# The ACMA plays a leading role in E-Security Code of Practice

## The ACMA is working with industry to develop a voluntary E-Security Code of Practice. This was launched recently during National E-Security Awareness Week.

The Internet Industry Association (IIA) will develop the code with input from the ACMA and the Department of Broadband, Communications and the Digital Economy. Its focus will be protocols for internet service providers (ISPs) when responding to reports or information about compromised computers on their networks.

A computer can become 'compromised' when malicious software (malware) is installed without the computer owner's knowledge. This malware enables the computer to be controlled remotely for illegal and harmful activities, including:

> disseminating spam
> hosting 'phishing' sites
> making distributed denial of service attacks on internet infrastructure.

The ACMA provides daily reports of such compromises to participating ISPs through the Australian Internet Security Initiative (AISI). The AISI collects data on compromised computers residing on Australian networks from a number of sources, and provides daily notifications to ISPs of compromises reported in the previous 24-hour period. The reports contain information on:

> the type of compromise
> the internet address of the computer that was compromised
> the time it occurred.

For many ISPs, the AISI is their main source of such data.The ACMA cannot identify a customer associated with a compromise; only ISPs can. They do so by correlating the internet address and the timestamp information contained in the AISI report. Once an ISP determines the customer associated with the internet address in the AISI report, it can then alert the customer and give them advice about fixing the problem.

The E-Security Code of Practice will provide guidelines for ISPs to deliver consistent messages to their customers when they receive AISI compromise reports from ACMA, and consistent approaches to customers who do not take remedial action when they are notified of a compromise.

The E-Security Code of Practice will provide guidelines for ISPs to deliver consistent messages to their customers when they receive AISI compromise reports from ACMA, and consistent approaches to customers who do not take remedial action when they are notified of a compromise.

The IIA hosted an industry forum during National E-Security Awareness Week as an opportunity for industry to directly contribute to development of the code. It was attended by around 50 internet industry representatives. Launching the event, Senator the Hon. Stephen Conroy thanked attendees for their continued participation in improving national e-security, and noted that 'ISPs sit at the gateway to the internet and are often a trusted point of contact for consumers when it comes to getting the most out of their time online'.

Bruce Matthews, Manager of the ACMA's e-Security and Do Not Call Register Section, gave an overview of the AISI. Mr Matthews reported there were currently 68 ISPs participating in the AISI, which is now reporting an average of 10,000 compromises per day. He noted that the ACMA acknowledges the importance of ISPs offering support and advice to customers regarding compromises, citing a recent ACMA survey of ISPs participating in the AISI in which ISPs reported their customers as generally being grateful when notified their computer had been compromised, and taking steps to remedy the problem.

Mr Matthews went on to say that the large number of daily AISI reports doesn't necessarily mean the rate of computer infection rates in Australia is getting worse: the ACMA is continually increasing the number of sources of compromise data feeding into the AISI, and the number of participating ISPs has also been steadily increasing, leading to more IP address ranges being reported on. However, the data does indicate that computer infection is a significant problem, consistent with international experience.

The integrity of AISI reports was strongly supported by all ISPs in attendance at the workshop, with one representative stating that they were a 'very reliable' source of information.

The IIA hopes to finalise the code by December 2009.

The ACMA welcomes ISPs wishing to participate in the AISI. More information on the AISI can be found on the ACMA website **www.acma.gov.au** (go to For the public: Consumer & community advice: Spam & e-Security > Protecting yourself online > Australian Internet Security Initiative).

More information on the IIA can be found on its website **www.iia.net.au**.