3

Cybersafety risks and threats for seniors

Introduction

3.1 The digital economy is constantly growing and diversifying: Australians are going online for business and pleasure, for social networking, to access government information or advance their education, for shopping, investment or other financial transactions.

3.2 As discussed in the previous chapter, there are significant financial and quality of life benefits in this for every sector of the Australian community. However, just as government and businesses embrace the internet to improve their services, so the market expands to host new generations of cyber-enabled crimes.

3.3 This chapter surveys the nature and extent of cybercrime before discussing the particular risks to older Australians and their perceptions of, and responses to, these risks. Finally, the chapter considers some basic measures to build the online confidence and consumer awareness of all Australians, and particularly those aged 55 plus.

The nature and prevalence of cybercrime

3.4 The immediacy and global nature of interaction on the internet, and its convergence with new technologies such as smartphones and portable tablets, offers senior Australians a new means of access to family and friends, education and health services, and business. These benefits are

not achieved, however, without exposing participants to an ever diversifying range of online threats and risks. The Australian Crime Commission (ACC) advised:

> As the cyber-world becomes increasingly embedded in every aspect of our lives, the opportunity for cyber enabled criminal groups and entrepreneurial actors also increases. The internet in particular is being utilised by organised crime groups to commit traditional crimes such as fraud in a manner that removes many of the associated risks. Cyber-criminals can operate from a distance across a borderless cyber-environment with a degree of anonymity that has never been seen before and against a significant quantum of potential victims. [They] are interested in attaining illicit wealth, either through the theft of personal information or through fraudulent investment scams and similar activities.[1]

3.5 The Australian New Zealand Policy Advisory Agency has defined cybercrime to cover:

- crime directed at computing and communications technologies themselves, such as unauthorised access to, modification or impairment of electronic communications or data; and
- crime where the use of the internet or information technology is integral to the commission of the offence, (sometimes referred to as technology enabled crime) such as online fraud (including Internet or email scams), online identity theft, online child exploitation and online intellectual property infringement.[2]

3.6 The *2012 Norton Cybercrime Report* estimated the global financial cost of cybercrime over the previous year at $110 billion. Over 556 million victims were affected with nearly half of these subject to malware or virus attacks, hacking scams, fraud and/or information theft.[3]

3.7 The borderless and anonymous nature of online activity, along with the versatility of organised crime, poses significant challenges to regulators internationally.[4] Australia's accession to the *Council of Europe's Convention on Cybercrime*, and recent implementation of legislation in support of it, intends to address this by enhancing the capacity for

1 Mrs Karen Harfield, Executive Director, Fusion, Target Development and Performance, Australian Crime Commission (ACC), *Committee Hansard*, 15 August 2012, p. 1.

2 Quoted in ACC, *Submission 9*, p. 7.

3 Symantec, *2012 Norton Cybercrime Report*, 2013, pp. [2–3].

4 ACC, *Submission 9*, p. 9.

international information and data sharing and enforcement co-operation.[5]

3.8 The Australian Government has established a goal that Australia should be among the world's leading digital economies by 2020. Evidence to the Committee highlighted a number of emerging cyber threats that have potential to jeopardise the economic prosperity expected with this economic expansion.[6]

Emergent cyber threats

3.9 According to the ACC, international cybercrime is now occurring at an unprecedented rate.[7] While the cost estimates of this to the Australian community vary, these are clearly significant: the Australian Federal Police (AFP) estimates that Australians lose in excess of $1 billion a year to cyber criminals.[8] The internet security company Symantec calculated the figure over 2012 was closer to $2 billion.[9]

3.10 The latest statistics from the Australian Competition and Consumer Commission (ACCC), which registers complaints about online scams,[10] confirms the growth in online frauds. In 2011 the ACCC received 83 150 scam related contacts from consumers and small businesses, almost double the number received in 2010, and four times that recorded in 2009.[11]

3.11 Top scams reported to the ACCC over 2011 were mass marketed advance fee frauds, covering upfront payment for services, products or rewards, which accounted for half of all reports, and computer hacking which was the second most reported scam type, accounting for 23 per cent of scams. This compared with 12 per cent in 2011.[12]

5 See Chapter 5 for more detail.

6 Australian Government, # *au20, National Digital Economy Strategy: Leveraging the National Broadband Network to Drive Australia's Digital Productivity*, Department of Broadband, Communications and the Digital Economy (DBCDE), 2011, and see DBCDE, *Submission 25*, p. 2.

7 ACC, *Submission 9*, p. 7.

8 Quoted in DBCDE, *Submission 25*, p. 6.

9 Symantec, *2012 Norton Cybercrime Report*, 2013, p. [6].

10 Australian Competition and Consumer Commission (ACCC), SCAMwatch <www.scamwatch.gov.au/content/index.phtml/tag/scamAboutUs/> viewed 30 January 2013.

11 ACCC, *Targeting Scams: Report of the ACCC on Scam Activity 2011*, 2011, p. 1.

12 ACCC, *Targeting Scams: Report of the ACCC on Scam Activity 2011*, pp. 1, 7.

3.12 A major driver of online crime is the availability of personal information used for identity theft and system hacking. The Centre for Internet Safety (CIS), a cybercrime centre in Canberra, advised that credit card skimming and online data theft can now be taken as a given, with decreasing prices for personal information in Australia commensurate with its increased availability in a thriving black market.[13]

3.13 The ACC reported that some organised crime networks specialise in the sale of personal data. While rates vary, Australia often ranks as the third or fourth least expensive source country after the United States (US), the United Kingdom (UK), and Canada:

> Average prices for a single Australian credit card range between A$7 and A$35, depending on the amount of credit available on the card. Prices for bank logins vary according to the bank balance. It costs on average A$100 for a login with a balance of A$1 000; A$200 for a login with a balance of A$3 000 and so on. Credit card magnetic strip coding information and PINs are also available, with prices ranging between A$70 and A$170, depending on the location.[14]

3.14 Cybercriminals are entrepreneurial and opportunistic, continually monitoring the online environment for vulnerabilities to exploit for criminal gain.[15] The ACC's Mrs Karen Harfield referred to online fraud activity during the global financial crisis:

> For example, you will remember the $900 bonus as part of the response to the global financial crisis. We saw, within 48 hours, that people were being directly contacted for their names, dates of birth and account numbers so that the payment could be diverted away from the legitimate person who was to receive it.[16]

3.15 According to the CIS, the most successful online threats now combine social engineering, involving psychological manipulation to gain personal information, and technical attacks, to gain access to systems.

---

13 Mr Alastair McGibbon, Co-Director, Centre for Internet Safety (CIS), *Committee Hansard*, 14 March 2012, p. 2.

14 Prices fluctuate and vary for different countries at different times, see ACC, *Submission 9,* Case Study, p. 13.

15 ACC, *Submission 9,* p. 9.

16 *Committee Hansard*, 15 August 2012, p. 3.

Spam meanwhile continues to be an important vector for spreading malware (malicious software), 'phishing' and social engineering scams.[17]

3.16 Research conducted by the Symantec security firm over 2011 found that around 72 per cent of adult internet users in Australia had experienced cybercrime with viruses and malware, online credit card fraud and social networking profile hacking being most reported.[18]

3.17 The following sections describe the nature and impact of key threats to Australians as identified in evidence: identity theft, by 'phishing' and company-based data breaches or 'hacking'; superannuation and investment schemes; online dating schemes; money transfer and lottery and charity scams.

