Internet Society of Australia
A Chapter of the Internet Society
ABN 36 076 406 801

C/- Maddocks, Level 7, 140 William Street
Melbourne, Victoria 3000
Accounts: P.O. Box 351, Glenorie NSW Australia 2157

To: Internet Industry Association

By email: securitycode@iia.net.au

Monday, 2 November 2009

DRAFT IIA E-SECURITY CODE

The Internet Society of Australia (ISOC-AU) welcomes this opportunity to comment on the Internet Industry Association's draft e-security code.

ISOC-AU's fundamental belief is that the Internet is for everyone. We provide broad-based representation of the Australian Internet community both nationally and internationally from a user perspective and a sound technical base. We also consistently promote the availability of access to the Internet for all Australians.

Security of the Internet is critical for Internet users. Without user confidence in the security of the Internet, user participation in the digital economy will not progress. The security issue was highlighted by the OECD as background for its 2008 meeting on the Internet Economy:

> These risks are manifold. They threaten personal security—that is to say, they may undermine the individual's ability to control the information that they have entered into or stored on connective devices such as PCs, mobile telephones, or databases operated by commercial organisations, government agencies and others. Victims typically suffer financial loss through fraud, though in cases of identity theft they may also suffer loss of reputation, or, in extreme cases, may be accused of crimes they did not commit.
>
> Online risks may also impact upon personal safety—by which we mean they may lead to direct physical or psychological harm to the individual. One high-profile threat is that posed to children by predatory paedophiles, who conceal their true identity whilst using the Internet to "groom" potential victims. Probably far more common is the online bullying of children by their peers, while even adults who injudiciously disclose personal information.[1]

Our response to this draft Code is as follows:

1 OECD, Malicious Software (Malware): A Security Threat to the Internet Economy (OECD Ministerial Background Report DSTI/ICCP/ REG(2007)5/FINAL, p. 8

1. INTRODUCTORY SECTIONS

The first four sections of the Code (Preamble, Objectives, Scope and Principles) are lengthy and, in some cases, not strictly relevant to this Code. For example:

- Clause 1.6 sets out the intention of Parliament for Codes generally. While this is generally true of industry Codes, it is not necessarily of particular relevance to this Code.
- In some cases, the Code objectives reword Code aims already suggested in the preamble.
- Again, in the Principles section, it is not clear what many of the 'principles' add for this particular code that have not already been stated elsewhere.

2. CODE RULES

2.1. *Introductory Statement*

While it is recognised that the Code is voluntary, The Code does suggest that, if an ISP does comply with Code provisions, that ISP can then use a 'trustmark'. Therefore, the language of the first sentence in section 6 should be more strongly worded. Specifically, if should read:

… several activities that ISPs SHOULD undertake with the end goal of improving Internet security. ISPs SHOULD take at least one of the items….

2.2. *Section 6.1: Detection…*

After the first sentence, insert the final sentence, changed to read:
ISPs SHOULD undertake one….

2.3. *Section 6.2: Actions*

The third sentence should be changed to read:
Examples of actions that ISPs SHOULD take…

The section should also suggest ISPs should tell consumers steps they can take to clean their potentially compromised computer. This might be a reference to a website on what steps they can take and/or reference to where they can access advice.

The question left by this section is what follow-up action ISPs should take once a potential compromised computer is identified. Even if the customer is informed and does follow advice from the ISP on steps that they should take to clean their computer, there may need to be follow-up monitoring to ensure that any action taken by the customer has adequately addressed the problem.

One suggestion is to refer to an IETF document, IETF, *Remediation of Bots in ISP Networks* September 2009 http://www.ietf.org/id/draft-oreirdan-mody-bot-remediation-03.txt on further steps an ISP might take.

2.4 Section 6.3 Educating Customers.

Part of this section is more correctly placed in section 6.2 – telling customers that their computer is compromised, and telling them of steps they should take to clean their computer. This section should be on general education of customers and how they should protect themselves against allowing their computer to become compromised. And the message should be a consistent one by all ISPs. We suggest that customers are referred to the DBCDE website, Stay Smart Online site, http://www.staysmartonline.gov.au for consistency of message. Indeed, the IIA website should provide a link to that website to ensure all customers are given a consistent message.

2.4. *Trustmark*

Having a trust mark for compliant ISPs will encourage compliance with the Code. However, this section does not include steps an ISP should take to demonstrate their compliance before they are allowed to use the mark. There are also no steps that the IIA might take if an ISP is found not to comply with the Code. If the trustmark is to have any credibility with the public and regulators, there should be steps that both ISPs and the IIA should take to ensure its ongoing credibility.

3. Schedule One

This Schedule provides standard information for customers. As stated above, it is important that customers receive a consistent message on steps they should follow to protect their Internet security. To ensure consistency of message, the wording should be the same as is provided by the Stay Safe Online website, with a link to that site for further information.

We will be happy to provide any further comments on issues raised by this submission

Tony Hill
President
Internet Society of Australia
President@isoc-au.org.au

Holly Raiche
Executive Director
Internet Society of Australia
ed@isoc-au.org.au