SUBMISSION NO. 25

Australian Government

Department of Broadband,
Communications and the Digital Economy

SUBMISSION TO THE JOINT SELECT

COMMITTEE ON CYBER-SAFETY

INQUIRY INTO CYBERSAFETY FOR SENIOR AUSTRALIANS

2012

Department of Broadband, Communications and the Digital Economy
38 Sydney Avenue, Forrest, Canberra ACT 2603 Australia website http://www.dbcde.gov.au

Summary

Australians are becoming increasingly engaged online, with new technologies such as smart phones, tablet computers, social media and cloud computing helping to change the way we live. Australian Bureau of Statistics figures show that at the end of June 2011, 79% of all Australian households had internet access at home.[1] Of these, approximately 92% were broadband connections.[2]

The digital economy is essential to Australia's long-term prosperity. The rollout of the National Broadband Network (NBN) is expected to bring substantial economic and social benefits to internet users. Improved access to health and aged care, increased online government service delivery and greater commercial opportunities will make life simpler, save time and drive economic growth.

However, both the extent to which Australians continue to engage online and the prosperity Australia derives from its engagement in the digital economy will depend upon the confidence and trust that Australian consumers and businesses have in the online environment. Malicious online activity has the potential to significantly undermine user confidence and prevent Australians from taking full advantage of the social benefits, commercial opportunities and improved access to services made possible by the digital economy.

One of the objectives of the national Digital Economy Strategy is to encourage all Australians to obtain the knowledge and confidence needed to secure the benefits of being online. This is true for everyone, but particularly for many seniors, who may not have had the same exposure to computing technology during their lifetime. Just over 53% of seniors accessed the internet during the 12 month period to June 2011.[3]

The Department of Broadband, Communications and the Digital Economy (the Department) aims to raise awareness of cybersecurity and cybersafety risks among Australian home users and small to medium sized businesses, and inform them of the simple steps they can take to protect themselves in the online environment. It does this through a number of initiatives, including:

- National Cyber Security Awareness Week, held annually in partnership with industry, community groups and all levels of government to deliver cybersecurity messages around Australia

- the Stay Smart Online website (www.staysmartonline), a key source of information for Australian internet users on cybersecurity and cybersafety issues. It provides

[1] Australian Bureau of Statistics (ABS), *8146.0 Household use of Information technology, Australia, 2010-11*, Household internet and computer access, Table 1
[2] ABS, *8146.0 Household use of Information technology, Australia, 2010-11*, Types of household internet access, Table 1
[3] ABS, *8146.0 Household use of Information technology, Australia, 2010-11*, Personal internet use, Table 1.

information on the simple steps users can take to protect their personal and financial information online

- the Stay Smart Online Alert Service, a free, subscription based service that provides information on the latest cybersecurity threats and vulnerabilities and possible solutions to address them

- the Budd:e cybersecurity education package for primary and secondary school students

- the Digital Hubs program, which helps communities gain the skills needed to maximise the benefits provided by the National Broadband Network and the digital economy

- the Cybersafety Help Button, a free application that provides internet users with easy online access to cybersafety information and assistance available in Australia

- The Easy Guide to Socialising Online website (www.dbcde.gov.au/easyguide), which provides cybersafety information on 26 different social networking sites, search engines and online games. This includes general tips on how to stay safe when using any social media site.

Introduction

The Department of Broadband, Communications and the Digital Economy welcomes the opportunity to provide input to the Joint Select Committee on Cyber-Safety Inquiry into Cybersafety for Senior Australians.

The Cyber White Paper discussion document[4] identifies the distinction between cybersafety, cybersecurity and cybercrime that the Australian Government makes for the purposes of its work. This distinction assists in the management of cyber issues by placing responsibility for these issues with the Commonwealth agencies best able to respond. We recognise, however, that the general public may not make these distinctions

Accordingly, this submission treats the term 'cybersafety' in its broadest sense, incorporating issues relating to cybersecurity and cybercrime, as well as those relating to cybersafety. This is in line with the terms of reference of the Inquiry. 'Seniors' are understood as Australians aged 55 and above.