Identity theft by 'phishing'

3.18 Identity theft involves fraudulent use of personal details, such as drivers licences, tax file numbers and electronic personal identity information (computer passwords and personal identification numbers—PINs), without permission or to illegally appropriate another persons' identity for unauthorised gain.[19]

3.19 'Phishing' is the term used to describe approaches designed to capture personal information by email, often by including hotlinks to 'poisoned' web pages.[20] The email may purport to be from a victim's bank or another trusted source and will request account information to be verified through the linked site.[21]

3.20 The Australian Tax Office (ATO) submission provided examples of ATO branded 'phishing' exercises over some years showing their increasing sophistication. Appendix F shows a recent version.[22] The ATO's Mr Todd Heather explained the enforcement challenges posed by these scams:

> When we discovered that people were using our brand in this way we created something that we call the phishing filter, by which we would detect that a scammer was coming to our website to try to

17 CIS, *State of the Nation,* December 2011, pp. 1, 6.

18 Symantec, *Norton Cybercrime Report* 2011, Cited in ACC, *Submission 9*, p. 7.

19 CIS, *State of the Nation,* December 2011, p. 8; ACC, *Submission 9*, p. 13.

20 See CIS, *State of the Nation,* December 2011, p. 9.

21 C Budd and J Anderson 'Consumer Fraud in Australasia: Results of the Australasian Consumer Fraud Taskforce Online Australia Surveys 2008 and 2009', *Technical Background Paper 93*, AIC, March 2011, p. 21.

22 Australian Taxation Office (ATO), *Submission 43*, p. 4.

> re-present our information to them. We would send a message back saying, 'This is a scam website; it is being blocked.' They got wind of that, so instead of referring directly to our website, they point to a copy they have made of our website.[23]

3.21 Over 2010–11, the ATO recorded a 74 per cent increase on total IT security incidents, with 67 per cent being ATO branded phishing attacks.[24]

3.22 Phishing scams may also involve notification of a fake lottery win, bequest or inheritance scams or requests to act as an intermediary to transfer funds from an overseas country in return for a commission (advance fee scams).[25] The AFP reported a recent phishing scam using its logo to lure consumers into paying money to unlock their personal computers.[26]

3.23 Another trend is the prevalence of phishing scams posted on travel websites and mailing lists, with links to non-existent resorts and holiday packages used to gather booking fees and personal information.[27]

Computer hacking

3.24 In addition to data theft from an individual's online activities and home computer, a major source of financial and personal information is through hacking into the computer networks and databases of institutions or businesses. As noted above, online hacking was the second most reported scam reported to the ACCC in 2011.[28]

3.25 Malware can be installed on computers through phishing invitations and used to redirect users from a legitimate URL to a false website in a process known as 'pharming'.[29] Spyware is used to gather information

---

23 Mr Tod Heather, Chief Technology Officer, Strategy, Planning and Assurance, Enterprise Solutions and Technology, ATO, *Committee Hansard*, 18 May 2012, p. 25.

24 In 2012, the most prevalent ATO branded scam was a fax related scam, in which real estate agents were asked to forward a 'rental income without deduction form' to landlords to elicit information to be faxed back to a designated 'ATO' number, see ATO, *Submission 43,* p. 4–5.

25 Brotherhood of St Laurence, *Submission 13,* p. 5.

26 Commander Glen McEwen, Manager, Cyber Crime Operations, Australian Federal Police (AFP), *Committee Hansard*, 13 March 2013, p. 1

27 AVG Technologies in *Age Traveller* <www.theage.com.au/travel/dodgy-deals-are-daylight-robbery-20130201-2dop4.html#ixzz2KkF26zhj> viewed 13 February 2013.

28 ACCC, *Targeting Scams: Report of the ACCC on Scam Activity 2011*, p. 7.

29 C Budd and J Anderson 'Consumer Fraud in Australasia', *Technical Background Paper 93*, AIC, March 2011, p. 21.

by monitoring online use without otherwise disrupting a computer's function.[30]

3.26 The Committee was told that few Australian Small and Medium Enterprises (SMEs) have the capacity to manage the data they hold, and even large companies are not immune to sophisticated attacks using malware.[31] According to Abacus-Australian Mutual, the industry body for mutually owned Deposit-taking Institutions (ADIs),[32] the cost to business of cybercrime was reported to be up to $624 million in 2008 alone.[33]

3.27 In the wake of a number of significant and well publicised hacking incidents overseas involving multinationals[34] and most recently in Australia against institutions and SMEs,[35] the Government has issued warnings and introduced legislation to better protect personal information. This is discussed in more detail in Chapter 5.

Superannuation fraud and boiler room investment schemes

3.28 The AFP reports that superannuation fraud is the largest earner for cybercriminals in Australia. Various means are deployed to obtain access to superannuation funds. The AFP advised:

> Criminals exploit a range of techniques including phishing in order to first steal the identity of victims before transferring their superannuation into self-managed accounts or applying for hardship payments.[36]

3.29 Crime experts agreed that domestic and offshore investment schemes pose an escalating threat to Australians, and especially to senior

30 See CIS, *State of the Nation,* December 2011, p. 8.

31 Professor Nigel Phair, Co-Director, CIS, *Committee Hansard,* 14 March 2012, pp. 2–3 and for detail on malicious software see CIS, *State of the Nation,* December 2011, pp. 5–6.

32 Abacus-Australian Mutuals represents 89 credit unions, seven mutual building societies and six banks, with a total of $ 85 billion total assets and 4.5m customers. See *Submission 44*, p. 1.

33 K Richards, 'The Australian Business Assessment of Computer User Security (ABACUS): a National Survey', *AIC Research and Public Policy Series no. 102*, June 2009, Forward. Data ref. in Abacus-Australian Mutuals, *Submission 44*, p. 1.

34 The largest recorded data breach occurred in April 2011 when 77 million Sony PlayStation accounts were hacked. See CIS, *State of the Nation,* December 2011, pp. 8–9.

35 Notably, a school and medical practices in Queensland had data stolen, encrypted and held for ransom. See DBCDE, 'Ransomware Attacks Will Increase in 2013', 21 December 2012, <www.staysmartonline.gov.au/alert_service/advisories/ransomware_attacks_will_increase_in_2013 > viewed 31 January 2013.

36 Australian Federal Police (AFP), *Submission 20*, p. 3.

Australians who are targeted because of their superannuation wealth.[37] Also known as boiler-room fraud or 'serious and organised investment fraud' (SOIF), these schemes use sophisticated techniques to solicit investment in non-existent or essentially worthless shares and other securities.[38]

3.30 The CIS stated that, typically, boiler room investment schemes are 'well backstopped', utilising a range of media to ensnare their victims.[39] The ACC advised that victims are first identified by stored online information obtained through the personal information leads market. Operators start with a cold call or emails and high pressure sales techniques to secure investment, sometimes grooming their victims over a long period. Victims are then directed to professional-looking websites which may be operated from anywhere in the world.[40]

3.31 Victims are usually encouraged to make a small upfront investment, with websites presenting investment growth over the long term to persuade people to invest more. Detection of loss may result in a subsequent scam for investigation at a fee, or sites simply close down and the 'investment' disappears.[41]

3.32 Explaining the success of these schemes, the ACC's Mrs Harfield said that the perpetrators of these crimes psychologically profile their victims, and the back up with phone calls, letters and faxes tends to legitimate the scheme.[42] The CIS's Professor Phair explained that SOIF websites also appear as part of a complex series of interrelated sites, which convinces even professional investment advisers.[43]

