Parliamentary Inquiry into Cyber Crime

Organisation: Australian Communications Consumer Action Network (ACCAN)
Date: Thursday 8 October, 2009
Location: Committee Room 814, Level 8, NSW Parliament House, Macquarie Street, Sydney
Time: 9:45am
Committee Members: Ms Belinda Neal (Australian Labor Party, Robertson), Mr Bruce Billson (Liberal Party, Dunkley) and Mr David Bradbury (Australian Labor Party, Lindsay)

Background

Though online security threats have recognisable names (malware, Phishing, Spam, adware), consumers aren't necessarily familiar with the technical complexity and constantly evolving nature of these threats. The situation is exacerbated by a cultivated culture of fear in which media hype, biased commercial information and questionable reach of government initiatives makes it difficult for consumers to be knowledgeable about the threats they may face online. As a result, consumers are not able to confidently guard themselves against these threats, instead becoming dependent on a range of prescribed solutions and ultimately leaving themselves vulnerable.

In light of today's Parliamentary Inquiry into Cyber Crime, ACCAN has built on research data collected for the 2006 CTN research project *Surfing on Thin Ice: Consumers and Malware, Adware, Spam and Phishing*, as attached in ACCAN's submission. The 2009 research involved a survey that aimed to investigate whether Australian consumers *really* understand online security threats and how to protect themselves against these. The questionnaire consisted of 27 multiple choice and extended response questions plus 2 additional questions on cybercrime, based on the original survey used in the 2006 research project *Surfing on Thin Ice*. The total sample size is 141 and was collected during the period of September 10 to September 28, 2009.

The results offer qualitative insights – a snapshot of consumer's experiences and opinions on areas of e-security that are constantly evolving. It is clear that much more on-going research across a range of consumer groups is needed. Further, industry, regulators and government also need to consult widely with consumers about e-security on an on-going basis.

Key Findings

ACCAN has highlighted the differences between the findings of the 2006 and 2009 surveys. 1 in 3 respondents of ACCAN's Online Security Survey 2009 were between the ages of 41 to 50 years old. Due to the small sample size, there were no respondents under the age of 18.

However, further research reveals that young people, aged 12 to 18, have a high level of awareness of cybersafety risks. The ACMA report, *Click and Connect- Young Australians' Use of Online Social Media* released in July 2009, reveals that 75 per cent of children surveyed claim they know the importance of not disclosing personal information online. They remember key safety messages such as 'people aren't always who they say they are online' and do not reveal their address or phone number online.

Chris Chapman, Chairman of the ACMA stated that 'Australian children demonstrate a good general knowledge of online behaviours that we might consider 'risky'—they know what not to do. Up to 78 per cent of parents also report having a 'high' level of knowledge of online risks'. The report emphasises an ongoing need for cybersafety material that resonates with young Australians, as well an improved flow of cybersafety information to parents.

ACCAN acknowledges the Department of Broadband, Communications and the Digital Economy's (DBCDE) implementation of the Government's E-Security intitiaves, including the enhancement and ongoing updating of the online security information website, *Stay Smart Online.* ACCAN also commends the Department for undertaking an E-security education package aimed at Australian school students, primarily between the ages of 3 and 9.

Further key findings of the ACCAN Online Security Survey 2009 include:

F1. An alarming rate of cybercrime

- 1 in 5 consumers surveyed had been victims of cybercrime. This indicates the extent of the problem is very high
- 1 in 3 consumers had experienced Personal Identity theft. Some consumer claims include: *"money [was] withdrawn from credit card account without authorisation"* and *"our credit card numbers were hacked."*
- 1 in 3 consumers experienced domain name renewal scams. One consumer stated that they were *"...approached by [a] rival provider implying that they were my current provider."*
- 4 out of 5 consumers had experienced spam scams (junk mail).
- 2 in 5 consumers had fallen victim to online auction and shopping scams.
- 1 in 10 consumers experienced modem jacking.
- 1 in 3 consumers experienced spyware and key-loggers.
- 3 out of 5 consumers had experienced 'Free' offers on the Internet but did not take up the offer.

F2. Consumer Perceptions

- More than 3 out of 5 consumers surveyed believed they had a solid understanding of the security risks they may face online.
- Results reveal that there is a much higher awareness of online security terminology amongst Australian consumers over the past 3 years. This could be due to heightened representation of online security risks in the media. Despite this increased knowledge of terms such as Worms, Trojan Horses, Phishing etc., consumers distrust their ability to sufficiently protect themselves online. Australians surveyed demand further educational tools about cyber protection, particularly in simple language for consumers with lower digital literacy levels.

F3. Searching for information on Online Security Issues

- 1 out of 5 consumers in 2006 and 2 out of 5 consumers in 2009 used government agencies as sources for information on online security. This positive increase reveals that consumers are actively responding to the promotion of government information materials. However, the survey revealed that very few consumers are using independent sources.
- More than 2 out of 5 consumers in 2006 and 2 out of 5 consumers in 2009 referred to media articles (online and print) as a source of information on online security concerns. This decrease reveals consumers placing less trust in media articles.
- More than 2 out of 5 consumers in 2006 and 3 out of 5 consumers in 2009 relied on friends and family as a source of information on security issues. This increase in a reliance on family and friends for information is concerning as the Government has allocated $73.6 million in funding towards providing information and enhancing the protection of home users.