Australian internet use

The Inquiry comes at a time when Australians are increasingly engaged online. At the end of June 2011 there were 10.9 million internet subscribers in Australia, an increase of 14.8% since June 2010.[5] Seventy-nine per cent of all Australian households now have internet access at home.[6]

A significant area of growth has been in the uptake of mobile wireless technology, which allows users to connect devices to the internet via a USB or Wi-Fi modem. Mobile wireless (not including mobile phone connections) is numerically the fastest growing internet access technology, increasing by 600,000 to 4.8 million in the six months to June 2011.[7]

At the same time, there has been a significant increase in the number of Australians accessing the internet through a mobile phone. During December 2010, 3.1 million Australians aged 14 years and over used the internet via a mobile handset. This compares with 1.9 million during December 2009.[8]

Senior Australians, too, are accessing the internet in greater numbers. In 2003, 21% had accessed the internet at least once in the previous 12 months. By June 2009 this figure had increased to 41%.[9] But while senior Australians are engaging online more than ever before, they are still less likely to do so than other age groups. Only 37 % of seniors aged 65 and above, and 71% of those aged 55 to 64, accessed the internet in the 12 month period to

---

[4] Department of the Prime Minister and Cabinet, *Connecting with Confidence: Optimising Australia's Digital Future*, http://cyberwhitepaper.dpmc.gov.au/white-paper
[5] ABS, *8153.0 Internet Activity, Australia, June 2011*, Summary
[6] ABS, *8146.0 Household use of information technology, Australia, 2010-11*, Summary Indicators, Table 1
[7] ABS, *8153.0 Internet Activity, Australia, June 2011*, Summary p1
[8] Roy Morgan Single Source, Dec 2010
[9] ABS, *8146.0 Household use of information technology, Australia, 2010-11*, Internet and computer use by older persons, Table 2

June 2011. This compares with more than 96% of Australians aged 18 to 24, and 93% of those aged 25 to 34.[10]

Of those seniors who used the internet at home, email (90%) and general browsing (84%) were the most popular online activities. Activities involving financial transactions were significantly less popular – 54% of seniors paid bills or used banking facilities online and only 34% purchased or sold goods, compared to 70% and 49% for other age groups. When providing reasons for why they did not make purchases online, seniors were more likely to respond with 'security concerns/concerned about providing credit card details online' (29%) than other age groups (19%). [11]

Nature and prevalence of online risks

Malicious online activity has the potential to undermine Australians' confidence in the internet. As Government and industry continue to invest heavily in new technologies to support the digital economy, it is important that people can engage online in a confident and secure manner. Attacks directed at people or businesses can have serious personal and financial implications and deter new users from taking advantage of the opportunities available. Large scale or widespread attacks have the potential to damage Australia's digital economy.

The volume and types of online threats have risen in line with the increased uptake of information and communication technologies within the economy - these same technologies that are providing Australians with so many benefits are also creating opportunities for those who seek to exploit them for personal or financial gain.

The following provides a snapshot of recent malicious activity on the internet:

- An increase in the number of scams delivered online and reported to the Australian Competition and Consumer Commission, from 14,101 in 2009, to 19,074 in 2010 [12]

- The personal and financial details of millions of internet users compromised in a series of security breaches at major corporations, including one of the largest data thefts ever recorded when the details of up to 77 million Sony PlayStation Network users worldwide were affected[13]

- 93% increase in the number of web based attacks in 2010 compared to 2009[14]

As the Australian Crime Commission (ACC) observes, the internet is an attractive medium for criminals because it is anonymous, fast, easily accessible, globally connected, borderless and contains high volumes of financial and personal data that can be exploited. It notes that

[10] ABS, *8146.0 Household use of information technology, Australia, 2010-11,* Household internet and computer use, Table 1
[11] ABS, *8146.0 Household use of information technology, Australia, 2010-11,* Personal internet use, Table 8
[12] Australian Competition and Consumer Commission, *Targeting scams – Report of the ACCC on scam activity 2010*, p 1
[13] PandaLabs, *Annual Report 2011 Summary*, page 6
[14] Symantec, *Internet Security Threat Report*, *Trends for 2010*, Volume 16, page 6

as more businesses move their enterprises online seeking new opportunities for profit, so too do organised crime entities.[15]

Estimates of the cost of cybercrime to the Australian economy vary. The Australian Federal Police estimate that Australian losses are in excess of $1 billion a year.[16] Internet security vendors generally put the figure much higher - a report by Symantec calculates that cybercrime cost Australians $4.6 billion in 2010.[17] While a precise figure is difficult to determine, it is clear that cybercrime has a significant economic impact on many Australians.