Online dating and romance scams

3.33 According to the ACCC, dating and romance scams are a major threat to Australian consumers; more money is lost through these scams by proportion than in all other scams.[44] Over 2011 dating and romance

37 AFP, *Submission 20*, p. 3; ACC, *Submission 9*, p. 17.

38 ACC, *Submission 9*, p. 17.

39 Professor Phair, CIS, *Committee Hansard*, 14 March 2012, p. 6.

40 ACC, *Submission 9*, p. 18.

41 Mrs Harfield, ACC, *Committee Hansard*, 15 August 2012, p. 2.

42 ACC, *Committee Hansard*, 15 August 2012, p. 2.

43 CIS, *Committee Hansard*, 14 March 2012, p. 6.

44 One in two people who reported a dating and romance scam lost money compared to around one in five across all types of scams. See 'ACCC Working with Industry to Target Dating and Romance Scams', *Media Release*, 29 September, 2011.

scams cost Australians more than $21 million.[45] Almost five per cent of consumers affected by this type of scam lost in excess of $100 000.[46]

3.34 Romance and dating scams are a category of advance fee scam where a payment is made in anticipation of a reward. Dating and romance scammers use social engineering techniques to promote emotional involvement and a sense of obligation. Criminals may use bogus profiles on social networking sites to befriend victims in order to get them to send money in the promise of love or relationship.[47]

3.35 The AFP notes that many victims are approached on legitimate dating websites, now a major growth industry with wide community engagement:

> These scams typically involve a genuine user of an online dating site being contacted by a potential admirer who is a scammer in disguise. After forming a relationship with the victim, the scammer plays on emotional triggers to get the victim to provide money, gifts or personal details.[48]

3.36 The ACCC's consumer guide *The Little Black Book of Scam*s warns that romance and dating scammers are usually extremely experienced at emotional manipulation:

> Even on a legitimate dating site, you might be approached by a scammer—perhaps someone who claims to have a very sick family member or who is in the depths of despair (often these scammers claim to be from Russia or Eastern Europe). After they have sent you a few messages, and maybe even a glamorous photo, you will be asked (directly or more subtly) to send them money to help their situation. Some scammers even arrange to meet with you, in the hope that you give them presents or money—and then they disappear.[49]

45 ACCC, 'Safer Dating Online' <www.accc.gov.au/content/index.phtml/itemId/1047887> viewed 31 January 2013.

46 ACCC, *Targeting Scams: Report of the ACCC on Scam Activity 2011*, p. 12.

47 Abacus-Australian Mutuals, *Submission 44*, p. 2.

48 AFP, *Submission 20,* p. 4, also see 'ACCC Working with Industry to Target Dating and Romance Scams', *Media Release*, 29 September, 2011.

49 ACCC, *The Little Black Book of Scam*s: *Your Guide to Scams, Swindles, Rorts and Rip-Offs,* 2008 (rev. 2011), p. 27.

Money transfer, lottery and charity scams

3.37 Money transfer, or advance fee, scams usually involves receipt of an unsolicited email promising an unexpected and significant cash payment, pending the payment of substantial 'administrative' fees by the victim to an overseas bank account.[50]

3.38 Originally issued from Nigeria, these scams are now generated in many other nations. According to the ACC many victims, on realising losses, continue to send funds hoping for a 'successful' completion. The perpetrators profit from only a small number of victims but the use of email means pervasive impact for a minimal cost.[51] Advance fee scams also include those in which the offender pretends to sell something that does not exist while taking money in advance, or provides a product of a lower standard than that which was offered for sale.[52]

3.39 Lotteries and charity scams rely on users' familiarly with legitimate lottery and prize sites.[53] The ABS, in its first fraud survey report released in 2008, found that fake lotteries accounted for the largest number of victims (84 100) over the previous year.[54] The ACCC advises that scammers may ask for fees upfront or call premium rate numbers to claim a prize, noting:

> These premium rate calls can be very expensive, and the scammers will try to keep you on the line for a long time or ask you to call a different premium rate number.[55]

3.40 Charity scams use online social engineering to play on human sympathies by masquerading as charities or disaster relief campaigns.[56] The CIS noted that social networking sites are a common vehicle for such scams. For example, during the Japanese earthquake, tsunami and nuclear incidents were exploited by poisoned hotlinks, social networking scams and malicious spam campaigns.[57]

---

50 Abacus-Australian Mutuals, *Submission 44*, p. 2, and ACC, *Submission 9*, p. 12.

51 ACC, *Submission 9,* p. 12.

52 Australian Human Rights Commission (AHRC), *Submission 2*, p. 6.

53 ACCC, *The Little Black Book of Scams,* 2008 (rev. 2011), p. 7.

54 ABS, *4528.0 Personal Fraud 2007*, 2008, p. 6.

55 ACCC, *The Little Black Book of Scams,* 2008 (rev. 2011), p. 7.

56 AFP, *Submission 20*, p. 4.

57 See CIS, *State of the Nation,* December 2011, p. 6.

Are seniors more at risk?

3.41 Anyone can be a victim of cybercrime but, the Committee was advised, Australia's seniors, as a relatively wealthy and recently growing demographic online, are an attractive target for innovative cybercriminals both domestic and international.[58]

3.42 Available research also suggests Australian seniors are being disproportionately targeted by, and fall victim to, certain types of online criminal activity dependent on age. The trends also reflect the uptake of online activities by older groups:

- 2008–09 research for the Australian Consumer Task Force (ACTF), found seniors aged 55–65 were most vulnerable to advance fee scams, such as Nigerian scams and 'phishing' scams, while those aged 55 to 64 years and 65 up were more likely to respond to lottery scams.[59]
- 2011 surveys by the Australian Institute of Criminology (AIC) showed seniors aged 65 plus as most vulnerable to advance fee fraud, with mid-life individuals aged 45 to 54 years most susceptible to dating scams.[60] The ASIC and ACC reported the growing victimisation of older people, 55 plus, by using cold calling to encourage investment in fake boiler room (SOIF) schemes.[61]

3.43 A range of specific factors, alone or in combination, were identified as heightening online vulnerability to these types of cybercrime which target the financial, psychological and social circumstances of senior Australians:

- financial situation—well-funded retirees wanting to invest or those with limited wealth seeking funds;
- reluctant users— required to go online to access health information, other government information or services;
- unfamiliarity with internet conventions—such as email management, formatting hierarchies and commercial drivers; and

58 AFP, *Submission 20*, p. 2; CIS, *Submission 26*, p. [3].

59 C Budd and J Anderson, 'Consumer Fraud in Australasia', *AIC Reports Technical and Background Paper 43,* p. 14.

60 C Ross and R Smith, 'Risk Factors for Advance Fee Fraud Victimisation', *Trends and Issues in Crime and Criminal Justice no. 420*', AIC, 2011 cited in AHRC, *Submission* 2, p. 6.

61 Australian Securities and Investments Commission (ASIC) *Submission 46*, p. 5 , ACC, *Submission 9,* p. 17.

- increased social networking and technology take up, given social trends and the take up of new technologies including android phones, and the rollout of the NBN.

