Earlier this week, I personally received over 1,200 e-mails in a day, of which most were unwelcome spam, from people I do not know. Many carried viruses, others were hoaxes or fraudulent tricks or were from companies too stupid to realise that junk mailshot marketing by email is the fastest way to kill your brand and image.

Spam is a major challenge, costing organisations and individuals many billions of dollars a year in lost productivity. The web-enabled world is at risk if current spamming trends continue with up to 50% growth in spam volumes every few months.

We are vulnerable to spam for two simple reasons:

Firstly, it costs just a few dollars to buy lists of maybe 400 million e-mails and a spamming programme, and it costs nothing to press a button every day to send out another 400 million spam mail messages. In comparison, it takes time (and cost on phone lines or mobile networks) to download, and time to deal with them. Worse still, in the snowstorm of spam, vital messages can easily be lost. And spam detectors can make mistakes - software designed to isolate spam can at the same time bury important messages along with all the junk. So long as this gross inequality exists between the costs of delivery and the costs to the receiver, the spammers will continue to rule.

Even if response rates fall to zero, you only have to have a new group of fresh hopeful spammers every few weeks, who have bought the software and lists, to go on making everyone's life a misery.

Secondly, spamming software exposes a major internet weakness: knowing who really sent you an e-mail. It is not easy for the average company or home computer user to tell who really sent a message. In a few seconds I could set up my own account so it looks like all my messages have originated from the White House, or Microsoft, or your best friend. I don't in most cases even need to know the correct e-mail address to carry out the deception, so long as the invented address looks believable.

Governments will be forced to take action sooner or later - including the US who until now has had a remarkably relaxed attitude to spam. More spam originates from the US than any other nation.

Steps could be taken rapidly to kill spam - for example by internet service providers blocking large numbers of identical messages from senders, once a warning system (confirmed by a human being) has identified a new spam wave. Penalties could be applied to internet service providers who allow spamming to pass through their systems once antispam protocols have been agreed.

Since the aim of marketing spam is usually to increase traffic to a particular site it would not be too difficult to get global agreement that certain sites are blocked if they are connected with spam (making sure of course that spammers are not deliberately pointing traffic to an unconnected site to encourage an innocent site to be "taken out".)

Viruses are a different matter of course, but related to spam attacks since some spamming techniques use viruses to take over host computers as new spamming machines.

At the very least it should be made illegal in as many nations as possible to carry out mass mailings to people who have not agreed to be contacted in this kind of way. In America such action has been criticised as against the spirit of freedom, but we need to recognise that last-century thinking about paper mailshots is totally innapropriate for spam, because the cost of marketing and making a nuisance is so small.

Bill Gates has proposed a solution which would deliver to the reader of every e-mail a small payment from the sender to compensate for the time to read it. Much like the postage stamp today, it would have an immediate impact on those who are mailing millions of people and a minimal effect on the rest of us (the cost per e-mail could be a fraction of a cent).

But it would be open to abuse, fraud and would involve running costs.

Far simpler to use recognition software across the network which activates warnings, so that blocks can be applied and sanctions made.

In the meantime the best software I have come across for an individual PC is Norton's own (symantec.com)
which integrates with Outlook. All e-mail is scanned as it arrives and spam is dumped into a separate folder. Norton is usually accurate and learns from mistakes.

However, a more robust solution prevents spam altogether. It works as follows: when you receive an e-mail, if the address of the sender is not already on your approved list, a reply is sent asking the sender to register. When they do so, they see a number appear on their screen which is assembled as a pattern which cannot be read by computers, but can be worked out by a human eye. This sender of the original email enters the number to prove that there really is a human being at the keyboard and not a spam robot. After that, the person's message is cleared, together with all future mail from the same address.

It may be robust, but it is tedious and can be annoying to those trying to communicate with you. There is also an alarming possibility that you may miss out altogether on vital e-mails - for example from a utility company or your bank - that have been sent by a machine and so blocked.

Article Written 2002.