SUBMISSION NO. 19

GOVERNMENT OF
WESTERN AUSTRALIA

RECEIVED
23/2/12

**Minister for Child Protection; Community Services;
Seniors and Volunteering; Women's Interests; Youth**

Our Ref: 36-07572

Senator Catryna Bilyk
Chair
Joint Select Committee on Cyber-Safety
PO Box 6021
Parliament House
CANBERRA ACT 2600

Dear Senator Bilyk

Thank you for your letter dated 24 November 2011 inviting the Western Australian Government to make a submission to the Joint Select Committee on Cyber-Safety's Inquiry into Cybersafety for Senior Australians. The Premier has requested that I prepare and submit this on behalf of the Western Australian Government.

The Western Australian Government welcomes the opportunity to respond to the Terms of Reference that form the foundation of this inquiry.

The Western Australian Government is of the view that it is critical to support our seniors to use new technologies, as these are increasingly becoming the primary means of providing information and services. However, at the same time there is the need to ensure that there are sufficient safeguards in place to maintain their safety and build their confidence in these systems.

Within this context, please find attached the Western Australian Government's submission addressing cyber-safety for seniors.

Yours sincerely

Robyn McSweeney MLC
**MINISTER FOR CHILD PROTECTION; COMMUNITY SERVICES;
SENIORS AND VOLUNTEERING; WOMEN'S INTERESTS; YOUTH**

17 FEB 2012

Inquiry into Cybersafety for Senior Australians
Submission from the Western Australian Government

Background

Internet based technology is advancing at a fast pace, offering opportunities to communicate, conduct business, and obtain information in ways that were not possible in the past. While senior Australians are a rapidly growing group of users, there is research showing that up to 40 per cent of senior Australians do not have the skills, knowledge, capacity to pay, or interest to use the Internet, due to concerns about security and viruses[1].

This highlights the need for strategies to improve safeguards and protect people's privacy, and to use this as a means of building their confidence in these systems [2]. However, the matter needs sensitive handling. If seniors continue to feel intimidated by the technology, they may be at risk of isolating themselves as more and more services move online.

Recent research[3] recommends the provision of cheaper computers and Internet access, free and more effective training (preferably one-on-one), a free Internet helpline, and more user-friendly web interfaces to overcome the barriers.

Other research findings[4] highlight that unlike other novice computer users, seniors are "in many cases required to turn to a web-based environment despite their desire to remain apart from it"[5]. This research investigated web-based security information sources (including government sites such as NetAlert (now defunct), CyberSmart, and StaySmartOnline), concluding that these do not provide adequate help both in terms of content or design. The researchers suggest that information portals need simple language, ease of navigation, and graphical step-by-step tutorials (not just descriptions) to be more effective.

The Council on the Ageing (COTA) WA published a report[6] that recommended:

- widely available, low cost training with targeted promotion of the benefits of the Internet for seniors
- better consumer protection
- advice and assistance to navigate the market
- more reliable and accessible technical support services
- more targeted government sponsored cyber security and safety campaigns
- consultation with seniors on e-government matters.

[1] Anna Salleh, 'Seniors Left out of the Online Loop', ABC Science, 8 August 2011, http://www.abc.net.au/science/articles/2011/08/08/3288396.htm

[2] A further threat to cybersafety is cyber bullying. Professor Donna Cross from Edith Cowan University Child Health Promotion Research Centre has done significant research into cyber bullying, mainly in relation to school age children.

[3] Dr Sandra Haukka, Australian Research Council Centre of excellence for Creative Industries and Innovation (CCI) at Queensland University of Technology (in conjunction with National Seniors Australia (NSA) and .au Domain Administration (auDA) Foundation), 'Older Australians and the Internet'

[4] David M. Cook, Patryk Szewczyk, and Krishnun Sansurooah, Edith Cowan University WA, 'Securing the Elderly', presented at the Second International Cyber Resilience Conference

[5] Ibid, p.21

[6] COTA WA (2011), 'Where do I Start? Female seniors and the Internet' based on a literature review, interviews with a provider of technology trouble-shooting service, an Internet provider, tutors for senior Internet users, and 15 female seniors. Additionally five focus groups of 35 participants were held.

