SUBMISSION NO. 20

AFP
AUSTRALIAN FEDERAL POLICE

Australian Federal Police

Submission to the Inquiry into Cybersafety for Senior Australians

2012

Introduction

The internet and new and evolving technologies open up a world of exciting possibilities and benefits for all Australians. While the internet and mobile technologies provide many benefits, they also pose many risks.

Seniors citizens are accessible, they represent the fastest growing demographic in our ageing population and they hold a large portion of Australia's wealth. Therefore, they are an attractive potential target for, and may fall victim to, an array of scams and frauds.

It is crucial that senior members of our community are equipped with the necessary knowledge and skills to use information and communications technologies (ICT) and have the necessary information to make informed decisions online and to become good digital citizens. It is clear that understanding how to navigate the cyber environment safely is an important element in the development of digital literacy.

Online risks that may affect seniors include stalking, exposure to inappropriate content, identity theft, financial fraud, breaches of privacy and online scams.

The AFP believes that 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.

The AFP's High Tech Crime Operations (HTCO) portfolio aims to build a highly technical investigative capability for the AFP by anticipating and identifying emerging technology challenges for law enforcement and to develop response strategies for these challenges through engaging with domestic and foreign law enforcement agencies, government, industry, academia and the public.

Due to the exponential growth in cybercrime in general the AFP is continuing to work closely with their state and territory counterparts and international law enforcement agencies to combat this crime type. The AFP also relies on the relationships built through the International Liaison Officer Network with members deployed to across the globe.

Technology reliance, combined with the reach and speed of the internet, allows criminal elements to operate from international regions with limited regulation or legislation. In this environment, the sharing of information internationally between industry, private sector, government and third-party organisations in an open and timely manner enables law enforcement to protect the community and develop safe strategies against technology enabled crimes.

The AFP has fostered working relationships with a number of industry partners to overcome some of the technological challenges that currently face law enforcement in this area. We also work very closely with Australian government agencies in relation to policy development and legislative reform to address the numerous challenges emerging in this environment.

With the roll out of the National Broadband Network (NBN) more people will have access to the internet and this will include seniors. There is great possibility that this demographic will not be technically savvy, may not have received any online safety training and may not be as comfortable in the online environment as other members of Australia's society. In short, they are more likely to be at risk of online crime.

The AFP with other Australian Government agencies is working to minimise the criminal exploitation of the NBN. The inherent risk of the NBN is that it could facilitate the continual growth and sophistication of online criminal syndicates' ability to commit cyber offences against online systems due to the attractiveness of the increased speed. Increased bandwidth available via the NBN may result in increased bandwidth available for committing or facilitating computer offences.

1. the nature, prevalence and level of cyber-safety risks and threats experienced by senior Australians

The AFP has a role in protecting seniors in the online environment. There has been and will continue to be an exponential growth in cybercrime and with this growth will come an increased risk and threat to senior Australians who use the internet.

Cold calling investment fraud scams (boiler room fraud) will continue to target Australians. On-line scams, phishing and pharming continue to be of significant threat. These are only the reported scams and it is difficult to say how widespread these scams are and what the actual losses to elderly Australians are.

Identity Theft

Identity theft associated with the compromise of personal information in the online environment is a current and ongoing threat. Risks of compromising identity are the same across all age ranges. The use of a computer by one person who inadvertently downloads malicious software onto the computer will have an impact on every other user of that computer. Malicious software downloaded onto a computer can now also be used to remotely access files, webcam or microphone on the compromised computer.

There should be an onus on online users to protect their personal information.

Data compromised in the online environment may include personal financial information, other personal information such as emails, identity data and photographs. Senior's details may be used to give legitimacy to communications designed to compromise the individual's computers or obtain personal and financial details.

Superannuation Fraud

From an Identity Crime perspective, the growing risk relates to Superannuation Fraud. Whilst the AFP Identity Security Strike Teams have not investigated this to date, it is a significant risk for elderly Australians and those nearing retirement age. Cold calling investment fraud scams (boiler room fraud) will continue to target Australians with a view towards having persons transfer retirement money into fake investment schemes offshore where the money is then lost (stolen).

Superannuation Fraud is the latest earner for organised criminals who are targeting unsuspecting victims across Australia with victims remaining unaware for years that they have been duped.

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. Identity rules around self managed funds and hardship payments are weak. The bank accounts receiving the stolen funds are not checked against existing records and can be in multiple names.

Investment scams

Investment scams can come in many forms from an unexpected phone call offering an investment opportunity to an email encouraging purchase of shares that are about to go up based on 'secret' information. Other scams might offer early access to your superannuation, gambling software or promised large tax deductions or refunds.

Investment scams were once typically based offshore but are increasingly operating locally.

Fraudsters operate without Australian financial licenses and use false addresses and phone lines often routed to another address. They use sophisticated websites and target Australians who are approaching retirement looking for investment opportunities. An estimated 2400 Australians have lost more than $93 million in such schemes.