F4. Changes in use and obtaining of Online Protection Software

- There has been a slight decrease of 4% in the past 3 years in regards to consumers using Anti-virus software and firewall software. However, there has been a 20% increase in the use of Internet and Email filters. This increase is in correlation with a higher percentage of consumers experiencing spam emails.
- Between 2006 and 2009, there has been a decrease of 5% in consumers paying for online security protection.
- There has been a decrease of 7% in consumers who are downloading free online security protection.

The Consumers Speak

Consumer Perceptions

"I think there are risks no matter what method use; you can't stop doing things just because there is a vague risk that 'something bad might happen to me'".

"I have read numerous articles that as a mac user we don't really have to worry..."

"I have not had personal problems but am affected by what I read and hear from others."

Fear of insufficient security:

"I am quite ignorant – what happens on my computer I do quite blindly, and trust that the anti-whatever software to catch what is bad. Sometimes it fails or expires and catches me out."

"I am fearful about doing any business on line, though I do risk paying for e.g. airfares with credit cards. I am very reliant on trusting the security system I have installed but suspect that it can only do part of the job. "

"I do not utilise the Internet as much as I should simply because I do not trust the system. More information as to how to protect my computer would be beneficial."

"Online security does not work very well at all despite all the claims, if you use windows for PC...It is clear that the hackers are ahead of the online security companies!"

"I refuse to do online banking for security reasons."

Education:

"The issues I have with end users is them not being educated and not using correct anti-virus and security software. Many people who purchase their first comp0uter rely on a salesperson who more than likely will try and sell them a package when free programs are readily available..."

"More education [for] consumers."

"Government to put out warnings in the newspaper or send info to households via snail mail etc to warn and educate vulnerable people about the damage virus[es] can do."

"A good source of info on products and especially compatibility issues is critical."

"When computer illiterate [consumers] are purchasing protection online, a clear and simple procedure for activating the program once paid for would be helpful."

Recommendations

Office of Online Security

In order to address the multitude of economic and social implications of online security issues, the Australian Government should develop an Office of Online Security. This Office will be housed in the Department of Broadband, Communications and the Digital Economy and have a similar model and significance to the current Office of Climate Change. Further developments required include:

- The Office of Online Security to report at Cabinet level on improvements, research and further challenges in cyber security.
- The Office to develop a National Strategy for E-Security Awareness as there is a lack of co-ordination between various bodies working on consumer awareness in E-security.
- It is not clear as to which demographics are being targeted in the field of consumer awareness and how, as well as whether all demographics in Australia are being covered sufficiently.
- A clearly articulated National Strategy on E-Security is necessary, focusing on raising awareness to all Australian consumers.
- The Office of Online Security should set benchmarks for basic pre-installed security features to be provided with the purchase of all computers.

The Australian Office of Online Security would follow suit of Cyber Security Offices implemented this year by both the UK Government and US Government.

Consumer Education

- Consumers should be encouraged to take more responsibility for their own e-security. ACCAN proposes the Office of Online Security develop an Online Competency Skills Test in Online Security. The test would be developed for consumers to highlight whether they are aware of online security threats and how to protect themselves.
- The Online Competency Skills Test would give consumers an understanding of their level of protection and also encourage those who scored poorly to actively seek out information to further educate themselves.
- Up-to-date lists of confirmed e-security threats, especially phishing scams, for consumers to refer to.
- Digital Communication - E-security education should be presented through television advertisements. Targeting consumers via television is crucial as many older Australians will not view education campaigns online due to a distrust of Internet safety and computer illiteracy. This would involve using animated demonstrations, real-life examples and plain language to explain how e-security threats work, how to identify them, and how to best deal with them.
- Using animated demonstrations, real-life examples and plain language, explanations of how e-security products and other e-security measures work, especially in the context of online transactions.
- Addressing the challenges consumers face in maintaining security measures across multiple computers, including work computers.
- Education resources should be widely promoted across all sectors of society, especially to young people, seniors and new computer users.

Role for Consumers and Community Organisations

- Regular consumer consultation is necessary for effective E-security Awareness campaigns. For example, in reaching seniors, the Office of Online Security could liaise with the Australian Seniors Computer Clubs Association (ASCCA).

Vendors' Responsibility

- Vendors (computer Hardware and Software manufacturers) need to take more responsibility by implementing safer protocols to ensure all equipment is not open and vulnerable to security threats.
- It is necessary for basic online protection software to be pre-installed in all computers available for purchase. This initiative by vendors will prevent security threats at the source, rather than relying heavily on consumer skills which are not always sufficient.

International Engagement

- As Internet security issues have a global effect, the Office of Online Security should promote ideas and share information at OECD and International forums.

ACCAN Initiatives

- ACCAN needs to work with Consumers International in the field of cyber-security to develop initiatives and research focusing on consumer protection.
- ACCAN should consider joining the steering committee for E-security Awareness Week to play a more active role in consumer awareness. ACCAN should also apply for a grant when they become available, to run activities during E-security Awareness Week.