Current Status

The response below to the Terms of Reference incorporates input from a range of Western Australian public sector agencies and organisations[7], for consideration by the Cyber-Safety Committee. The WA Department of Commerce (Consumer Protection) provides the majority of comments and examples, informed through complaints and investigations from the WA community via ScamNet[8].

1. **The nature, prevalence, and level of cybersafety risks and threats experienced by senior Australians**

Internet scams and schemes are an escalating problem and many people fall victim every year. In 2007 the Australasian Consumer Fraud Taskforce—a group of 21 Australian and New Zealand government agencies—conducted a survey in partnership with the ABS to profile scam victims in Australia[9] .

While it is difficult to be precise because many victims do not report the crime, some estimates are that one in 20 Australians are caught by scams every year. It is also estimated that about two-thirds of consumer fraud now occurs online.

In the twelve months prior to the 2007 survey, people aged 35 to 44 years had a victimisation rate of 2.6 per cent for all scam types, while those 55 and over had a rate of 1.6 per cent. Those earning a personal weekly income of between $1 500 and $2 499 had a victimisation rate of 3.9 per cent. The rate was lower for people earning a weekly personal income of less than $499 (1.6 per cent).

Lotteries accounted for 84 100 victims (victimisation rate of 0.5 per cent), pyramid schemes 70 900 victims (0.4 per cent) and phishing and related scams 57 800 victims (0.4 per cent).

Reports from the Seniors Telephone Information Service at the WA Seniors Card Centre (Department for Communities) also confirm that lottery scams, where a person is asked to send through their bank details or pay a fee to obtain their 'winnings' is most prevalent. Phishing, where a person receives a bogus email requesting confirmation of credit card details or other personal information, is the next most frequently reported scam.

The 2007 survey indicates that seniors are not commonly the targets of online scams. However, the Western Australia Police Computer Crime Squad (CCS) suggests that senior Australians are more vulnerable to cyber offences than other adult age categories.

Consumer Protection believes that the older generation are generally cautious online, especially in areas in which they do not have extensive experience, such as credit card use. Seniors may find it hard to distinguish between safe and unsafe sites, and this may contribute to their reluctance to engage in online commerce. Seniors do not necessarily

[7] Agencies that provided input for this submission: lead agency - Department for Communities (including the Seniors Card Centre), Department of Commerce (Consumer Protection), Disability Services Commission, Department of Finance, Department of Health, Office of the Public Advocate, State Library of Western Australia, Department of Training and Workforce Development, and the Western Australian Police

[8] WA ScamNet does not provide a breakdown of data according to demographics such as age, so comments are generalised. However, reports suggest that white-collar males aged 45-55 who gamble sustain the largest losses. Though seniors may lose less in material terms than this group, the impact of any losses are much greater and there is less ability to recover as many seniors are on a fixed income.

[9] http://www.abs.gov.au/Ausstats/abs@.nsf/0/0BFD18E71ADFB95FCA2574740015D60C

understand how the cyber world works. For example, when doing a Google search, many would not be aware that the first few results are often advertisements, rather than the top search results. Seniors may also not understand the risks associated with sending on forwarded emails and chain mail.

Reports to the Department of Commerce's WA ScamNet indicated that the common cyber risks to seniors include emails asking for wire transfers, dating scams (limited), and work from home schemes. The scams often highlight the opportunistic nature of cyber-fraud. For example, charity scams often mimic real campaigns such as the Queensland floods or bush fire appeals.

Cyber-wise, seniors may also be more at a risk of losing personal information and identity than money. For example, the Office of the Public Advocate and State Administrative Tribunal recently established that a senior in a particular investigation did not have the skills and knowledge to use the Internet. The investigator assessed that the son of the elderly man wrote emails that suggested that they had come from his father, thus appropriating his father's identity.