The methods used by criminals to exploit the online environment are varied. They are also increasingly targeted and sophisticated. Scams continue to be a significant source of such risk: in 2010, the internet was the most common medium used to approach Australian consumers, with 45% of reported scams starting with online contact[18].

The popularity of social media continues to provide opportunities for those who wish to exploit it for malicious purposes. Easier access to personal information makes it easier for criminals to commit identity theft, or use that information to gain access to other information through targeted phishing attacks.

Another area of concern is attempts to exploit the growing popularity of smartphones. Smartphones allow users to access the internet from a handset and perform similar online activities to those performed on traditional computers, but are not generally thought of as such by users. This may mean that users are less likely to be aware of, or take steps to avoid, potential threats. According to a June 2011 report, 46% of Australian mobile phones are smartphones, with 23% of those owned by users aged over 50.[19]

The volume of malware targeted at mobile platforms has steadily increased since 2009[20], but in general this threat remains limited in the number of devices it affects as well as its impact.[21] Currently, fewer people are using smart phones to perform financial transactions online than on traditional computers.[22] It is highly likely that as this changes the volume of malware targeted at smart phone users will increase.

<u>Seniors</u>

Research into the effects that malicious online activity has had on senior Australians is relatively limited. While considerable research has been conducted into the cybersafety risks faced by children and teens, there have been few major research reports or initiatives

[15] Australian Crime Commission, http://www.crimecommission.gov.au/publications/crime-profile-series-fact-sheet/cyber-crime
[16] Australian Federal Police, 2010, Referenced in Cyber White Paper – Discussion Paper
[17] Symantec, *Internet Security Threat Report*, *Trends for 2010*, Volume 16
[18] Australian Competition and Consumer Commission, *Targeting scams – Report of the ACCC on scam activity 2010*, p 1
[19] Nielsen, *Telstra Smartphone Index – June 2011*, page 4
[20] McAfee, *McAfee Threat Report Third Quarter 2011*, page 4
[21] Symantec, *Internet Security Threat Report*, *Trends for 2010*, Volume 16, page 6
[22] ACMA*, The internet service market and Australians in the online environment*, July 2011, p22

centred on the cybersecurity and cybersafety of senior citizens. Much of the existing research tends to be a sub-section of a larger and more general report or survey on internet demographics rather than a specific investigation of senior Australians.

The Department itself does not generally distinguish between the online risks faced by senior Australians and those faced by the broader adult population. Rather, our approach to awareness raising focuses on behavioural types, with senior Australians represented as a subset.

The Department conducted segmentation research in 2011 to quantify internet behaviour amongst Australian internet users, and identify opportunities to better target the Department's awareness raising activities. It identified four behavioural segments: 'comfortable but wary'; 'watchful transactors'; 'confident and (tech) savvy'; and 'fearful avoiders'. The 'fearful avoiders' segment (22%) was the group most likely to feel that they do not know enough about how to keep themselves and their details safe online (or protect their privacy online) and comprised mainly older users.

Research conducted by the Australian Communications and Media Authority (ACMA) indicates that seniors are increasingly interested in learning digital skills.[23] The two most popular skills of interest for those aged 55 and over were how to manage personal information online and how to use the internet safely, with 44 per cent of respondents in this age group expressing an interest in these skills.

Awareness & confidence

The Department undertook a survey in 2010 to establish baseline data on the level of cybersecurity awareness amongst Australian internet users. A further survey was undertaken in 2011 to measure the degree of change in this level of understanding. No specific data was collected on Australian seniors. However, just under a third of respondents in both these surveys (31% and 32% respectively) were aged 55+.

