# 4

# Community Awareness and Vulnerability

## Introduction

4.1 This chapter discusses the current level of e-security awareness among Australian home users and small businesses. The evidence demonstrates a considerable inconsistency between levels of awareness of e-security threats and actual online behaviour, indicating that home users and small businesses remain highly vulnerable to a range of cyber crime types.

## Levels of Awareness and Uptake of E-security Measures

4.2 As mentioned previously in this report, there is a wide variety of inconsistent and often incomparable information on the level of cyber crime activity due to varying definitions of cyber crime, fragmented intelligence gathering and the under reporting of cyber crime by victims.[1]

4.3 These data collection issues have also given rise to a number of conflicting statistics on the level of cyber crime awareness in the Australian community. While some sources indicate that the level of awareness is high, other sources show that this does not necessarily translate into better online practices.

4.4 Evidence to the Committee supports the notion that home users have some awareness of cyber security risks:

[1] Mr Alistair MacGibbon, Internet Safety Institute, *Transcript of Evidence*, 11 September 2009, p.63.

- a July 2009 Australian Communications and Media Authority (ACMA) survey of Australian home users between the ages of eight and seventeen found that 75 per cent of respondents knew not to divulge personal details on the internet;[2]
- a March 2009 ACMA survey of 1,631 adult home users found that 81 per cent of respondents assessed their online skills as average or above;[3]
- a 2008 survey by internet security provider AVG found that 77 per cent of Australian respondents were aware of the need to regularly update their internet security software; [4]
- a 2006 survey by the Consumers' Telecommunications Network (CTN) found that almost 90 per cent of respondents were aware of and understood spam, and more than 66 per cent of respondents were aware of and understood malware;[5] and
- the same 2006 CTN survey found the 75 per cent of respondents recognised and did not respond to scam emails.[6]

4.5 The evidence also suggested that Australian small businesses possess some understanding of cyber security issues:

- a 2009 global survey by Symantec of 1,425 small and medium sized enterprises (SMEs) found that these businesses are acutely aware of today's security risks;[7]
- a 2009 ABS survey of Australian small businesses found that 85 per cent of respondents used one or more computer security tools such as anti-virus or encryption software;[8] and
- a 2006 AusCERT survey of Australian organisations found that 99 per cent used virus protection and 98 per cent used firewalls.[9]

[2] ACMA, *Click and connect: Young Australians' use of online social media – 02: Quantitative research report*, ACMA, July 2009, p.10.

[3] ACMA, *Australia in the Digital Economy: Trust and Confidence*, ACMA, March 2009, p.29.

[4] AVG, *Australia Tops Global Cyber Crime Impact Survey*, media release, AVG, 10 June 2008, viewed 21 January 2010, <http://www.avg.com.au/news/avg_cyber_crime_impact_survey/>.

[5] Consumers' Telecommunications Network (CTN), *Surfing on thin ice: consumers and malware, adware, spam and phishing*, CTN, November 2009, p.9.

[6] Consumers' Telecommunications Network, *Surfing on thin ice: consumers and malware, adware, spam and phishing*, CTN, November 2009, p.33.

[7] Symantec Corporation, *Submission 32*, p.9

[8] K Richards, *The Australian Business Assessment of Computer User Security: a national survey*, Australian Institute of Criminology, 2009, p.xii.

[9] AusCERT, *Computer Crime and Secuirty Survey*, AusCERT, 2006, p.8.

4.6 However, a range of other evidence indicated that Australian home users and small businesses still take insufficient precautions against cyber crime.[10] This evidence includes, for example:

- a March 2009 ACMA survey of 1,631 adult home users found that only 49 per cent of those who assessed their online skills as high had installed anti-virus software;[11]
- a 2008 AusCERT survey of 1,001 Australian adult home users found that 11 per cent of respondents never update their operating system and eight per cent never update their anti-virus software; [12]
- the 2008 AusCERT survey also found that 75 per cent of respondents connect to the internet using an administrator account and 30 per cent had clicked on links in spam emails (both of which significantly reduce the effectiveness of computer security mechanisms);[13]
- the 2009 Symantec survey of SMEs found that out-of-date or improper security measures each accounted for over a third of the security breaches against Australian SMEs;[14] and
- only ten per cent of respondents to a 2006 AusCERT survey of Australian organisations thought they were managing all aspects of computer security well.[15]

4.7 The level of cyber crime in Australia demonstrates that end users are not heeding advice on e-security threats. For example, while the Australian banking industry said that customers are highly aware of the threat posed by phishing emails,[16] a 2007 ABS survey estimated that, in the twelve months prior to the survey, 30,400 Australians were the victim of online phishing scams.[17]

[10] See for example: Australian Computer Society (ACS), *Submission* 38, p.8; Dr Russell Smith, Australian Institute of Criminology (AIC), *Transcript of Evidence*, 19 August 2009, p.9; Mr Peter Coroneos, Internet Industry Association (IIA), *Transcript of Evidence*, 11 September 2009, p.18; Australian Federal Police (AFP), *Submission 25*, p.10; AusCERT, *Submission 30*, p.12.

[11] ACMA, *Australia in the Digital Economy: Trust and Confidence*, ACMA, March 2009, p.39.

[12] AusCERT, *AusCERT Home Users Computer Security Survey 2008*, AusCERT, 2008, p.3.

[13] AusCERT, *AusCERT Home Users Computer Security Survey 2008*, AusCERT, 2008, p.3.

[14] Symantec Corporation, *Symantec Survey Reveals More than Half of Small and Midsized Businesses in Australia and New Zealand Experience Security Breaches*, media release, Symantec Corporation, 12 May 2009, p.1.