Wealthy or seeking wealth

3.44 Mr Michael O'Neill, CEO, of National Seniors Australia Ltd (NSA) informed the Committee that Australia's seniors are increasingly 'targets for nefarious activities', being relatively cashed up at retirement and lacking sophistication with internet and interface technologies. It is this combination which heightens their vulnerability to unscrupulous online scammers.[62]

3.45 The AFP advised that superannuation fraud and boiler room investment schemes are major online threats to midlife and senior Australians.[63] The deposit taking industry peak body Abacus-Australian Mutuals reported:

> Seniors have become vulnerable to investment scams particularly since the Global Financial Crisis. The need to supplement reduced incomes, or repair investment portfolios, has made seniors targets for criminals here and overseas…The victims of these scams are usually already in distressed financial circumstances.[64]

3.46 The primary victim profile for SOIF schemes are people over 50 years with a university education or high school diploma and good financial knowledge.[65] The multi-agency Task Force Galilee, in operation since 2011, reports Australian losses to SOIF scams at $113 million, with investments ranging from $500 to just over $ 1 million. The oldest victim, who was 91 years old, lost everything.[66]

3.47 While the victims of sophisticated SOIF investment schemes tend to be well educated, financially literate and internet savvy,[67] less cyber savvy seniors are susceptible to 'phishing' scams via phone or email.[68]

3.48 The Brotherhood of St Laurence advised that phishing scams trade on older people's confidence in established institutions and can have a deleterious impact on a person's reputation if their identity is used to

62 *Committee Hansard*, 31 October 2013, p. 1

63 AFP, *Submission 20*, p. 3.

64 Abacus -Australian Mutuals, *Submission 44*, p. 2.

65 Mrs Harfield, ACC, *Committee Hansard*, 15 August 2012, p. 1.

66 Mrs Harfield, ACC, *Committee Hansard*, 15 August 2012, p. 7.

67 ACC, *Submission 9*, p. 16.

68 AHRC, *Submission 2*, p. 7, Australian Taxation Office (ATO), *Submission 43*, p. 1.

commit fraudulent or illegal acts.[69] The ATO confirmed that retirees are particularly susceptible to ATO 'branded' phishing scams, especially those using phone call centres.[70]

3.49 Research conducted by ACTF has established that people in the 55–64 and 65 plus year age groups are statistically more likely to respond to lottery scams than other age groups.[71]

3.50 Online lottery scams are particularly attractive to seniors whose incomes are finite and are hence more likely to take a 'flutter' on gambling or lottery sites to gain a fund injection. US studies indicate that people with negative life experiences, such as medical problems and financial difficulties, are most vulnerable to advance fee scams.[72]

3.51 The AIC advised that seniors affected by these scams have limited potential to recover from the loss of their retirement incomes.[73]

Reluctant and online

3.52 Research from Edith Cowan University in WA suggests that, in contrast to other age groups who have quickly embraced online activity, many seniors now participate in online interaction because they must.[74] Brisbane Seniors Online Association confirmed:

> It is becoming increasingly difficult to obtain information without seeing the phrase "for more information go to www…" Organisations at all levels, be they governments, local councils, utilities or business of all types and sizes are gradually 'forcing' their clients to use the internet as a means of doing business by making all other mechanisms too difficult or too expensive. This particularly affects seniors who cannot easily adapt to the new technologies and are fearful of the possible consequences.[75]

---

69 Brotherhood of St Laurence, *Submission 13*, p. 5.

70 ATO, *Submission 43*, p. 5.

71 C Budd and J Anderson, 'Consumer Fraud in Australasia', *AIC Reports Technical and Background Paper 43,* p. 14.

72 AHRC, *Submission 2*, p. 7.

73 A 2011 study of advance fee fraud victims found that of 59 per cent of respondents had sent an average of $12 000 each overseas, and 43 per cent of them reported emotional trauma, 40 per cent loss of confidence and 12 per cent marital or relationship problems due to the victimisation. See AIC, *Submission 12*, p. 3.

74 D M Cook, P Szewczyk and K Sansurooah, 'Securing the Elderly', Edith Cowan University WA, presented at the Second International Cyber Resilience Conference, p. 21; cited in Western Australian (WA) Government, *Submission 19*, p. 1.

75 Brisbane Seniors Online Association Inc. (BSOL), *Submission 34,* p. 1.

3.53 NSA suggested that the 'lack of interest' reported in many surveys of seniors attitudes to the internet may be feigned to avoid stigma and mask confusion and fearfulness about the technology.[76]

3.54 Over 2011 the Department of Broadband, Communication and the Digital Economy (DBCDE) conducted segmentation research to better target cybersafety awareness programs for Australian internet users. Seniors comprised 22 per cent of the 'fearful avoiders' group, who were most likely to report that they did not know enough to protect their privacy or personal information online.[77]

3.55 According to the AIC, fearfulness of the internet can increase vulnerability to technology based crime, online or off.[78] Worries about online security may prompt unwary seniors to subscribe to fake IT security products which introduce viruses onto their computer to collect financial information. Offline scams such as the Do Not Call Register Hoax target seniors frustrated by cold calling, and solicit mobile numbers or other information for use in cybercrime.[79]

3.56 The ubiquitousness of the 'Microsoft Scam', where victims are told their computer has a virus which can be rectified by giving external access to hacker, was widely cited to indicate the vulnerability of seniors to multimedia scams.[80]

3.57 Older users may be forced onto the internet because of poor health or lack of mobility. They may be isolated or reluctant to seek help, not wanting to burden their friends or family, or fearful of breaking the computer.[81] Those on a limited income may be reluctant to invest in computer upgrades and security systems necessary to keep safe. As discussed later in this chapter, cost was raised as a barrier to internet use by seniors in submissions.

---

76 NSA, *Submission 29*, p. 15.

77 The surveys identified four online behavioural segments: 'comfortable but weary', 'watchful transactors'; 'confident and (tech) savvy'; and 'fearful avoiders'. DBCDE, *Submission 25*, p. 7.

78 Dr Rick Brown, Deputy Director (Research), AIC, *Committee Hansard*, 10 October 2012, p. 1.

79 WA ScamNet advice to WA Government, *Submission 19*, p. 3; Stay In Touch Pty Ltd, *Submission 47,* p. 3; Dr Cassandra Cross, *Submission 49*, p. 5.

80 Moorook 8 Neighbourhood Watch, *Submission 14*; WA ScamNet advice to WA Government, *Submission 19*, p. 3; Stay In Touch Pty Ltd, *Submission 47,* p. 3, and Mr MacGibbon, CIS, *Committee Hansard*, 14 March 2012, p. 5.

81 Australian Research Council Centre of Excellence for Creative Industries and Innovation (CCI), *Older Australians and the Internet*, 2011, cited in ACMA, *Submission 24*, pp. 7–8.