The surveys indicated that Australian internet users have a reasonable knowledge of common security risks that may be faced when using the internet. The most commonly mentioned risks were malicious software (53% in 2011, 56% in 2010) and loss of financial information (51% in 2011, 50% in 2010), followed by identify theft (35% in 2011, 37% in 2010) and online scams and hoaxes (31% in 2011, 32% in 2010).

As can be expected, knowledge of risks and the confidence to deal with those risks tends to increase the more people use the internet. ACMA research indicates that people using the internet more than 15 hours per week are more likely to feel confident in managing the security of their personal information online, and protecting themselves from malware when accessing media, than those who access the internet less than seven hours a week.[24] For people who are high users of the internet there is no significant difference in confidence levels between age groups. Seniors who use the internet a lot are as confident online as other users. However, as the research does suggest that senior Australians are generally

[23] ACMA, *Digital Australians – expectations about media content in a converging media environment*, 2011, page 74
[24] Ibid, page 68

lighter users of the internet than other age groups, a greater proportion of seniors are likely to be represented in the groups that lack confidence.

Current initiatives

Internet security is a responsibility shared by all who engage in the online environment. While Government efforts to create a safe and secure online environment span regulation, enforcement, education and awareness raising and international engagement, ultimately it is businesses and individuals who must take responsibility for their own safety and security online. This means being aware of the potential risks and taking the necessary steps to protect themselves. Businesses should develop safe practices to protect both themselves and their customers, and promptly report incidents when they occur. Individuals should ensure that they take appropriate measures to protect themselves online.

The Government's 2009 Cyber Security Strategy outlines the Department's responsibility for raising awareness of online risks with a view to improving online practices and behaviour. The Department targets Australian home and small to medium sized business users, regardless of age, and aims to inform them of the steps they can take to protect themselves in the online environment. It does this through a range of initiatives, including:

National Cyber Security Awareness Week (Awareness Week)

The Awareness Week aims to help Australians understand cybersecurity risks and educate home users (including older Australians) and small businesses about the simple steps they can take to protect themselves, their families and their businesses online. It is held annually in partnership with industry, community groups and all levels of government, though collaboration continues all year. Over 530 organisations partnered with Government in the 2011 Awareness Week to deliver cybersecurity messages around Australia, an increase from the 156 organisations that participated in the 2010 Week. This increase was largely due to an increase in the number of schools participating. There was also a significant increase in media coverage across print, radio, television and online sources, from 150 media items in 2010 to 260 media items in 2011.

During Awareness Week, there is some focus on seniors through engagement with the Australian Communications Consumer Action Network (ACCAN) and the Australian Seniors Computers Clubs Association (ASCCA). The President of ASCCA is an NBN champion and is a member of the Awareness Week Steering Committee, representing the needs of senior Australians.

This year's Awareness Week will be held from 4 – 8 June 2012. A range of events will be held in partnership with industry and consumer groups, community organisations and government agencies at all levels, across metropolitan and regional Australia. The Department has developed a program of activities to increase public awareness of cybersecurity messages and enhance the support and engagement of partners in the lead up to Awareness Week. The program emphasises at least one theme per month, and includes:

> January to February 2012: 'back to school' - retailers invited to deliver cybersecurity promotional material at major outlets

March 2012: 'fraud awareness' - the Department working with the Australian Competition and Consumer Commission to raise public awareness of identity crime issues as part of National Fraud Awareness Week.

April to May 2012: 'privacy awareness' - the Department working with the Office of the Australian Information Commissioner to raise understanding of the dangers of handing out personal information, especially over the internet, as part of Privacy Awareness Week.

Awareness Week will conclude with an Over the Horizon Forum, which brings together experts from the public and private sectors to discuss current and future cybersecurity challenges and how the government and the private sector can work together to address these challenges.

