Spam code registered

A world-first code of practice on countering spam for internet and email service providers, developed by industry to support the *Spam Act 2003*, was registered by ACMA in March 2006.

Registration of the *Internet Industry Spam Code of Practice* shows Australia is again leading the world in the global fight against spam, which requires joint action by industry, regulators and end-users.

Industry codes represent one element of Australia's multilayered strategy against spam, which includes legislation, technical counter-measures, education and awareness initiatives and international cooperation.

Under the code, internet and email service providers must provide spam-filtering options to their subscribers. They must also give end-users information about how to deal with spam and have a process for handling complaints from subscribers.

The code also sets out how internet and email service providers will address the sources of spam within their own networks, including actual spammers, misconfigured customer email servers and the virus-infected computers used to spread spam (known as 'zombies').

Suggested technical best practices for hardening the network against spam and related threats such as zombies are also included in the code. These are consistent with the technical best practices being promoted by global internet and email service provider associations.

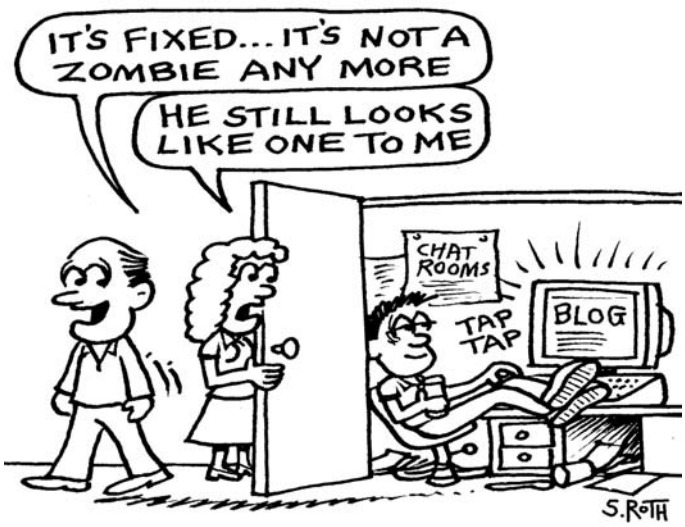
The Australian internet industry is already actively combating spam. For example, three-quarters of all internet service providers in Australia already voluntarily offer a spam-filtering product to their customers as either a free or charged service (Australian Bureau of Statistics figures).

The code applies to all 689 active internet service providers in Australia, as well as global email service providers in Australia, such as Hotmail and Yahoo.

Registration of the code allows ACMA to direct individual internet and email service providers to comply with the code if necessary. The code obligations will come into force on 16 July 2006.

The code was developed by an Internet Industry Association (IIA) Task Force, which included representatives from the Western Australian and South Australian internet service provider associations, and was chaired by Mr Jeremy Malcolm of the Western Australian Internet Association. The IIA committee consulted on a draft of the code with consumer and business representatives, including calling for public comment.

The code is on the ACMA website at www.spam.acma.gov.au.



Summary of code provisions

The code requires internet service providers and email service providers:

- to provide spam filtering options to their subscribers
- to tell subscribers what default filtering of the subscriber's email the internet or email service provider does at its own servers
- to advise subscribers how to deal with and report spam
- to ensure their acceptable use policies prohibit the use of their networks for spamming; and to inform subscribers to that effect and
- to comply with all lawful requests of law enforcement and regulatory agencies investigating spam activity.

The code requires internet service providers:

- not to have open relay or open proxy servers, and to impose the same obligations on their subscribers through their acceptable use policies
- to retain the right in their acceptable use policies to scan their own networks for subscribers' misconfigured mail and proxy servers
- to ensure their acceptable use policies allow for the immediate termination of connections they host where the connection has become an open relay or open server (a zombie), either due to intentional misconfiguration or to unintentional infection by a virus or other intrusion
- if notified that a subscriber's account is spamming (for example, where the subscriber's computer is a zombie), to take reasonable steps to warn the subscriber and offer suggestions on how to correct the problem—the internet service provider may immediately terminate the connection if the problem is serious or continuing and
- if the internet service provider is using dynamic IP address allocation, to use all reasonable efforts to retain records of subscriber allocation for at least seven days.

SUMMARY OF BEST PRACTICE TECHNICAL MEASURES

An internet service provider or email service provider

- should publish sender policy framework (SPF) records for each domain administered by it and
- shall comply with all Asia Pacific Network Information Centre requirements for keeping WHOIS (domain names and IP addresses) data updated, including ensuring that their own internet service provider customers do the same.

IN ADDITION, AN INTERNET SERVICE PROVIDER SHOULD:

- impose reasonable limits on the rate subscribers can send email
- allow subscribers to authenticate to their mail servers using SMTP AUTH (see below) or an equivalent
- not distribute customer premises equipment that is configured by default so as to allow remote administration across the internet
- prevent automated registration of email accounts
- provide reverse domain name system entries for any server on an internet service provider's network being used to send email, including those of the internet service provider's subscribers and
- where technically and commercially viable, not permit computers at dynamically allocated internet protocol addresses to connect directly via internet port 25, which is generally used for SMTP.

Note: SMTP-AUTH extends SMTP (simple mail transfer protocol—a protocol for sending email messages between servers) to include an authentication step through which the client effectively logs in to the mail server during the process of sending mail.