

Stopping spam

The origin of the word SPAM is dated back to the end of the 2nd world war, when the American Government was trying to face famine by handing out canned meat called “special ham” people used to abbreviate in SPAM to stress its low quality. Today we call SPAM high-volume unsolicited advertising messages that fill up Internet users’ in-boxes in order to pitch products or trick people, who do not always manage to avoid receiving them.

Typically, SPAM are bogus “special offers” that promise people to get money easily. For instance, many people receive messages about Work-at-Home opportunities requiring them to buy the whole equipment to do the job. Usually, only after having spent a lot of money, people discover the trick. Also chain letters have a similar scheme: people have to buy valuable items to receive a big return on their investment, but it does not come about. Often, SPAM is sent only to annoy people through hard-core erotic messages and explicit sexual images. These are only a few example of scams which spammers carry out every day by exploiting Internet communication power and forcing people to take measures in order to prevent or stop SPAM.

The most-used defence means which consumer protection agencies suggest is a spam filter which filters out e-mails with a certain keyword content and channels them in a special in-box folder where users can delete them. Another one is spam killers which allow people to fill a blacklist with spammers’ e-mail addresses and to use this list to prevent known spam from reaching people’s in-boxes. However, these sophisticated software have limits: filters often block valid messages too which contain the general keyword chosen to avoid spam, and killers cannot defend against unknown junk mail senders. Consequently, both these programs do not entirely solve the problem. In addition, people can fall back on more empirical strategies to avoid SPAM such as choosing more unique e-mail addresses to avoid being found through spammers’ dictionary attack attempts, or outputting their addresses from newsgroups, chat rooms spammers most use to get e-

mail addresses. However, as spammers often buy lists of e-mail addresses from brokers who harvest them from every website, often these measures are unable to remove the spam threat.

Surely, the most effective approach to stop spam streaming once and for all is the legal one. The American Federal Trade Commission is working in this direction as seen in the “Can Spam Act”, signed on December 16th, 2001 by the U.S. President George W. Bush, which provides for law enforcement actions against spammers. But, as senders hide their identity to avoid being tracked down by Internet Crime Policy, finding them takes much time and skilled computer detective work. Consequently despite the fact that the new law took effect on January, 1st 2004, today, “Bringing actions quickly against spammers is still impossible. These cases will take time to build” said Timothy J. Muris, the chairman of the Federal Trade Commission.

In conclusion, despite several strategies have been devised up by common people, and legal measures have been taken by law officials to stop or cut down the spam threat, today spammers carry on exploiting Internet powerful resources to sell products, to trick or only to annoy Internet users who still have to put up with spam pouring into their in-boxes.

References:

<http://www.ftc.gov/bcp/online/pubs/alerts/spamalrt.htm>
<http://www.ftc.gov/bcp/online/pubs/online/inbox.htm>
http://reviews.cnet.com/4520-3534_7-5024577-1.html?tag=tm