

## **DEALING WITH SPAM**

"Spam" has become such a part of the online community's vocabulary that it was only recently that I discovered the etymology of the word. Strangely enough it was on the SPAM website (the use of upper and lower case will become clear).

Use of the term "SPAM" was adopted as a result of the Monty Python skit in which a group of Vikings sang a chorus of "SPAM, SPAM, SPAM..." in an increasing crescendo, drowning out other conversation.

This is a quote from the official SPAM website - that's SPAM as in the luncheon meat.

We do not object to use of this slang term ... although we do object to the use of our product image in association with that term ... if the term is to be used, it should be used in all lower-case letters to distinguish it from our trademark SPAM, which should be used with all uppercase letters.

These days there are probably as many email users who have seen the Monty Python "skit" as have actually eaten SPAM - not many.

Spam has become so common that it is in danger of "drowning out other conversation", i.e. legitimate emails, it could lead, if not to the end of email, then to a severe decrease in its use.

I receive, on average, two thousand emails a day. Every morning I am met with an Inbox that is 70% unsolicited email. The reason for this is that I have a lot of alias email addresses because of the work that I do and these email addresses are in the public domain. Discounting these addresses, though, I would still say that an unacceptably large proportion of the mail that I receive is spam.

It has gotten so bad that in my zeal to delete or filter spam out of my Inbox I often lose emails from friends or, much worse, colleagues or clients.

Message Lab (a Managed Service Provider specializing in e-mail security) recently published a report stating that 30 percent of all e-mail is unsolicited and will continue to grow throughout 2003 until it surpasses non-spam sometime mid-way through the year.

### **So what can we do about it?**

Well let's first look at how the spammers get their data and this may suggest some solutions to tackling the problem.

The first method is quite legitimate; we give them the data freely and without thinking. When you fill out a form online the information is stored in a database somewhere. All legitimate websites should have an "opt in" option whereby you give them permission to use the information that they collect from you within certain parameters. If they are part of a larger conglomerate they will usually ask for permission to pass your details along to other companies within the group. On some forms it is made quite clear that your details will be sold ("passed" is the term they will use) to other companies. It is entirely up to you whether you tick the box or not. Technically it is not spam if somewhere along the line can prove that you opted in to receive "more information".

Read the wording of these messages very carefully, some forms are worded so that you have to tick a box NOT to receive email in the future - this is called "opting out", but due to the Data Protection Act this is becoming less and less common.

If you do have to fill out online forms try not to use the email account you use every day (e.g. your work email).

The second method of collecting email addresses is called harvesting and it is diabolical. An email harvester is a piece of software that gathers email addresses by trawling through websites, newsgroups and, theoretically, chat rooms for email addresses. It works like someone wandering around the Internet copying down all the email addresses that are in plain view - only it does it a lot quicker. A harvester cannot enter the databases that companies keep as these are protected behind firewalls, what they can do is collect addresses that are held within the HTML of a web page.

The best way to combat harvesters is to be vigilant about how you use your email address. Use a fake one on newsgroups and chat rooms. Most ISPs will put safe guards in place that do not allow this type of software to work on the sites that they host. It is a good idea, though, to speak to your ISP, or your friendly Sys Admin person, and ask them about the anti-spam protection they have in place.

If you use Outlook a good solution to the spam problem is to use the "Junk Email" function within "Organise", ensuring that all such mail is put into your delete folder. Every time you get a piece of spam mark it as "Junk Email". It is quite an

effective method of dealing with repeat offenders, but has, in my case, led to me losing some friends' email.

A longer-term strategy that is becoming common in the US (the source of a lot of spam) is to resolve never to buy anything from a company that has spammed you. The purpose of spam, after all, is to sell something, if the spammers don't get the results they need, then they will have to find another method to get us to buy from them.

Our personal data; address, phone number, mobile number and email address are all valuable pieces of information. Valuable, that is, to marketers. Be very protective of your valuables, you wouldn't give your house keys to a complete stranger.

© Steven Gaythorpe 2008