Lovely Spaaam! Wonderful Spaaam!**

Ivan Trundle

Manager, communications and publishing
ivan.trundle@alia.org.au

It had to happen. Last month in *inCite*, I promised that the following month's article would discuss ways of preventing e-mail abuse — how to fight spam and how to manage your e-mail account. Shortly after publication, two things happened: firstly, following a glitch in a few user's e-mail addresses, I received 36 000 e-mails that rapidly filled my mailbox and rendered it useless; and secondly, a spate of spam attacks affected a number of users at the alia.org.au domain. In the light of these two experiences, I was sorely tempted to switch the theme of this month's column and instead discuss ways of avoiding becoming preposterously wealthy. Or how to prevent radiant good health. Yet the two unpleasant incidents I experienced last week highlight the difficulties that people face in day-to-day communication via e-mail.

Sorting the good from the bad

What exactly is spam? Loosely defined as junk e-mail, it is widely-distributed and unsolicited e-mail sent to multiple addresses. It is universally loathed by the online community, generally because of the waste of time, resources, and money in dealing with them. Fighting spam is a little like having to stare down a bully in the playground. Ultimately, the best defence is to studiously ignore anything that remotely resembles spam, and to avoid being provoked into responding to the source of the message.

Indeed, the parallel can go one step further. There are various channels of reporting that circumvent the message sender (akin to going to the teacher). But this is one step ahead. Better to work out how to avoid spam first, then how to deal with what does eventually get through.

1. Make it hard for people to find and use your e-mail address. Avoid having it listed on web-sites, or at the very least, avoid having it displayed in static pages (those that are not drawn from a database upon a query). Of course, this has its impracticalities, not unlike having your phone number unlisted. Alternatively, if you need to have your e-mail address listed, make it 'slightly' fake, such as "ivan.trundle# alia.org.au" and provide a qualifying note beside the reference to alter the '#' to a '@' — or whichever character you prefer. This, too, has its drawback, but since many web-bots (robots that trawl the web for addresses and other useful data) look for the '@' symbol, you can effectively cut them out of the information-gathering loop early.

2. Your e-mail details are invariably added to your internet configuration files and settings within your mail client or elsewhere. In these settings you will find a 'Reply-To:' address field. In many cases it can be left blank, or with a coded address that people can understand but robots cannot: ivan.trundle@'no-spam'alia.org.au is a good example — so long as I tell people to remove the string, 'no-spam'. Anonymous remailers are another option here. Anonymous remailers are mail servers located on the internet that take your e-mail and forward it anonymously to your intended recipient, thus obliterating your own address in the process (unless you choose to add it to your message). Anonymous remailers are reliable and trustworthy, but in some instances are considered offensive by the recipients of messages emanating from such services. [http://www.cs.berkeley.edu/~raph/remailer-list.html is an automatically-generated list of such remailers — search engines will give you more information on how to use them]

3. If you still get too much spam, it may be time to fight back. However, this does not mean communicating with the spam mailer — which will only confirm your address and allow it to be used by others for spam (never believe those that offer to remove you from their mailing list unless you deliberately subscribed to the list in the first place). But to do this, you need to know what you are up against.

By looking in the 'header' information that comes with every e-mail message, you should be able to work out where the message came from, which may differ from the 'Reply-To:' field. Check the domain component (refer to last month's column) and jot this down. Then, send a note to either or both of the following: postmaster@xxxxx.xxx.xx (substituting the domain address for the string of xxx's) or abuse@xxxx.xxx.xx (again, switch the x's for the domain name), outlining the message that you received and preferably by forwarding the message complete. All domains must have a postmaster to be registered, and a message to this source will always get through to a human, eventually. Invariably, if the spammer is using an ISP or has generated an e-mail account through Hotmail or Yahoo (as examples), then the terms and conditions of use of such a service will most likely mean that this user will have his or her account cancelled forthwith.

Filtering as an option

With the more sophisticated e-mail clients that exist today, it is also possible to filter out unwanted messages (and even the wanted ones if you are not careful) by setting up rules that are automatically and slavishly followed by your e-mail client software to either delete or move unwanted messages. Once you define which are the component parts of the incoming e-mail that you want to be tripped up by your filtering system, you can then decide which mail you finally get to read. I use and recommend this kind of approach all of the time — if set up correctly, it can organise your incoming e-mail so effectively that you will wonder how you managed without such a mailbot! ■

** *Monty Python fans will know of the Spam song. The rest will stay bemused...*