Australian Communications Consumer Action Network

Suite 4.02, 55 Mountain St
ULTIMO NSW 2007
Ph: 02 9288 4000
Fax: 02 9288 4019
Email: info@accan.org.au
www.accan.org.au

John Hilvert
Communications Director,
Internet Industry Association
PO Box 3986 Manuka,
ACT, 2603
By email: securitycode@iia.net.au

10 November 2009

Dear Mr. Hilvert,

ACCAN would like to thank the Internet Industry Association for the opportunity to respond to the call for public comments on the *Draft E-Security Code.*

About ACCAN

The Australian Communications Consumer Action Network (ACCAN) is Australia's new communications consumer watchdog. The purpose of ACCAN is to improve consumer advocacy, undertake research and analysis from a consumer perspective and to make the market work for communications consumers. The operations of ACCAN are made possible by funding provided by the Australian government.

Introductory Comments

ACCAN commends the Internet Industry Association (IIA) for developing an E-Security code which aims to empower consumers by raising “awareness and educating [consumers] about e-Security risks.” ACCAN understands that there is an urgent need for an E-Security Code in Australia; however we support a mandatory code over the current voluntary code.

ACCAN’s recent research has highlighted astronomical incidences of cybercrime among Australians. In addition, Industry has proven continuously that it will not regulate itself satisfactorily and while a Trustmark is a positive incentive, it does not sufficiently encourage ISPs to engage in self-monitoring.

ACCAN believes that the E-Security Code must be enforceable in order to ensure optimum protection for consumers. Enforcement of the Code by the Australian Competition and Consumer Commission (ACCC) can be made possible by the registration of the code under section 51 of the Trade Practices Act (1974).

ACCAN has also noted that the Draft E-Security Code is focused too strongly on actions the consumer should take in protecting themselves, as opposed to the many actions that ISPs should undertake. Whilst it is very important to take all measures to empower consumers, the IIA must recognise that consumers will always be less informed than ISPs about online threat protection and ISPs have the skills required to protect consumers.

Education

As addressed in Schedule 1 of the Code, education is vital for consumers to minimise online security threats. While the protection measures suggested will provide useful information for consumers, the method of promoting such material is not mentioned in the Code. ACCAN recently conducted research into consumer awareness of E-Security issues which revealed that there is a much higher awareness of online security terminology amongst Australian consumers over the past 3 years. Despite this increased knowledge of terms such as Worms, Trojan Horses, Phishing etc., consumers distrust their ability to sufficiently protect themselves online. Australians surveyed demanded further educational tools about cyber protection, particularly in simple language for consumers with lower digital literacy levels. Many consumers also indicated they prefer not to read extensive information.

ACCAN recommends that the online protection information suggested in Schedule 1 of the Code is presented interactively through an online video on the ISP's website. To make sure all consumers are aware of such a useful resource, ISPs should also provide the information in an Auslan (Australian Sign Language) and captioned online video. The IIA may be able to produce a standardised message in multiple formats as well as video and text. This is a relatively cheap and effective method of information distribution.

ACCAN Recommendations

1. *Schedule 1 – Standardised Information for Customers* to be changed to highlight that the mandatory information is presented in basic text and online video (including Auslan and multiple languages) format to be hosted on ISPs' websites.

2. ISPs provide an online video which includes a set of exercises that educates consumers in detail about updating their software.

ISP Responsibility

ACCAN research has also shown that alarmingly, 1 in 5 consumers had been victims of cybercrime. Of these Australians, 1 in 3 had experienced spyware and key-loggers. ACCAN firmly believes that vendors and ISPs must take more responsibility

by implementing safer protocols to ensure all sold computer equipment is not open and vulnerable to security threats. To protect Australians, 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.

ACCAN suggests ISPs and vendors work in union to inform customers that their computer ports may be open and therefore easy targets to online threats. ISPs should inform the consumer of methods to both check and protect their ports. This information must be in an easy to understand manner, so as not to overwhelm the consumer.