[15] AusCERT, *Computer Crime and Security Survey*, AusCERT, 2006, p.4.

[16] Mr Anthony Burke, Australian Bankers Association NSW Inc, and Mr John Guerts, Commonwealth Bank of Australia, *Tanscript of Evidence*, 8 October 2009, p.59.

[17] Australian Bureau of Statistics (ABS), *2007 Personal Fraud Survey*, ABS, Cat. No. 4528.0, 2007, pp.14, 21.

4.8 Similarly, despite an apparent awareness of the threats posed by identity theft and fraud, the ABS survey estimated that 76,000 Australians were victims of online credit card or bank card fraud in the year preceding the survey.[18]

4.9 Even where end users do take sufficient technical precautions, they may still fall victim to online scams due to emotional vulnerabilities. For example, the ACCC informed the Committee of an increasing number of dating or romance scams.[19] Additionally, the 2006 ABS survey indicated that at least 31,700 Australians were the victims of online scams in the twelve months prior to the survey.[20]

4.10 The continued impact of romance scams provides a particularly good example of how knowledge of cyber crime risks is not necessarily translating into protective actions. The Queensland Police Service (QPS) informed the Committee that, in the case of romance scams, 76 per cent of victims who lost large amounts of money continued to willingly participate in such scams despite being notified by the QPS that they were being victimised.[21] Similarly, Mr Peter Shenwun, Consular Minister, Nigerian High Commission in Australia, told the Committee that many victims of advance-fee fraud originating out of Nigeria seek to continue contact with scammers, despite being advised not to by Nigerian authorities.[22]

4.11 AusCERT argued that the range of seemingly inconsistent evidence indicates that home users may hold misconceptions about the level of protection provided by their security measures. AusCERT's *Home Users Computer Security Survey 2008* found that:

- 68 percent of people were confident or very confident in managing their own computer security;
- 92 per cent thought their ISP should inform customers of malware infections (which does not necessarily occur); and
- 46 per cent incorrectly believed that data exchanged with secure websites cannot be accessed by hackers.[23]

[18] ABS, *2007 Personal Fraud Survey*, ABS, 2007, pp.14, 21, 24.

[19] Mr Scott Gregson, Australian Competition and Consumer Commission (ACCC), *Transcript of Evidence*, 18 November 2009, p.1.

[20] ABS, *2007 Personal Fraud Survey*, ABS, 2007, pp.14, 21, 24.

[21] Detective Superintendent Brian Hay, QPS, *Transcript of Evidence*, 17 March 2010, pp.3-4.

[22] Mr Peter Shenwun, Nigerian High Commission, *Transcript of Evidence*, 17 March 2010, p.1.

[23] See for example: AusCERT, *Submission 30*, p.12; AusCERT, *AusCERT Home Users Computer Security Survey 2008*, AusCERT, 2008, p.3.

4.12 The Tasmanian Government stated that although there appears to be a general awareness in the community of the need for some level of protection, most home users and SMEs do not have adequate security.[24]

4.13 The Australian Computer Society argued that Australians seem to be aware of, and are taking precautions against, old cyber crime threats but are not aware of, or taking steps against, new and emerging cyber crime threats.[25] For example, while users may be installing anti-virus software to combat some e-security risks, QPS informed the Committee that they observed a 1,000 per cent increase in the incidence of romance scams between 2006 and 2009.[26]

## Issues that contribute to low levels of awareness

4.14 The Committee received evidence on a number of factors that contribute to the low level of awareness of cyber crime threats among Australia home users and small businesses:

- limitations of current educational initiatives;[27]
- a complex public policy response to cyber crime;[28] and
- inadequate online safety mechanisms that may not alert end users to new cyber security threats and attacks.[29]

4.15 These issues, and proposals to deal with them, are examined more thoroughly in the following chapters.

[24] Tasmanian Government, *Submission 51*, p.3.

[25] ACS, *Submission 38*, p.8.

[26] Detective Superintendent Brian Hay, QPS, *Transcript of Evidence*, 17 March 2010, p.4.

[27] See for example: Consumers' Telecommunications Network, *Surfing on thin ice: consumers and malware, adware, spam and phishing*, CTN, November 2009, p.21; Internet Safety Institute, *Submission 37*, p.10; Mr Terry Hilsberg, ROAR Film Pty Ltd, *Transcript of Evidence*, 8 October 2009, p.69; Telstra, *Submission 43*, p.4.

[28] See for example: Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.15; Mr Mike Rothery, Attorney General's Department (AGD), *Transcript of Evidence*, 25 November 2009, p.14; Commander Neil Gaughan, AFP, *Transcript of Evidence*, 9 September 2009, p.2; Internet Safety Institute, *Submission 37*, p.8; Fujitsu, *Submission 13*, p.7; IIA, *Submission 54*, p.5.

[29] See for example: Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.9; Mr Scott Ridgway, ACCC, *Transcript of Evidence*, 18 November 2009, p.7; Dr Paul Brooks, *Transcript of Evidence*, 9 October 2009, p.11; Mr Mike Rothery, AGD, *Transcript of Evidence*, 25 November 2009, p.12.

## Committee View

4.16 The Committee considers that the level of awareness of cyber crime threats among Australian home users and small businesses is insufficient to ensure their safety online.

4.17 The Committee is of the view that the vulnerability of Australian home users and small businesses presents a risk to all sections of the Australian community. The insufficient uptake of simple e-security measures means that home users and small businesses will continue to be victimised by cyber criminals. This has direct financial and emotional impacts on the victims themselves, and exposes other sections of Australia's ICT systems to attack, including areas of government.

4.18 Community education and awareness raising is part of the Australian Government's *Cyber Security Strategy*. The adequacy of Australia's current initiatives is examined in Chapter 10.