WA ScamNet reports suggest that seniors tend to be more commonly targeted by letter or phone scams. However, it should be noted that many scams involve an online component even if they did not start online. They may begin with a phone call or a letter but move online with the exchange of emails and links to fake websites.

A recent 'Microsoft' scam[10] followed this pattern. Householders were telephoned and asked to go to their computer and follow some verbal prompts to allow the 'Microsoft' technician remote access to their machine. Seniors may have been more vulnerable to these scams, as they may lack the technological knowledge and general computer literacy that helped alert many who were contacted that this was a scam. Seniors are also more likely to be at home during the day, where they can answer a scammer's phone call and be led to a cyber-scam.

Seniors can be at a cyber-risk because of lack of awareness of the conventions of online commerce. The extensive terms and conditions often presented at the last stage of a transaction can be complex, but they are important.

The informality of some sites may also be an issue. Some rental and retirement decisions may lead seniors to be exposed to cyber criminals, via real estate offers on on-line sales sites.

Seniors' caution about scams and the Internet could lead them to be scammed by hoaxes that warn about undesirable occurrences. An example is the Do Not Call Register hoax, where consumers were warned via email that they needed to register their mobile numbers with the Do Not Call Register, to avoid being open to telemarketers' calls. This was a hoax, presented as protection from something undesirable.

[10] http://www.microsoft.com/australia/presspass/post/Microsoft-issues-warning-on-phone-scam

2. The impact and implications of those risks and threats on access and use of information and communication technologies by senior Australians

As seniors are worried about being scammed and see the Internet as a place where this can happen, they are generally cautious. Seniors can have difficulty distinguishing between real and fake websites or online offers and this may then limit their willingness to engage in cyber commerce and communications. Seniors who have been scammed find it particularly difficult to go back to doing any type of cyber activities.

Seniors can be afraid of the Internet and do not use it as much as they could. While this reluctance to engage could protect them from some scams, they also miss out on the benefits the Internet provides. This can mean that seniors become disengaged from society in general and miss out on positive experiences. If Australia is moving towards a 'digital democracy', that is where views and preferences are expressed in the virtual world; seniors may be left out of this system due to their fear of the cyber world. As many government departments are moving towards electronic means of communication, such as online publications, forms, and e-health initiatives, seniors are more likely to be unable to access these items if they are not online. The divide is further increasing with the move to conducting online activities via smart phones and other portable devices.

According to the State Library of WA, despite the decreasing cost of purchasing a computer and the associated communications charges, many seniors are unable to afford a computer. These costs are compounded by the cost of software and ongoing support required to download and regularly update software (such as anti-virus and security software), and to trouble shoot technical problems. The Council on the Ageing (COTA) WA also notes a frustration at the pace of change, where new devices render previous technologies obsolete. This may further isolate seniors as they struggle to 'keep up'.

The Department of Commerce is concerned that the upcoming transfer to digital televisions will also provide an opportunity for scammers to take advantage of a lack of knowledge and awareness in the community. As a result, scammers may knock on doors offering to 'upgrade' the old television for an inflated cost. Information about the digital transfer is mostly available online, meaning that seniors have limited access to it. This may result in seniors being more vulnerable to scams relating to this transfer, even if by non-cyber means, due to the information not reaching them. While the scam would not be a cyber-scam, seniors' lack of use of the cyber world would lead to them being more vulnerable to certain scams due to lack of education.

There is the additional concern that seniors' hesitation to use credit cards online could result in them using less protected methods of payment, such as wire transfers. Wire transfer payments are a common method for scammers to receive money, as it is very difficult to trace wired money.

Anecdotal evidence from the Seniors Ministerial Advisory Council notes that a further impact from low participation rates concerns those seniors who are cyber-literate and face the issue of 'burn out' if they operate in organisations staffed mainly by seniors. These seniors are the ones who keep the organisation connected and viable. Increasing online participation generally would assist in reducing this pressure.