Stay Smart Online

The Stay Smart Online website (www.staysmartonline.gov.au) is a key element of the Government's cybersecurity awareness raising initiatives. The website provides information for Australian internet users on cybersecurity issues and the simple measures they can adopt to use the internet in a secure and confident manner. The website provides access to a range of resources, including top tips, quizzes and fact sheets and is designed to educate users at all levels of computer literacy, including the 'fearful avoiders' group. It also directs parents, grandparents and teachers to existing resources that will help them protect children online. In addition, it provides a series of videos that feature older Australians and covers relevant material relating to online dating and financial scams.

During 2011 (January – December), the site received an average of 19,385 visitors per month. There was a peak of 33,127 visitors in July 2011, following the Awareness Week which was held 30 May – 3 June 2011.

The Department is currently undertaking a review of the website to better meet the needs of Australian internet users, including senior Australians.

Stay Smart Online Alert Service

The Stay Smart Online Alert Service provides information in plain language on the latest cybersecurity threats and vulnerabilities and possible solutions to address them. This free subscription based service is delivered through the Government's Stay Smart Online website.

The service had a 17.8% increase in subscriptions from July 2010 to June 2011. Feedback from subscribers indicates that 94% found the service useful and 97% understood the content. The Alert Service is being revamped as part of a review of the of the Stay Smart Online website.

Cybersafety Help Button

The Cybersafety Help Button provides internet users, particularly children and young people, with easy online access to cybersafety information and assistance available in Australia. It offers counselling, reporting and educational resources to assist young people deal with online risks including cyberbullying, unwanted contact, scams and fraud, and offensive or inappropriate material.

While primarily aimed at providing help and advice for young people, the Cybersafety Help Button has benefits for all users, including seniors, as noted by the Gadget Guy, Peter Blasina:

"There are times when not only young people, but everyone using the internet needs help and advice on how to handle a situation that disturbs them – such as when they are subjected to cyberbullying, or they receive other unwanted contacts, a suspicious email or see content that is upsetting."

Easy Guide to Socialising Online

The 'Easy Guide to Socialising Online' provides cybersafety information for 26 different social networking sites, search engines and online games, and gives step by step instructions on how to report cyberbullying, abuse and inappropriate content on these sites. It was developed in partnership with industry and young people to help parents, children and educators combat cyberbullying and inappropriate content online. It provides clear information on how to adjust safety and privacy settings on websites as well as tips on how to stay safe when using any social media site.

Direct engagement with seniors groups

The Department is currently negotiating with the Council of the Ageing (COTA), the peak organisation concerned with all issues related to ageing, to develop a cybersecurity training package for older people. This will be delivered through COTA's peer education program. The Department is also preparing articles on cybersecurity issues for distribution through COTA's communication channels. It is working with COTA to identify other opportunities, such as seminars and conferences, to promote cybersecurity awareness among older people.

The Department also engages more broadly with senior groups by supporting activities, such as conferences and seminars conducted by the ASCCA. It also does some collaborative work with the Department of Families, Housing, Community Services and Indigenous Affairs through its Broadband for Seniors initiative.

Digital Hubs

A 2011 survey found that approximately 21% of Australians do not use the internet.[25] This figure is higher for senior Australians and people in regional areas.

[25] ABS, *2010-11 Household Use of IT*, Personal internet use, Table 1

The Digital Hubs program, administered by the Department, aims to encourage Australian households to realise the benefits of greater digital engagement and how to do so safely and securely. The program aims to establish a Digital Hub in the 40 communities to first benefit from the NBN, providing local residents with online training and the opportunity to experience NBN-enabled services and technology.

Targeted action is required to minimise the extent to which digital exclusion overlaps with, and exacerbates, social exclusion and to maximise the extent to which the benefits of greater digital engagement are enjoyed by all Australian families and communities. Older Australians are recognised by the program as a target group that has concerns about online safety and security.

The key tool that will deliver the necessary digital literacy training in a Digital Hub is a new website www.InternetBasics.gov.au currently under development within the Department. The design, site name, digital media, graphic elements and scope of content of the new website has been informed by capturing the needs of users through User Needs Analysis and User Expectations research. This research was conducted through focus groups held across four NBN connected communities plus a qualitative survey of over 1000 Australians. Information is presented through short videos with a friendly (real) person introducing complex information in plain English about:

- Protecting your computer,
- Protecting yourself and
- Protecting your children online.

