

"The War Against SPAM" By Stuart Cliffe

Reprinted with permission; first appeared in www.freepint.com newsletter

Virtually everyone with an email address seems to suffer from unsolicited emails for commercial, personal or pornographic services. There are various names for this sort of email.

Probably the oldest (with apologies to a well-known luncheon meat) is 'SPAM'. Spam seems much more intrusive than junk mail delivered by post. Perhaps because the information is delivered direct to your computer and can be read by anyone, or because much of the content would probably be illegal if sent by post. The language and pictures used can be very worrying for parents of young children. The usual queries about spam include - Why Spam? How did they get my email address? and What can I do about it?

Why Spam?

Spam is a highly cost effective way to generate income. Sending the same information by post would be extremely costly - and in some cases illegal. Dealing with replies would be expensive in terms of an enquiry telephone line, reply-paid envelopes, and generally coping with the results of the mailing. Also the person operating the scheme would be highly visible, traceable through telephone and office rental records, and subject to possible legal attack in the country concerned. On the other hand, sending information by email is very cheap - a telephone connection allows tens or hundreds of thousands of emails to be sent anonymously more or less at the stroke of a key, and for the cost of a local phone call. The contents can be anything - spammers send from email addresses set up especially for that mailing, with replies to different email addresses or to websites with disguised addresses. No matter how unlikely the offer, for every 100,000 emails sent, there are bound to be a certain number of replies - and even if these are requests to 'unsubscribe', the spammer is happy. These are confirmed live email addresses that can be sold on to others, and used for future mailings.

There are all sorts of reasons for spam - some viruses generate their own little spam shower in the course of transmitting the infection to others; emails may be deliberately offensive to panic people into using the 'unsubscribe' option - and confirm that their address is valid; various frauds try to part you from your money; porn sites try to tempt new members to subscribe; hackers send 'trojans' to get control of computers, or persuade the unwary to visit websites that can install unfriendly software on your machine. All of the above should suggest that if you receive an unwanted, unexpected or just plain suspicious email, the best response is NOT to reply to it, open it or do anything other than delete it - or report it to the system it came from.

How did they get my email address?

If you ever gave your email address to apply for a username and password for a website; signed a guest book; sent a newsgroup message; emailed a query; or (the worst case) sent an 'unsubscribe' request, your email address became public property. Even if you have not done any of these things, your address may be churned out by a random address generator. Don't be confused if you receive an email apparently addressed to someone else, or to 'undisclosed recipients'. Emails can be 'blind copied' (BCC'd) to a long list of addresses, but each person will see only the original 'to' address, not the - possibly thousands - of BCC addresses used by the spammer.

What can I do about it?

To protect children from seeing unwanted mails, and to deal automatically with as much spam as possible, it is necessary to become a little technical - or to know someone who can do the necessary setting up. Complaining about each item you receive would help to stamp out spam more quickly, but that does require that you read and carry out some work on each email. You may decide it's better to delete as much as possible and only protest at anything which catches your eye as being especially annoying. Virtually all email software includes message 'rules' which allow the user to move emails around and delete them based on the sender, the recipient or the content. For children, you may want to set up an arrangement that will only allow emails i) addressed to the correct email address AND ii) sent by one of a small number of specified email addresses to be put into a personal mail box. You can limit receipt of emails to those sent by friends and family. For older email users, a small number of rules should take care of most junk email.

Try to find email software like Outlook Express that can delete emails from the server, without even downloading the message to your computer. Because much spam is not addressed personally, you can delete any message that does not show a correct email address. Because porn spam includes words or phrases you would not expect to see in normal correspondence it is possible to delete any message that contains those terms - a rule that may be unpleasant to set up, but will avoid any further exposure. If these rules for some reason exclude emails you do want to receive, you can set up an 'exception' for specific sending email addresses. If spam still sneaks through, you may be able to set up additional rules, or vary an existing rule to exclude stray messages. Much more information is available from your email software help screens, and generally on the Internet. Look on one of the main search engines under 'spam'.

Reporting Spam

Most responsible Internet service providers take a very dim view of spam, attempted fraud, or any other abuse of their standard terms and conditions. If you are particularly offended by a specific email, you need to learn to read the header information to identify where it came from. This may have nothing to do with the email address shown in the 'from' information - spammers can easily forge such information. For this reason don't overreact when you report the problem to the ['abuse@'](#) address of the ISP. If you do make any such reports, send the header of the email as well as the message text. Don't under any circumstances seek revenge – your technical expertise is almost certainly not up to it. 'Mailbomb' software exists that can fill up your mailbox with thousands of duplicate messages to cut you off from any email contact. Your ISP may shut down your own account if you have major problems. And finally unless you are an Internet anorak, you may not appreciate that the Spam wars have generated an increasingly sophisticated range of weapons. Software will now search through the Internet for contact email addresses left on websites, guest books and in newsgroups. Defensive software can generate spoof email addresses to confuse such searches. Spam specialist email software can mail out in bulk from a disguised address, keep track of responses, eliminate duplications and highlight 'confirmed' addresses from unsubscribe requests. Similar routines can also provide all possible email addresses at a specific domain just by working through popular combinations of nouns and names.

Emails can contain 'spyware' - even just reading the email loads an illustration into the message and can confirm your email address back to the sender. While viruses are only

peripherally connected with spam; never, never, EVER open an attachment to an email - even from a friend - unless you know exactly what it is and were already expecting it. Beware even of following a link from an email to a web page - the link may start a disguised attachment and infect your machine, or a web page may use built in scripting to place a file on your computer which gives someone else control of your system. If you access the Internet, you must have up to date antivirus software, and it is advisable to have a 'firewall' which controls all access to and from your computer.

Author Stuart Cliffe is originally an insurance underwriting, marketing and systems specialist based in Wales. Chief Executive of the National Association of Bank + Insurance Customers he is also an expert on consumer and small business financial service issues.

Contact him via the NABIC website <<<http://www.LemonAid.net>>>