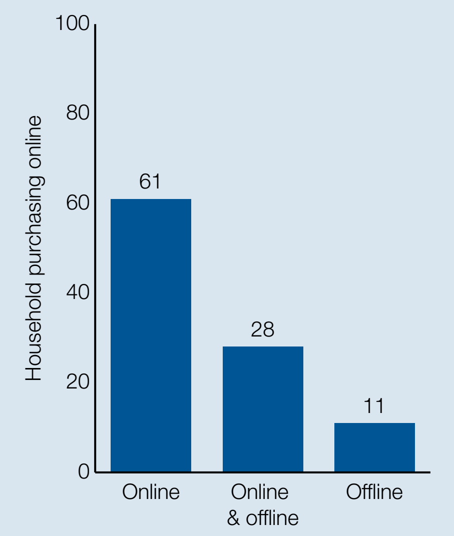
Source: AIC ICVS 2004 [computer file], n = 7,001

Figure 2: Reasons for not making internet purchases (percent)



Source: AIC ICVS 2004 [computer file], n = 1,828

Figure 3: Mode of payment for internet purchases (percent)



Source: AIC ICVS 2004 [computer file], n = 2,989

Table 1: Problems with online purchases

	n	%
Problems experienced		
Households who made purchases by giving card details	2,654	100
Households who had one or more problems	289	11
Problems experienced		
Not as advertised (quality or quantity)	106	4
Goods/services not provided	80	3
Money taken at another time	80	3
More money taken than authorised	57	2
Other	21	1
Total one or more problems	344	
Monetary loss		
Households with a problem that led to a monetary loss	222	77
Range of loss ($)	5–12,000	
Mean ($) (range)	399 (232–567)	
Median ($)	100	
Reported to		
Police	8	3
Bank	74	26
Other agency	59	21
Don't know if reported	7	3
Not reported	146	51
Total	289	100

Source: AIC ICVS 2004 [computer file]

purchasers were asked if a range of specific problems were experienced. The options canvassed were not limited to fraudulent or criminal incidents and included goods not being as advertised as to either quality or quantity.

The percentages of internet purchasers who experienced the problems listed in the questionnaire are shown in Table 1. Most prevalent were situations in which the goods or services received were not as advertised (4%). Occurring at similar frequency were situations where the goods or services were not provided at all (3%) and where money was taken from the purchaser's account at another time that was not authorised (3%). Two percent reported that more money was taken at the time of the purchase than was agreed to. Other unspecified problems were claimed by one percent of online purchasers.

When problems were experienced

Approximately half (47%) the reported problems occurred in the period from January 2004 (interviewing took place from August to November 2004). Twenty-four percent of problems occurred in 2003, 26 percent prior to that (back to 1999) and in three percent of cases the time could not be specified. The almost twofold increase in reported instances from 2003 to 2004 (a partial year) suggests a growing incidence of internet related purchasing problems as the number of internet purchasers increases. The ICVS asked about repeat incidents in the complete calendar year of 2003, and 22 percent of those experiencing problems reported experiencing more than one in that period.

Value of losses

Just over three-quarters (77%) of problems reported resulted in a monetary loss and the amounts involved ranged from $5 to $12,000. Households were asked to estimate the value of the loss before any repayment through insurance, banks or legal action. The average (mean) loss was almost $400 and the median loss was almost $100. The median value indicates that half the incidents with monetary loss fell below $100 and half fell above. Mean losses are higher as very high losses bring up the average.

The 289 households where respondents reported a problem associated with internet purchases represent four percent of the total sample. Weighted to the total population, the figures for claimed financial loss represent an estimated 214,000 Australian households suffering a financial loss while conducting an internet purchase. Weighting these losses to the 214,000 households results in an estimated total loss of between $50m and $121m during the five-year period of the survey.

Reporting behaviour

Overall, half of all households that experienced difficulties in relation to an internet purchase reported the problem to the police, a bank or some other agency. Incidents were more likely to be reported to a bank (26%) or another agency (21%) – typically the company through which the purchase was made – than to the police (3%). Less than five percent did not know whether the problem had been reported, perhaps because household members other than the respondent had experienced the problem.