3. The adequacy and effectiveness of current government and industry initiatives to respond to those threats, including education initiatives aimed at senior Australians

Whilst the StaySmartOnline website is a useful resource with practical information on one site, increased promotion is required to raise awareness. The Department of Health and the Department of Finance both suggest the addition of a new section for seniors to the website that contains specific information for this audience. Though information may be similar to that contained on the 'Home Internet Users' tab, a seniors section needs simpler language and graphical examples, which better suits novice users.

The Department of Commerce's WA ScamNet names known scams and provides information on current scam activities. Each year WA ScamNet receives approximately 39 000 scam reports of suspect letters, door-to-door traders, telemarketers, SMS and online scams (emails, websites etc.). While Commerce does promote information concerning current scams in the media (via media statements and through regular media columns and radio spots) the archive of information is made available online. Commerce notes that this inadvertently limits the audience to more educated online users and excludes many seniors from finding this information, and will consider addressing this in the future.

Of note, the Australian Securities and Investments Commission (ASIC) and the Australian Competition and Consumer Commission (ACCC) scam sites do not identify specific traders by name, they provide general scam information and a description of the type and characteristics. Commerce's WA ScamNet names traders, making the information more specific to consumers' needs and commonly if the name of the scam is put into search engines such as Google, the Department of Commerce's warnings will be amongst the top search items.

Western Australia has a network of 233 public libraries that act as community hubs. Most of these libraries provide free access to computers for their members with up-to-date software loaded, including the necessary anti-virus and other security measures. This provides seniors with some confidence as the computers they are using are from a trusted source.

A primary role for libraries is the provision of computer literacy training for people of all ages. Offered in a non-threatening environment with people of their own generation, many libraries provide classes for seniors not only in how to use a computer, but also in particular programs and areas of interest (e.g. genealogy, business, books etc.), providing trusted guides to the best places to go for these resources.

As part of these training packages, many libraries provide information on maintaining security on the Internet and on cybersafety. For example, the City of Stirling libraries have on their website a page on "Cyber Safety" with links to relevant resources. http://www.stirling.wa.gov.au/Home/Library/Whats+On/Cyber+Safety.htm

Some public libraries have taken advantage of programs such as the Australian government's "Broadband for Seniors", to provide dedicated kiosks for seniors to use the Internet and providing a place where group or individual training can be offered.

The WA Department of Training and Workforce Development also funds community-based organisations under the First Click and Second Click programs to provide free basic computer literacy skills that include how to operate a computer and how to use the Internet and email. Program resources cover security issues and protection of privacy through topics on passwords, Internet banking, chat lines, and email. Seniors are one of the target groups for this program. For further information on these programs go to http://www.trainingwa.wa.gov.au/firstclick/detcms/navigation/what-are-first-click-and-second-click/

The Australian Communications and Media Authority (ACMA) have various cyber-smart programs. A valuable addition would be a seniors' specific program.

The research articles mentioned earlier suggest a mixed degree of success with existing initiatives. Either increased promotion or increased targeting of resources is required to raise confidence levels amongst seniors.

4. Best practice safeguards, and any possible changes to Australian law, policy, or practice that will strengthen the cybersafety of senior Australians

A program that educates seniors about cyber-scams but also emphasises the benefits of cyber commerce and communications may be effective. Many messages seniors receive about the Internet are negative. When this is combined with seniors' lack of cyber operational knowledge, it contributes to their hesitation to engage online. More positive stories are needed to outline the benefits of cyber commerce and communications, including information about online culture and behaviours. This empowers seniors to identify a scam and be confident about using legitimate services. The Department for Communities believes that information needs to be pitched at the most basic level to avoid confusion and frustration. Peer training is even more effective as presenters can empathise with seniors and share their experiences of learning how to operate online at a later stage in life. Peers successfully demonstrate that it is possible to learn new technology, and reduce initial apprehensions.

Following are some current WA initiatives and suggestions that can be considered at an Australia-wide level.