Unfamiliarity with cyber 'conventions'

3.58 While older people can be more cautious about online risks than younger users, the Committee was told that the ease of 'surfing the net' at home tends to induce a false sense that online interaction is secure, private and confidential:

> Unfortunately when people get home they are in a relaxed environment—they have a mug of Milo with them, perhaps the fluffy slippers on—feeling pretty relaxed and all of a sudden they divulge all this information which, I would contend, they normally would not in a social real-world setting.[82]

3.59 The Alannah and Madeleine Foundation noted that a senior's usually 'acute judgement of character' can be disabled without visual cues.[83] Deprived of these cues, and the normal caution exercised during face to face business or personal interaction, seniors can fall prey to online manipulation.[84] The Consumer Health Forum Australia (CHF) advised that an older person's trust in published material may also make them less sceptical about information on the internet purporting to be factual, such as health information.[85]

3.60 Increased opportunities for online interactions for business and shopping have also opened up new risks for trusting seniors. A West Australian (WA) Government survey found that older users are often unaware of the commercial underpinnings of much online interaction. Lengthy terms and conditions statements in the last stages of online transactions may be ignored and the informality of real estate sites may encourage ill-considered rental and retirement decisions.[86]

3.61 DBCDE advised that seniors may be disconcerted by the 'organic' nature of internet search engines.[87] They may not realise that the top of web search lists are often advertisements,[88] that product reviews can be fabricated, or that 'pop up' offers on websites may not be verified by web managers, and can be vehicles for fraud or identity theft.[89]

82 Professor Phair, CIS, *Committee Hansard*, 14 March 2012, p. 3.

83 The Alannah and Madeleine Foundation, *Submission 35*, p. 6.

84 AFP, *Submission 20*, p. 2; Professor Phair, CIS, *Committee Hansard*, 14 March 2012, p. 3.

85 Ms Carol Bennet, CEO, Consumer Health Forum of Australia (CHF), *Committee Hansard*, 19 September 2012, p. 1.

86 WA Government, *Submission 19*, p. 2.

87 Mr Abdul Rizvi, Deputy Secretary, Digital Economy and Services Group, DBCDE, *Committee Hansard*, 12 September 2012, p. 2.

88 WA Government, *Submission 19*, pp. 2–3.

89 ACC, *Submission 9,* p. 13.

3.62 Seniors can also lack a general awareness of the protocols of emailing, such as the risks of forwarding emails and chain mail.[90] Stay in Touch, a seniors' computer training provider, noted that they:

> …[are] often unaware that unwanted emails can appear to be alright when it comes from family or friends when in fact a virus has gotten onto that person's computer and automatically sends an email out to everyone in those peoples' address books.[91]

3.63 The Australian Seniors Computer Clubs Association (ASCCA) advised that older people may consider they are protecting themselves by clicking on phishing emails to 'unsubscribe' before deleting.[92]

3.64 The Federation of Ethnic Communities' Councils of Australia (FECCA) alerted the Committee to the vulnerabilities of Culturally and Linguistically Diverse (CALD) seniors to the growing threat of cyber racism and bullying.[93] The African Seniors Club advised that African seniors in Australia, many without formal education, are inclined to accept everything on the internet as factual and to tolerate abuse by scammers without complaint.[94]

3.65 The Alannah and Madeline Foundation referred to similar risks for Aboriginal and Torres Strait Islander Elders.[95] The Committee notes the ACCC's recent alerts on Nigerian charity scams targeting remote Indigenous communities in South Australia.[96]

Increased social networking

3.66 Social networking is becoming an increasingly important tool for communicating with friends and family, with over 10 million Australians having active accounts on the Facebook social networking site.[97]

3.67 As the population becomes more mobile and families are dispersed, keeping in contact with family and friends through email, cheap internet

---

90 WA Government, *Submission 19*, p. 3; Mrs Nancy Bosler, President, ASCCA, *Committee Hansard,* 23 March 2012, p. 21.

91 Stay in Touch Pty Ltd, *Submission 47*, p. 4.

92 ASCCA, *Submission 7,* p. 6.

93 The Federation of Ethnic Communities' Councils of Australia (FECCA), *Submission 40*, pp. 2–3; 5.

94 African Seniors Club—Australia Inc., *Submission 18,* pp. 1–2.

95 Alannah and Madeline Foundation, *Submission 39*, p. 13.

96 SCAMwatch, ACCC 'Beware of Distress Emails Targeting the APY lands', Media Notice, January 2012: <www.scamwatch.gov.au/content/index.phtml/itemId/914432>

97 Facebook, *Submission 36,* p. 2.

phone calls, skyping and social networking sites is increasingly important for seniors. It also offers utility for those who live in outlying regions or who are unable to drive.[98]

3.68 Mrs Diana Edwards, Manager of the Italian Australian Pensioners Welfare Association of Tasmania Inc. Day Centre, told the Committee of the importance of Skype to migrant Australians:

> Cyberspace as I know it is really a good tool because it opens up, especially for ethnic or cosmopolitan people, a world out there that they can actually bring into their house—to pay bills, to socialise. If I could not see my two grandchildren on Skype I would be most upset, because my son lives in Brisbane.[99]

3.69 However, the Committee also heard that older people communicating with relatives or friends on social networking sites maybe easily targeted for identity or information theft.

3.70 While Facebook offers users privacy controls and provides advice for people over 50 to keep safe online,[100] Dr Cassandra Cross's research suggested that few seniors have adequate knowledge of security settings on their accounts and believe that only their contacts can access the information.[101] The AIC advised that offline crimes such as burglary are supported by information, about holiday plans for example, shared on these sites. Other household members or relatives can also use shared information on computers to perpetrate financial abuses.[102]

3.71 Victims of romance and dating scams are often first identified through personal information on social networking or dating sites. While these sites are not as well patronised by seniors compared to younger age groups, many seniors are lonely, isolated and vulnerable to approaches for love or friendship.[103]

---

98 NSA Productive Ageing Centre, *Older Australians and the Internet*, September 2011, p. 8, attachment to NSA, *Submission 29* and see Facebook, *Submission 36,* p. 2.

99 Mrs Diana Edwards, Manager of the Italian Australian Pensioners Welfare Association of Tasmania Inc. Day Centre, *Committee Hansard*, 7 August 2012, p. 2.

100 Facebook, *Submission 36,* pp. 2–3.

101 Dr Cassandra Cross, Lecturer, School of Justice, Faculty of Law, Queensland University of Technology, *Committee Hansard,* 6 February 2013, p. 9.

102 AIC, *Submission 12,* p. 2. See also Office of the Public Advocate advice to Government of WA, *Submission 19*, p. 3.

103 ACCC, *Targeting Scams: Report of the ACCC on Scam Activity 2011*, p. 12.

3.72 Dr Cross advised that the insidious nature of dating romance frauds is not easily counteracted by education, and compounds financial damage with a sense of perceived personal loss.[104]

The NBN and technology take-up

3.73 While senior citizens are showing an increased interest in going online, there is still a 'digital divide' in the Australian community, with low rates of connection among those over 65 years, across rural populations, and among lower income groups.[105]

3.74 The rollout of the National Broadband Network (NBN) into regional areas is expected to compound risks associated with low skill or confidence levels, as less cyber savvy regional seniors seek to capitalise on opportunities newly accessible on the web or are required to do so to access services long distance such as banking, telehealth, applying for licences and so on.[106]

3.75 The Committee's cybersafety survey provides an indication of this potential, with the second most reported problem, malicious software installation, affecting 42.9 per cent of seniors in a rural setting and 31.3 per cent in regional areas, compared with 29.4 per cent in urban areas.[107] The ASCCA advised that many seniors unfamiliar with new technologies don't know how to obtain security software, how to install it or that it must be updated regularly.[108]

3.76 At the same time, seniors' organisations recorded a burgeoning interest in smartphones and portable tablets which are a more intuitive technology for seniors.[109] Data from Telstra confirms seniors' interest in the use of new technologies such as the smartphone.[110] However, the CIS advised that cybercriminals are increasingly adept at infecting smartphones with malware that send out SMS messages, while cross

104 Dr Cassandra Cross, *Submission 49*, p. 26.

105 The Alannah and Madeline Foundation, *Submission 35*, p. 5.

106 AFP, *Submission 20*, pp. 2–3.

107 See Appendix D.

108 ASCCA, *Submission 7*, p. 6.

109 A survey conducted of Y*OURLifeChoices* magazine's subscribers over 2011 found ownership of EBook readers and Smartphones had more than doubled compared with 2010 and nearly a quarter of subscribers said that they would purchase an iPad during the next year, while slightly less than a fifth, would invest in a smartphone or e-reader. Y*OURLifeChoices, Submission 38*, p. 4.