Other forms of credit and bank card misuse

Other types of credit card fraud not involving the internet were addressed in the survey through the following question:

Table 2: Offline credit card fraud

	n	%
Total sample	7,001	100
Total had credit/bank card used illegally (excluding internet purchase)	371	5
Monetary loss		
Households with a problem that led to a monetary loss	324	87
Range of loss ($)	2–50,000	
Mean ($) (range)	2,230 (1,697–2,764)	
Median ($)	700	
Reported to		
Police	89	24
Bank	265	72
Other agency	30	8
Don't know if reported	3	1
Not reported	46	12
Total	371	100

Source: AIC ICVS 2004 [computer file]

> (Excluding anything you have already mentioned) in the last 5 years, has anyone illegally used any of your credit or bank cards, or your card details, to buy things or withdraw cash?

This question measures credit and bank card misuse that is not attributed by the respondent to an online purchase. Illegal use of credit or bank cards may occur as the result of use of a stolen or lost credit card, or the theft of credit or debit card account information, and may be perpetrated either online or offline. Results are shown in Table 2.

When problems were experienced

In contrast to online purchasing problems, one-fifth of other forms of credit card and bank card misuse occurred in the period from January 2004. Twenty-three percent of problems occurred in 2003, 56 percent prior to that (back to 1999) and in one percent of cases the time could not be specified. These results suggest a fall in these types of incidents in recent years but an increase in online purchasing problems.

The ICVS asked about repeat incidents in the complete calendar year of 2003 and 32 percent of problems were reported to have occurred more than once in that period. This is 10 percentage points higher than the rate of repeat victimisation reported in relation to online problem transactions and may reflect instances where a credit or bank card is misused multiple times although several instances may stem from a common event, such as the stealing of a credit card from a purse or wallet.

Value of losses

Compared with internet related purchasing difficulties, a higher proportion of instances of unauthorised use of credit or bank cards resulted in a monetary loss. The range, the mean loss and the median loss were substantially higher than for problems attributed to online payment transactions. Given that the question asked about illegal use of a credit or bank card information to buy things or withdraw cash, it might be expected that the reporting of monetary loss would be high. Eighty-seven percent of instances of credit or bank card misuse resulted in a monetary loss and the amounts involved ranged from $2 to $50,000. Respondents were asked to estimate the value of the loss before any repayment through insurance, banks or legal action. The average (mean) loss was almost $2,230 and the median loss was almost $700.

The number of households where the respondent reported a problem associated with unauthorised use of credit or bank cards offline was 371, which represents five percent of the total sample. Weighted to the total population, it is estimated that 312,000 households were affected by offline credit and bank card misuse and that these activities resulted in a cost between $529m and $862m over the five-year period.

Reporting behaviour

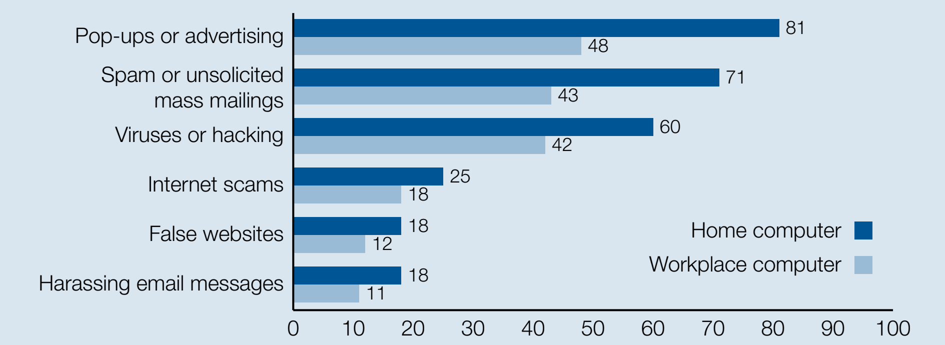
These incidents were more likely to be reported than problems with online payment transactions. Overall, 88 percent of households where offline credit or bank card misuse had occurred said the problem had been reported to the police, a bank or some other agency. Almost one-quarter (24%) were reported to the police. However, incidents were more likely to be reported to a bank (72%) and fewer were reported to another agency (8%).