ACCAN Recommendations

1. ISPs and Vendors should establish a coalition working towards informing customers about the various ways their computer may be currently at risk.
2. Vendors should ensure online protection software is pre-installed in all computers available for purchase.
3. E-Security Code to include a clause stating that at point-of-sale, ISPs must inform customers that their computer ports may be vulnerable and must then explain the appropriate measures for protection.

Affordability

ACCAN acknowledges that the IIA has recognised the cost involved for consumers when engaging in online protection. ACCAN notes that the Draft E-Security Code entails a provision whereby consumers are encouraged to utilise free-ware (free protection software such as anti-virus and anti-spyware programs) as protection. Consumer awareness of free software availability is crucial however, many Australians are not aware of the free-ware available. Therefore, these awareness raising strategies must be easily accessible and easy to comprehend.

ACCAN Recommendation

1. The E-Security Code to include a provision where ISPs promote the availability of free-ware to customers using online videos on the ISPs' websites, DVDs, other hardcopy manuals and by email.

Consumer Consent

Section 6.2 outlines steps that ISPs must take once a compromised computer has been detected. ACCAN believes that in the instance of temporary suspension of a consumer's account, the consumer's consent is fundamental. Consumers rely on VoIP and other Internet services for everyday use. In some instances, the reliance on such services is a basic necessity and includes access to emergency services. Disconnecting an Internet service without consent would prove detrimental to these consumers and should be avoided.

Additionally, ACCAN is concerned about the wording in the title of Section 6.2: "Actions to be taken once a *compromised customer* is detected". Here "compromised customer" should be changed to "customer's compromised computer".

ACCAN Recommendations

1. Development of a guide to consent for ISPs, built around the consistent definition published by the Australian Communications and Media Authority (ACMA).
2. Inclusion of a definition of 'consent' in the *E-Security Code.*
3. The Code ensures customer consent is to be recorded either over the phone or by email before an ISP suspends their compromised account.
4. In the title of 6.2, "compromised customer" to be changed to "customer's compromised computer".

Trustmark

ACCAN congratulates the IIA in introducing a Trustmark so that ISPs may be certified if they comply with the Code. This incentive could provide some level of standards of online protection on which consumers may base their purchasing decisions. Therefore, it is crucial that the Trustmark has credibility. To ensure such legitimacy, the Code must clearly outline the compliance criteria and Code monitoring processes. Prior to an ISP acquiring the Trustmark, they must commit to this compliance and monitoring framework.

An example of the danger of losing credibility is the Heart Foundation's Tick which was developed to help identify with healthy food products. The Tick was initially considered credible but soon was the subject of scrutiny after it appeared on McDonalds' products. To ensure complete credibility of the Trustmark, a benchmark or specific methods of attainment must be set out in the E-Security Code.

ACCAN Recommendation

1. Code to include a clear outline of criteria that must be met in order for an ISP to attain a Trustmark.

2. ISP compliance with Trustmark criteria to be avidly monitored by the IIA.

Code Enforceability

Ultimately, ACCAN urges the IIA to take appropriate measures that will allow the E-Security code to be mandatory and enforceable by the ACCC. Such enforcement is critical as the draft E-Security Code does not guarantee optimum protection for consumers in its current provisions. ACCAN understands that due to the Code becoming mandatory, implementation may be delayed.

ACCAN Recommendation

1. The E-Security Code to be registered and an applicable (mandatory) under section 51AE of the Trade Practices Act (1974).

2. Contravention of the code by an ISP to become enforceable by the Australian Communications Competition and Consumer Commission (ACCC).

3. An implementation period of no longer than 6 months, beginning in 2010.

Should you require more information, please contact Kirisha Thanapalasuntheram (Policy Assistant) on (02) 9288 4000.

Yours sincerely,

Allan Asher
Chief Executive Officer

Australian Communications Consumer Action Network

accan