Online Dating and romance websites

Online dating and romance scams cause significant harm to Australian consumers, targeting people from all walks of life, education, background and age group. Between January and October 2011, more than 1600 complaints and over 17 million dollars in losses have been reported to the Australian Competition and Consumer Commission (ACCC).

These scams typically involve a genuine user of a dating website being contacted by an apparent admirer who is a scammer in disguise. Some have gone to great lengths to gain their victim’s trust over the course of several months in forming their relationship with the victim. The scammer plays on emotional triggers to get the victim to provide money, gifts or personal details.

A group of industry representatives has been working on draft guidelines to address this issue since July 2011. The ACCC would like dating agencies to provide clients with warnings about scams and verify online profiles to detect and disrupt the activities of those seeking to engage in fraud. This initiative is fully supported by the AFP.

Phishing scams (requests for information)

Phishing involves using a form of spam to fraudulently gain access to people’s internet banking details. The term 'phishing' refers to the use of spam emails purporting to be from a bank, in this way criminals 'fish' for legitimate bank customer's logon information.

Criminals send out millions of these fraudulent emails to random email addresses in the hope of luring unsuspecting innocent persons into providing their personal banking details.

Typically, a phishing email will ask an internet banking customer to follow a link to a fake banking website and enter his or her personal banking details.

Charity scams

These scams play on peoples’ generosity and involve a scammer posing as a genuine charity in order to fraudulently collect money.

Money transfer requests (Nigerian scams)

With the rise of internet banking it is easy to transfer money across the world in minutes. Unfortunately, this has also meant an increase in the number and types of scams that try to trick people into sending money to overseas scammers.

The scammers may promise huge rewards or what looks like an easy way to make money. Other scammers trick people who are trying to buy or sell products over the internet.

People should be very cautious about sending money to someone they don't know as once the money is sent, it can be very difficult to get it back especially if it was an overseas transaction. Seniors, like others may be vulnerable / susceptible to this type of scam.

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

The Government's Cyber-Safety initiative is part of a whole-of-government initiative involving the Department of Broadband, Communication and the Digital Economy (DBCDE), the Australian Communications and Media Authority (ACMA), the Commonwealth Director of Public Prosecutions and the AFP. The Cyber-Safety initiative is a continuation of the former Government's 'Protecting Australian Families Online' initiative implemented in 2007-2008. Funding for the Cyber-Safety initiative is $49 million over four years (2009-2012).

The messages regarding cyber safety are not new; numerous awareness campaigns are in their second or third iterations. We should question whether awareness is reaching across the entire community through all socio economic and culturally and linguistically diverse aspects and age groups and therefore reaching the most vulnerable.

Cyber-safety prevention and awareness raising campaigns need to be underpinned by sound research and longitudinal research however such research can take years. That is one of the challenges associated with requiring an evidence based approach to cyber-safety that the AFP would like addressed.

The AFP has a commitment to preventing online crime and education is an important part of that commitment. Australians need to take some responsibility for their online experiences, as they do in the offline environment. This should ensure they are better equipped and empowered to enjoy their cyber experience. Cyber-safety requires a multi-faceted approach; law enforcement; policy and legislation; education and some level of user vigilance.

The AFP's HTCO portfolio has been innovative in Australian policing by establishing a Crime Prevention Team dedicated specifically to address cyber safety and security. The aim of the Team is to implement crime prevention strategies which seek to raise awareness and empower all Australians to protect themselves online.

Senior Australians who are computer users are at increasingly greater risk online so the AFP has partnered with the Australian Senior Computer Club Association (ASCCA) to deliver sessions to senior users on how they can protect their personal and financial information, secure online banking and securing their wireless connections.

The AFP provided the Australian Seniors Computer Clubs Association (ASCCA) with a key message for their Open Forum during National Cyber Security Awareness Week 2011: *Awareness is the best weapon for online security.*

The ASCCA is pro technology for seniors and it runs computer clubs nationally to train seniors on how to use technology. Microsoft has had a strong partnership with them for years and at their annual 2 day conference in December 2011, Microsoft had a keynote speaking position following Senator Conroy.

The AFP participates on a yearly basis in National Cyber Security Awareness Week (NCSAW), and in 2010 was involved in over fifteen different awareness raising activities with a number of other stakeholders. This demonstrates the importance of working together to achieve a safe online experience for all.

During NCSAW in 2011 ThinkUKnow presentations were delivered to ASCAA. This was followed by a panel forum with guest speakers including Microsoft and Telstra. ThinkUKnow also manned a table at the ASCCA 2011 conference. ThinkUKnow is a cyber-safety program that is aimed at bridging the knowledge gap that exists between adults and young people when it comes to the internet and mobile technologies and to encourage a more open dialog between them. ThinkUKnow is a partnership between AFP, Microsoft and is proudly supported by ninemsn, and now Datacom.