Departmental research also defined seven persona types which help explain the barriers preventing individuals taking the first steps toward engaging online. Seniors were not defined as a persona type for this website as the target audience is not based on age demographics; rather it is those Australians who currently are not online or rarely participate online. Nevertheless, the Department recognises that seniors are over represented in the target audience and across all the seven personas developed in the User Needs Analysis.

Older Australians who attended focus groups held in four NBN connected communities all identified with multiple barriers to getting online and expressed fears in terms of theft of identity, finances and private information.

The seven personas, or barriers, the research identified are:

- Paranoiac – “I'm worried someone will steal my identity”
- Techno overwhelmed – “ I wouldn't know where to start”
- Sceptic – “ the internet is not relevant to me”
- Economically disadvantaged – “ I can't afford the internet”
- Low literacy and numeracy – “I have trouble understanding the internet language”
- Differently abled – “the internet is not accessible to me”
- Geographically disconnected – “I have learnt to live without the internet”

Other Australian Government agencies are also undertaking awareness raising activities that benefit seniors, for example:

Broadband for Seniors

Broadband for Seniors is a Department of Families, Housing, Community Services and Indigenous Affairs initiative providing older Australians with free access to computers and the internet, as well as training in basic computing skills. The initiative aims to support older Australians in gaining the confidence and skills they need to use new technology, so that they can fully participate in and share the benefits of the growing digital economy. Up to two thousand internet kiosks have been opened across Australia where seniors can learn how to access computers, surf the internet and send emails in a supportive and friendly environment.

Kiosks have been established in places that seniors regularly visit or that provide existing services to seniors, such as community centres, libraries, retirement villages and clubs. Training is provided in a friendly face-to-face environment by volunteer tutors. Seniors are also provided with training materials so they can learn at their own pace as well as on their computers at home.

Cybersmart

Cybersmart is a national education program administered by the ACMA that provides a range of practical and age appropriate resources for teachers, students, parents and carers of children. The program hosts a cybersafety website, www.cybersmart.gov.au, which provides practical help and advice on cybersafety issues. It has relevance for senior Australians needing assistance in understanding and dealing with cybersafety issues impacting those in their care, particularly grandchildren.

SCAMwatch

The Australian Competition and Consumer Commission produces *The Little Black Book of Scams* and manages the SCAMwatch website, which together provide a wealth of information for consumers and small businesses about how to recognise, avoid and report scams, including those online.

Conclusion

With the internet playing an ever increasing role in the daily lives of many Australians, it is clear that the level of trust that consumers and businesses have in the digital economy is critical to its success, and consequently, Australia's future prosperity.

The Department's activities in this space are aimed at raising awareness of these risks and providing information on the steps that can be taken to protect against them. Many risks can be avoided simply by following good online practices or procedures. These can be as simple as using updated security software, maintaining strong passwords or thinking carefully before clicking on links or attachments in emails. Such practices help to protect all Australians who engage online, regardless of age. This is a useful approach to online security as good practices can mitigate multiple threats.

Based on our experience, the vulnerability of an individual to a specific online risk is related less to the individual's age than the individual's knowledge and behaviour, that is, knowledge of the risk, and behaviour when confronted with it. Research indicates that those seniors who are regular users of the internet are no less confident in their abilities to protect themselves online than users in other age groups.

This is significant in that statistics show that seniors are overrepresented in the percentage of Australians who are either light users of the internet or who are not online at all. From this perspective seniors could be said to be more vulnerable to online risks, not because the risks are any greater than those faced by other age groups, but because seniors as a group are less likely to have the knowledge and confidence to deal with those risks. As such the Department recognises the benefit of programs such as Digital Hubs and Broadband for Seniors in helping to give seniors the skills to engage in the digital economy with confidence.

More research into user behaviour and online risks would be of value and may elicit trends specific to seniors that we are not seeing now. If that were the case the Department would consider new ways to assist seniors in better protecting themselves online.