The experience of distributed computer problems

Other types of internet related incidents occurring on home and work computers can have a significant impact on individuals and businesses. This survey inquired about experiences of various criminal and non-criminal problems when using computers at home and in the workplace. The various problems were reported by between 18 percent and 81 percent of all households with internet access (Figure 4). Thirty-nine percent of the sample had internet access through a workplace computer. Workplace related incidents were reported at a lower rate for each problem, ranging from 11 to 48 percent of those with workplace internet access.

Not surprisingly, the most commonly reported problem for householders was pop-ups or advertising, affecting just over 80 percent of households with internet access. Spam was the next most common followed by viruses or hacking and both these problems affected more than half of households with internet access. One in four households with internet access were exposed to internet scams and almost one in five were exposed to false websites and harassing email messages.

Figure 4: Households experiencing distributed computer problems on home and workplace computers (percent)



Source: AIC ICVS 2004 [computer file], n = 4,869 household and 2,729 workplace computers

Conclusion

This survey shows that concern about the security of internet transactions is a major inhibitor of householder use of the internet to make purchases, and yet the experiences of those who engage in online purchasing using their credit or bank card indicate a lower level of risk of monetary loss than more traditional forms of credit or bank card misuse. Over the survey period the amount claimed by householders to have been lost due to problems with internet purchases represented $50–121 million across all households compared with $529–862 million in relation to other forms of credit or bank card misuse.

The apparent differences in risk may reflect a degree of circumspection on the part of internet purchasers as to the value of transactions completed online. In any event, results indicate that, at least for the survey period, the illegal use of credit or bank cards occurred at a rate similar to problems in making purchases over the internet using credit or bank card details online. There was an upward trend in the incidence of online payment transactions, while other forms of credit card and bank account misuse decreased over the survey period.

Importantly, even allowing for the wider category of problems related to purchases completed online, the rate of reporting of such problems is much lower than for other forms of credit or bank card misuse. This may simply be a reflection of the lower values involved or uncertainty regarding the actual terms of the transaction generally, so that the purchaser puts the problem down to experience and vows to be more careful in the future. Whatever the cause, under-reporting of problems with internet purchases is an issue for law enforcement in responding to internet based crimes that are high in volume and low in value. It also means that internet based purchasing problems will be severely undercounted in police statistics.

While problems with internet purchasing appear to be growing, the incidence of distributed computer problems such as spam and viruses or hacking is already high. The higher levels of exposure to scams, false websites and harassing email reported by householders compared with workplace internet access could be a matter of awareness on the part of householders who, of necessity, are the administrators of their home computer and thus more likely to have to deal with problems directly. In the workplace, computer systems may be protected by staff who are professionally trained computer specialists.

The results of this survey serve as baseline indicators of householder experiences when using the internet. Further research is needed to explore other types of internet problems, such as those associated with online banking.

Acknowledgment

The Australian Government Attorney-General's Department and the (then) Department of Immigration and Multicultural and Indigenous Affairs funded the Australian component of the ICVS.

References

All URLs were correct at 14 November 2006

Australian Bureau of Statistics 2004. *Measures of a knowledge-based economy and society, Australia*. Canberra: Australian Bureau of Statistics. http://www.abs.gov.au/ausstats/abs@.nsf/94713ad445ff1425ca25682000192af2/4f377c757da4394fca256d97002c1a68!OpenDocument

Challice G & Johnson H 2005. *The Australian component of the international crime victimisation survey (ICVS)*. Technical and background paper no. 16. Canberra: Australian Institute of Criminology http://www.aic.gov.au/publications/tbp/tbp016/

Lyman P & Varian H 2003. *How much information? 2003*. Berkeley CA: University of California Berkeley, School of Information Management and Systems http://www.sims.berkeley.edu/research/projects/how-much-info-2003/index.htm

**Dr Tony Krone was a high tech crime analyst engaged as part of a research partnership between the AIC and the Australian High Tech Crime Centre.
Dr Holly Johnson was a visiting research fellow at the AIC during 2003–05.**

**General editor, *Trends & issues in crime and criminal justice* series:
Dr Toni Makkai, Director,
Australian Institute of Criminology,
GPO Box 2944 Canberra ACT 2601
Note: *Trends & issues in crime and criminal justice* papers are peer reviewed.**

The AIC is a statutory body with a Board of Management comprising Australian, state and territory government representatives, administered under the *Criminology Research Act 1971*.