110 According to a June 2011 report, 46 per cent of Australian mobile phones are smart phone, with 23 per cent owned by users aged over 50. See *Telstra Smartphone Index – June 2011*, cited in DBCDE, *Submission 25*, p. 6.

platform Trojans are designed to enable a range of spamming and other criminal activities.[111]

3.77 Access under the NBN and use of smartphones also brings into focus seniors' concerns about information security under eHealth initiatives.[112] A CIS study observed that eHealth is already using mobile devices (mHealth) to collect vital data and as such will be open to traditional network vulnerabilities.[113]

Seniors' responses to risk

3.78 Reluctant seniors adopt two main ploys to reduce their risk to cybercrime: avoidance; or selective use. Submissions from seniors' organisations reported that privacy and security are major concerns for older Australians, with fears about these the main reason for avoidance of the internet.[114]

3.79 Recent research cited by the Western Australian (WA) Government suggested that up to 40 per cent of senior Australians avoided internet use, considering themselves to be without the necessary skills, knowledge or interest given concerns about security and/or online viruses.[115] Telstra noted that a lack of online skill fosters such fears, and that all internet users are vulnerable if they lack adequate skills.[116]

3.80 According to Dr Cross's research, seniors adopting selective use typically avoid online banking or other financial transactions such as online shopping, even while continuing with research or social networking activities.[117] Online fraud victims usually withdrew from using the internet, and through shame or embarrassment kept their experiences to themselves, contributing to their stress and sense of isolation.[118]

---

111 CIS, *State of the Nation,* December 2011, pp. 11–12.

112 *YOURLifeChoices*, *Submission 38*, p. 4.

113 CIS, *State of the Nation,* December 2011, pp. 11–12.

114 Australian Seniors Computers Clubs Association, *Submission 7*, p. 7; Hobart Older Persons Reference Group, *Submission 8*, p. 1; Stay In Touch Pty Ltd, *Submission 47,* p. 6.

115 ABC Science survey, 8 August 2011, quoted in *Submission 19*, p. 1.

116 Telstra Corporation Ltd, *Submission 22*, p. 5.

117 Data varies to sample: the Committee's online survey (appendix D) found that 76 per cent of respondents use the internet for banking, more than for any other activity online. See also Legacy Australia for data on 75 plus group, *Submission 10*, p. 2, and BSOL, *Submission 34*, p. 1.

118 Dr Cassandra Cross, *Submission 49,* p. 5.

3.81 The Australian Human Rights Commission (AHRC) held that any failure to support older Australians to engage confidently, safely and competently online would demonstrate a threat to their human rights as economies shift to online services.[119] Referring to the 'digital divide' for seniors above 65, more than half of whom do not access the internet, the Australian Age Commissioner the Hon. Susan Ryan AO stated:

> What that means is that those people are missing out on all of the benefits that the rest of the community is enjoying—services like shopping online, banking online, but more and more the access to essential information, including the information that the government provides to Australians on their websites. Often now you find that the information is exclusively available or the service is exclusively available on the net. So it really becomes an equity issue. If older Australians cannot get access then they are missing out on the benefits that the rest of us can enjoy.[120]

3.82 The WA Government submission reiterated this position noting that seniors will be denied the benefits of the 'digital democracy', and that the digital divide may consolidate as technology use becomes even more prevalent across the general population.[121]

Building seniors' confidence and safety online

3.83 The Australian Government and its law enforcement and consumer protection agencies are currently monitoring the prevalence and evolving nature of cybercrime threats to Australians.[122] A cybersafety focus in policy in recent years has been on the internet safety of younger people, with children and teens being increasingly exposed to online bullying and stalking. This was the subject of the Committee's interim report, *High Wire Act: Cyber–Safety and the Young*, tabled in Parliament in June 2011.

3.84 Evidence covered in this chapter suggests that senior Australians are, in some incidences, disproportionally affected by a range of consumer

119 These rights are preserved under Article 19 of *The Universal Declaration of Human Rights 1948* which states that everyone has the right to 'seek, receive and impart information and ideas through any media regardless of frontiers'. See *Submission 2*, p. 3.

120 *Committee Hansard*, 23 March 2012, p. 1.

121 Government of WA, *Submission 19*, p. 4.

122 See Chapter 5 for an overview of Government consumer protection and enforcement measures.

fraud activities to which the broader community is also exposed and could benefit from additional assistance and advice.

3.85 The Committee does not, however, endorse the position that senior Australians are by definition lacking any necessary capacity to keep safe online. While there is evidence of a 'digital divide' for those above 65 years, there was also an enormous range of IT skills across senior cohorts, and evidence that the proportion of cyber savvy seniors is growing, even as the population ages.

3.86 Mrs Joyce Hocking (formerly Sheasby) from Toowoomba was one of those highly skilled seniors who, at 83 years, teaches other older people computer skills. She summed up the value of training to empower the less cyber savvy senior:

> They remind me of hares in the headlights of a ute when they come in, but, by the time they get to the fifth session, they are confident. It has always surprised me that you can change a person's total outlook by a little bit of knowledge.[123]

3.87 In Chapter 4, the Committee covers a broad range of initiatives advanced by the Government and the private sector to improve seniors' cybersafety awareness.

3.88 While training and improved user competence were universally agreed as fundamental to enhancing cybersafety among all age groups, there was also a view that government and industry could do more to protect consumers from growing cyber threats.[124] These issues are discussed in more detail in Chapters 5, on government's consumer protection framework, and 6, on the role of industry.

3.89 At a more fundamental level, a number of basic measures were proposed to Government to improve seniors' confidence and capacity to negotiate the web safely. These were to:

- Keep it simple: key safety messages must be headlined
- Keep it clear: intuitive web design and format
- Keep it safe: access to security software and advice
- Keep it easy: a single portal for reporting and advice.

123 Mrs Joyce Hocking (formerly Sheasby), *Committee Hansard*, 31 October 2012, p. 6.

124 Mr MacGibbon, CIS, *Committee Hansard*, 14 March 2012, p. 1.

Keep it simple: key messages for keeping safe

3.90 Given the range of risks to the consumer and the dynamic nature of the evolving cybercrime scene, regulators have recognised that, even with appropriate frameworks in place, online safety rests very much on the acuity of individual internet users.[125] The AFP advised:

> …there must be a degree of online responsibility commensurate with care taken in the real world. It is critical that all internet users exercise a prudent degree of caution in their cyber transactions, be they social, financial or commercial.[126]

3.91 The DBCDE, which is in charge of producing information for cyber awareness, has expressed confidence that older people are receptive to cybersafety messages, referring to recent consumer confidence research on computer security management and online shopping.[127] Given this receptivity, there was strong support for a new approach to cybersafety awareness: less about the types of risks and more on the real life consequences of certain behaviours.[128]

3.92 Dr Cross, having conducted extensive research in this area in the UK, Canada and the US, considered the Australian approach focusses too much on the 'white noise' around fraud, that is 'the journey and not on the destination':

> …We focus on the different ways in which a person can be defrauded…It does not matter how a person is approached for money or why they are approached, we need to focus our prevention message on that transfer of money.[129]

3.93 The fundamental message: 'Do Not Send Money', coupled with the advice that 'if it is too good to be true, it probably is', was reiterated by the AFP, which noted the criticality of promoting these messages as the NBN expands opportunities for computer offences against less technically experienced users.[130]

---

125 See also DBCDE, *Submission 25*, p. 8.

126 AFP, *Submission 20*, pp. 1, 3.

127 Mr Rizvi, DBCDE, *Committee Hansard*, 12 September 2012 p. 4 and see Ipsos survey conducted for 2012 National Cyber Security Awareness Week (held 12 to 15 June 2012) which recorded older people's receptiveness to online security advice and relative online caution compared with younger age groups, in DBCDE, *Supplementary submission 25.1,* p. 1.