Consumer Protection in WA (a division of the Department of Commerce) conducts compliance visits to retirement villages. These visits (and those conducted by equivalent agencies elsewhere in Australia) can distribute cyber-awareness and cyber-smart educational material.

Education initiatives aimed at reducing the 'shame' aspect of being scammed and encouraging people to come forward are also helpful. It is hard for anyone who has been scammed to come forward and admit it. Without this information, it is difficult for consumer protection agencies to identify operational scams. Awareness of these scams can be used to protect others from being scammed.

In WA, Consumer Protection's regional officers educate post office staff about cyber scams. As many scammers rely on wire transfers to make their money, post office staff can look out for seniors who may be wiring money to potential scammers. These staff can then advise senior clients to contact Consumer Protection for further advice before going ahead with their transactions.

A greater focus on coordinating consumer education concerning wire transfers through federal departments is recommended. A commonly held view by people who are caught in a scam and sending funds offshore is that they know the person they are sending it to. The belief that a relationship established by way of an online profile, some email communication or even a telephone conversation is difficult to counteract. Commonly the wire transfer system is used as funds arrive in cash at the destination of choice and can be collected with little or no identification. Wire transfer has become the primary choice of scammers and convincing a victim that they are a victim is difficult at the front counter of a post office.

Strengthening the laws in relation to online advertisements, and making publishers responsible for their online site content is another avenue to consider. Many sites only react and remove content once something has been reported, rather than monitoring the issues and preventing the issues at the outset. If publishers have to check the legitimacy of advertisements on their sites it would significantly reduce one avenue scammers use to recruit victims. Not being able to promote on popular news and social media websites helps remove a veneer of legitimacy that associating with these sites provides.

Genuine websites need to provide clear warnings of scams relating to their business. This includes government websites such as the Australian Taxation Office and Centrelink. Commercial companies should also be encouraged to include scam warnings and information / tips in their standard computer packages.

WA Police recommend a national information portal (such as StaySmartOnline) also incorporate a reporting facility for online events and offending. However, experience from WA ScamNet shows that identification and prosecution of scammers is very difficult. There is a community perception that if a scam is reported it can be closed down. Due to the global nature of cyber-crime, this is not always the case. International networks need to act against scammers and there needs to be cooperation between countries in prosecuting scammers who reside in one country and scam in another. This needs to happen in a timely manner so that the extent of the scam is limited, instead of taking a long time going through various departments and stages of approval, both in Australia and internationally.

The Department for Communities recommends a free support helpline, where seniors can talk to real people about their issues. However, this should *not* be an IT call centre as technical experts may explain problems at an advanced level. Support needs to use language that novice senior users can understand.

It is useful to provide a list of secure Internet resources such as libraries and Wi-Fi hotspots that seniors can be confident about accessing a portal such as StaySmartOnline. According to WA Police, this measure can accompany a government certification standard / scheme for security systems and devices that are easier to use and are reliable. The scheme can also promote the use of escrow and insurance services, with a complementary endorsement system for trustable services of this nature. In addition, both the Department of Health and the Department of Finance suggest that Internet Service Providers provide more information on security on their websites including information on their security products (e.g. anti-spam) that comply with the government standard, and possibly offer discounts for seniors.

Communities also suggests that there may be scope to develop technology for seniors that is similar to 'net nannies' for young people. This may limit potentially harmful content, and thus reduce exposure to scams.

The Office of the Public Advocate believes that from a legal perspective, there may be a need to examine how misrepresentation on the Internet is covered by identity fraud.

Recommendations

In summary, the following measures may be most effective in increasing cybersafety and participation of senior Australians in the online environment:

- Enhancements to the StaySmartOnline website to improve accessibility and user-friendliness , via graphical step-by-step instructions and introducing the ability to report offences
- More promotion / education of advantages and disadvantages related to technology
- Targeted training for seniors that also emphasises the benefits of the Internet, as well as the risks
- A dedicated free support helpline
- Financial assistance to ameliorate training, hardware, software and support costs