The AFP promotes the following safeguards to ensure best practice protection online:

- Install security software and update it regularly
- Turn on automatic updates so that all your software receives the latest fixes
- Get a stronger password and change it at least twice a year
- Stop and think before you click on links or attachments
- Stop and think before you share any personal or financial information - about yourself, your friends or family
- Visit www.staysmartonline.gov.au for further advice and information.

Other cyber safety related safeguard messages promoted by the AFP include:

- Don’t believe everything you read – make sure you know its coming from a reliable source
- Don’t provide any private information about yourself, your family, friends or other people you know over the Internet
- Make sure your social networking profile is set to private
- Only accept friend requests from people you know – even if it is a friend of a friend it is not a good idea to add them as friends unless you know them personally
- Tell your friends to ask for your permission before uploading and/or tagging photo’s of you on social networking profiles
- If you ever see content online that is inappropriate or upsetting, tell someone you trust and contact your local ISP and law enforcement agency.

The AFP is looking at what works in raising awareness and what works in changing behaviour with a strategy to improve the information targeted at senior Australians.

4. best practice safeguards, and any possible changes to Australian law, policy or practice that will strengthen the cyber-safety of senior Australians.

The AFP also has a role in the prevention, mitigation and disruption of cyber crime through liaison with key partners and stakeholders, incident response and proactive investigative processes.

Specific AFP objectives are to enhance the AFP's contribution to combating technology crime impacting Australian families by:

- Increasing research into the evolving digital landscape and emerging threats to better predict trends and capabilities and develop proactive targeting, prevention and disruption strategies for online crimes.

- Promoting community awareness through active liaison with government and non-government organisations such as educational agencies and community groups.

Legislation

Since the early 1990's the Commonwealth has pursued a range of legislative and regulatory initiatives to enhance cyber-safety.

Commonwealth law enforcement have been given specific powers for the examination and seizure of computers under the *Crimes Act 1914* search warrant powers including the ability to move a computer off-site for examination, compel the provision of passwords and access data held at another premises via the on-site computer. In addition to more traditional investigative methods Commonwealth legislation enables cybercrime investigators to access telecommunication interception under the *Telecommunications (Interception and Access) Act 1979*, surveillance devices under the *Surveillance Devices Act 2004* and controlled operations incorporating undercover operatives under the *Crimes Act 1914*.

The Commonwealth legal and regulatory framework is under constant review. Law reform in this area presents a number of challenges due to the rapidly changing digital environment and the transnational and highly adaptable nature of online criminality.

Online crime is borderless and evidence can be transitory, highly volatile and located overseas. As a result a key legislative issue for law enforcement is an effective and efficient legal framework for the exchange of information and evidence with overseas agencies to underpin the strong working relationships the AFP has developed with overseas partners. The current scheme provided by the *Mutual Assistance in Criminal Matters Act 1987* (MACMA) can be cumbersome and is not suited to the online environment. Reforms to the MACMA in the Cybercrime Legislation Amendment Bill 2011 presently before Parliament will enable greater sharing of information between Australian and foreign law enforcement agencies.

In April 2011 the Attorney-General announced Australia's intention to accede to the Council of Europe Convention on Cybercrime. The convention provides benefits to law enforcement and contains procedures to make investigations more efficient and provides systems to facilitate international co-operation, including:

- helping authorities from one country to collect data in another country
- empowering authorities to request the disclosure of specific computer data
- allowing authorities to collect or record traffic data in real-time

- establishing a 24/7 network to provide immediate help to investigators
- facilitating extradition and the exchange of information.

However, the Convention is neither a simple or quick solution to a difficult problem to the issues of international evidence and criminal intelligence sharing. As the cyber criminal environment operates in a very fluid and rapidly changing environment more work needs to be done on ensuring that international law enforcement has the ability to quickly exchange evidence and intelligence in a timely fashion.

The AFP works closely with government departments, particularly the Attorney-General's Department to ensure the Commonwealth legal framework remains robust. The domestic legislative process can also be a lengthy process that struggles to remain current against emerging technologies. Accordingly, the application of existing legislation and the development of case law will remain critical.

The AFP has in the past run awareness sessions and presented to various members of the judiciary, including the Standing Committee of Attorneys General (SCAG), regarding current and emerging issues in the cyber environment.

The AFP has enhanced strategic alliances within the Australia and New Zealand Police Advisory Agency.

- The AFP is a member of the National Cyber Security Awareness Week (NCSAW) Steering Group. NCSAW (6 June – 11 June 2010) is an initiative led by DBCDE in partnership with other Australian Government Departments, state and territory governments and many leading business, industry and community organisations.

- The AFP participates in the Consultative Working Group (CWG) on Cyber-safety that provides advice to government on priorities for action. The CWG is made up of experts from industry, community organisations and government.

The ability to work closely with other law enforcement agencies, domestically and internationally, industry, academia and the community is critical to ensuring capabilities and capacity of police is enhanced. By sharing information and intelligence, expertise and specialist skills and by building solid training programs in support of law enforcement efforts, many challenges can be met.