128 Life Activities Clubs Victoria, *Submission 5,* p. 7; CIS, *Submission 26*, p. 2; AFP, *Submission 20*, p. 2.

129 *Committee Hansard*, 6 February 2013, p. 9.

130 AFP, *Submission 20*, p. 2.

3.94 The CIS specifically referred to the need to apply 'real world sensibilities' to requests for money when using dating sites, given the efficiency of modern methods of money transfer:

> ….Certainly do not send the money by Western Union where, once it is in the system, you cannot get it out and it is highly efficient at delivering it to the country that you are sending the money to.[131]

3.95 How these messages might better inform government awareness campaigns is discussed in more detail in Chapter 5.

Keep it clear: user friendly web design and interfaces

3.96 Another fundamental recommendation to assist seniors use the internet safely was to ensure that web design and content is presented in a clear and user friendly format.

3.97 A review of online security information conducted in 2011 found that government sites, such as the Cybersmart and Stay Smart Online sites, did not meet the needs of seniors and were deficient in terms of content and design. The researchers recommended use of simple language, ease of navigation, and graphical step-by-step tutorials to be more effective.[132]

3.98 Ms Fabienne Balsamo, Senior Policy Officer, AHRC, contrasted the Broadband for Seniors website in Australia with Britain's online access point for seniors:

> …the Age UK website is…incredibly user-friendly. When you go to that website all you need to do is put your postcode in on a big front page and it tells you what services are available in your region and what supports are available. The Broadband for Seniors website has much more embedded information and is much harder to navigate. It took me a while to find where my local services were. I think they have got some really good usability stuff happening in the UK.[133]

3.99 The NSA considered that government and company fora should promote awareness of the issue in a joint campaign to make accessible websites 'normal business'. Its submission referred to developments by the

131 Mr MacGibbon, CIS, *Committee Hansard*, 14 March 2012, p. 3.

132 D M Cook, P Szewczyk and K Sansurooah, 'Securing the Elderly', Edith Cowan University WA, presented at the Second International Cyber Resilience Conference, 2011, p. 21; cited in Government of WA, *Submission 19*, p. 1.

133 *Committee Hansard*, 23 March 2012, p. 2.

National Institute on Ageing and the National Library of Medicine websites as good examples.[134]

3.100 The ASCCA reiterated the demand for user friendly websites and accessible learning opportunities if the trend to internet dissemination of government information is to be viable.[135] In particular, for eHealth:

> Designers must make sure that the e-health tools are designed so that they can be used with an absolute minimum of technical knowledge! Even a highly technically skilled person may not be able to use complicated equipment when in a state of wellness or trauma.[136]

3.101 The Committee has noted that the Government introduced 'Web Content Accessibility Guidelines' for government internet sites in 2010 to ensure people with a disability are not disadvantaged online.[137] The guidelines contain mandatory requirements for accessibility including design, navigation, content and quality of presentation and searching results.[138]

3.102 On inspection, it appeared to the Committee that the *Web Guide* is complex and technical, being broken down into many topics addressing legal requirements and obligations.[139] The Committee could see utility in the development of a supplementary web style guide to promote the user friendly design of government information portals.

Recommendation 4

That the Australian Government develops, as a supplement to its *Web Guide*, a web style guide prescribing the key elements of web design to ensure simplicity of language, visual clarity in design and logical navigation tools. This could be supported by graphical step-by-step tutorials for use where applicable.

---

134 NSA, *Submission 29*, p. 29.

135 Recommendation 4, ASCCA, *Submission 7*, p. 5.

136 Recommendation 5, ASCCA, *Submission 7*, p. 6.

137 The Hon. Lindsay Tanner MP (former) Minister for Finance and Deregulation and (former) Parliamentary Secretary for Disabilities and Children's Services, the Hon. Bill Shorten MP, 'Dealing with Government Online to Become Easier for Australians with Disabilities', Joint *Media Release 05/2010*, 23 February 2010.

138 Australian Government, *Web Guide: Usability Requirements* <webguide.gov.au/accessibility-usability/usability-testing/> viewed 11 February 2013.

139 *Web Guide* <webguide.gov.au/> viewed 23 February 2013.

3.103 Departments and agencies are required to report their compliance with the current guidelines to the Australian Government Information Management Office (AGIMO).[140]

Recommendation 5

In support of the previous recommendation, the Committee also recommends that, in addition to conducting compliance audits based on the web style guide requirements, the Australian Government Information Management Office should offer an Annual Award for user friendly web design, in part based on public input on the utility of government websites.

Make it safe: access to computers and security advice

3.104 The 2011 report *Older Australians and the Internet* found that high costs and uncertainty about computer products and security requirements are barriers to seniors who otherwise were interested in using the internet.[141]

3.105 The State Library of WA observed that, despite decreasing computer costs and associated communication charges, many seniors are still unable to afford the upkeep of a computer. These costs include those for anti-virus and security software and upgrades, and to trouble shoot technical problems. The Council of Ageing WA also advised of frustration about the pace of change and the rate at which technologies became obsolete: seniors are isolated in their struggle to 'keep up'.[142]

3.106 Other concerns were the cost and unreliability of broadband services in regional areas. The Hobart Older Persons Reference Group saw broadband cost as a major limit on seniors' online access and skills.[143] Tandara Lodge Community Care, Sheffield Tasmania, commented on lack of competition between providers in the area, and on the price of antivirus software, computer hardware, printer inks and the 'hidden costs' associated with online shopping.[144]

140 Former Minister for Finance and Deregulation and former Parliamentary Secretary for Disabilities, 'Government Releases Website Accessibility National Transition Strategy', Joint *Media Release, 37/2010*, 30 June 2010.

141 CCI, *Older Australians and the Internet*, 2011, cited in ACMA, *Submission 24*, pp. 7–8.

142 See survey of agencies in Government of WA, *Submission 19*, p. 4.

143 The Hobart Older Persons Reference Group, *Submission 39*, p. 1.

144 Tandara Lodge Community Care, Sheffield Tasmania, *Submission 1*, pp. 1–2.

3.107 The Committee notes that the Government is supporting seniors by funding free secure internet access and training in libraries, through Seniors Kiosks, under Broadband for Seniors initiatives and at NBN Digital Hub trial sites. Proposals for free online access and training to seniors at these and other community centres had wide support in submissions.[145]

3.108 However, the NSA contended that while:

> Free internet kiosks and digital hubs will address the barriers of cost and lack of training in those areas that benefit from these initiatives…they are unlikely to fully address the barriers of lack of transport to reach these facilities, ineffective classes and instructional materials, low awareness of the existence of these services, and the need for extra support for older people who access the internet from home.[146]

3.109 As more services go online and face to face and telephone supports are reduced, the burden of upgrading to new systems and security products will be an increasing strain for seniors, especially if they are physically or mentally fragile.

3.110 The Government may wish to consider subsidies or a partnership with private industry to improve seniors' ability to access, apply and maintain security on their home computer or mobile systems. This is considered along with industry's costs settings for computers and security products, in Chapter 6.

Make it easy: a single portal for reporting and advice

3.111 A major obstacle to understanding the true extent of victimisation experienced by seniors is the low reportage rate of online crime. Factors which may contribute to this include embarrassment, lack of certainty about the illegality of an activity, or the conviction that there will be no result from reporting.[147]

3.112 The Committee also heard that the lack of clear reporting avenues for the different varieties of scam and online fraud is a major deterrent to crime

145 AHRC, *Submission 2*, p. 9; Australian Library and Information Association (ALIA) and National and State Libraries Australasia (NSLA), *Submission 6*, p. 2; WA Government, *Submission 19*, p. 5; DBCDE *Submission 25*, p. 3.

146 NSA, *Submission 29,* p. 29.

147 C Budd and J Anderson, 'Consumer Fraud in Australasia', *AIC Reports Technical and Background Paper 43,* pp. 5; 13.

reportage.[148] The AIC's Dr Rick Brown, Deputy Director of Research, explained:

> To illustrate, in Australia government agencies that may take reports of cybercrime include state or federal policing agencies, state and territory consumer protection agencies, the Australian Competition and Consumer Commission, the Australian Communications and Media Authority, the Australian Securities and Investments Commission and the Australian Taxation Office. Other organisations that may receive complaints include banks and financial institutions and online trading and auction sites, as well as social media sites. Expand this to multiple victims in multiple jurisdictions and the picture relating to just one case can become very complicated.[149]

3.113 There was strong stakeholder support for the streamlining of reporting arrangements, with a range of proposals made for the structure and functioning of an online central reporting point for all cybercrime:

- The CIS recommended an 'online central clearing house for complaints', noting that seniors in particular are confused and distressed by current arrangements.[150]
- The ACC also envisioned a single portal or co-ordinated gateway to direct the user to the correct information, and for help and advice.[151]
- Internet shopping site eBay and payment manager PayPal recommended a single contact point or a 'co-ordinated set of entry points' to provide all victims with guidance and support.[152]
- YOURLifeChoices, the online seniors' magazine, advocated for an industry and government supported 'one-stop-shop' for seniors in particular, backed up by telephone support, with access to education and advertising of cybersafety issues.[153]

148 *YOUR LifeChoices*, the seniors' online magazine conducted an online survey and received 701 individual comments on why seniors did not report a scam. 14 per cent stated they didn't know who or where to report the crime. See Mr Drew Patchell, Publisher Owner Director, *YOURLifeChoices* website, *Committee Hansard*, 18 May 2012, p. 2.

149 Dr Rick Brown, Deputy Director (Research), AIC, *Committee Hansard*, 10 October 2012, p. 2.

150 Professor Phair, CIS, *Committee Hansard*, 14 March 2012, pp. 1, 10.

151 Mrs Harfield, ACC, *Committee Hansard*, 15 August 2012, p. 3.

152 eBay and Pay Pal, *Submission 11*, Recommendation 4, p. [3].

153 YOURLifeChoices website, enewsletters and magazine, *Submission 38*, p. 4.

- The South Australian and WA Governments suggested that the DBCDE's Stay Smart Online site be upgraded for both information and reporting of offences, with a specific seniors' tab.[154]

3.114 Submitters emphasised that a user friendly format, with clear language and graphics and less embedded information, is particularly important to engage seniors.[155] WA ScamNet recommended its model where scam warnings appear at the top of search engine lists, noting that ACC and ASIC websites do not currently do this. An archive of online warnings could also be uploaded.[156]

3.115 The site should also link to a seniors' victim support or help line for personalised, non-technical advice.[157] Dr Cross reported that the UK and Canada have well developed online reporting sites which also offer victim support services, delivered by charitable agencies:

> In the United Kingdom, support for victims is facilitated by having a central reporting authority. When a victim calls Action Fraud to report whatever fraudulent experience they have had, they are then asked about the impact of that fraud on their life. If they rate the impact as quite severe they are then given the opportunity to receive a follow-up call from Victim Support, which is a charitable organisation over there, and they are able to receive some follow-up counselling to help them get back on their feet. That can be through either a telephone call or face-to-face counselling. Canada has a very similar program.[158]

3.116 The Committee notes that the Government has recently launched a seniors' helpline under its Broadband for Seniors initiative.[159] The Committee, however, believes that there would be merit in centralising reporting and support mechanisms for all cybercrime victims who need support or advice.

---

154 WA Government, *Submission 19*, ref. WA Department of Health and Department of Finance, p. 5; and Recommendation p. 8; SA Government, *Submission 37*, p. 11.

155 Government of WA, *Submission 19*, p. 5; Mr MacGibbon, *Committee Hansard*, 14 March 2012, p. 11; Ms Balsamo, AHRC, *Committee Hansard*, 23 March 2012, p. 2.

156 See, WA Government, *Submission 19*, p. 5.

157 WA Government, *Submission 19,* ref. Department of Communities, and Rec. p. 8.

158 *Committee Hansard*, 6 February 2013, p. 10.

159 In November 2012, see FaHCSIA, Broadband for Seniors website < www.necseniors.net.au/> viewed 15 February 2013.

Recommendation 6

That the Australian Government develops a centralised user friendly reporting and cybersafety awareness portal for all types of cybercrime with links to relevant regulators.

The site should feature a dedicated reporting tab, a seniors tab and be backed up by a telephone service which links individuals to appropriate victim support, training and other advice.

Recommendation 7

In support of the above, the Australian Government should investigate options for the contracting of appropriate non-government organisations or private organisations to provide support and advice to victims of online and technology related crime.

3.117 Another strong commendation for the centralised reporting facility is the need to collect and collate data on the various types of cybercrime and its effect on different segments of the community, including seniors. The criticality of this data to target both consumer education and to fine tune legislation and enforcement measures against cybercrime was universally emphasised by stakeholders.[160] The role for government in progressing this initiative is discussed in Chapter 5.

Concluding comments

3.118 Compared with the rest of the world, Australian seniors are an attractive target for cybercriminals. Relatively new to the internet, many are also relatively affluent.

3.119 Australia's mandatory superannuation requirements allow a lot of Australians to retire with lump sums to invest, or operate their own self-managed funds. Others may seek to establish an income stream for retirement, or be living on part or full pensions, and be tempted by online gambling, lotteries or other windfall schemes.

160 AFP, *Submission 20*, p. 5; CIS, *Submission 26*, ACMA, *Submission 24*, p. 2 and see Mr Rizvi, DBCDE, *Committee Hansard*, 12 September 2012 p. 4.

3.120 Given the dynamic nature of the internet and opportunism of global organised crime networks, the rollout of the NBN into regional areas, and seniors' increasing attraction of the tablet and the smartphone, it will be essential to ensure older Australians are upskilled and aware of both the risks and benefits of using digital technologies.

3.121 In addition to the range of cyber threats to which the community is exposed, the Committee also heard about the negative consequences of some seniors' risk averse behaviours. In the Committee's opinion, overcoming the fear of the unfamiliar will help seniors over 'the hurdle' of the digital divide.

3.122 In support of this, the Committee has made recommendations in this chapter to help seniors help themselves by providing for clear and more user friendly government information online, and by establishing a centralised access point for information and crime reportage, with follow up support for victims when needed.

3.123 In the following chapters, the Committee examines possible measures to address education and training needs, proposals for improved consumer awareness and regulatory reform, and the potential role of industry to help seniors gain confidence and remains safe online.