

The All Party Parliamentary Internet Group (APIG) inquiry into stemming the flow of bulk unsolicited email ("spam") to UK Internet users.



27 June 2003

About EEMA and EEMA's involvement in SPAM

As Europe's e-Business industry association, EEMA has a particular interest in addressing the impact of **spam** on the productivity of European organisations. The topic is of enormous concern to our members (over 250 European Organisations) and of particular interest to our User Organisation members, all of whom service a cross-border network of users communicating electronically. Members say that despite ever increasing efforts to block **spam**, the amount of **spam** received has increased significantly during the last six months.

Such is the extent of our members' concern, that we are currently developing a best-practice guide to give suggested methods of dealing with **spam** to the EEMA community. The guide will be a result of users voluntarily pooling their thoughts and resources at interactive workshops, to exchange ideas and provide suggested solutions to other EEMA members. Other initiatives are being investigated, and our involvement with the APIG would, we feel, be useful to the Group, and to our member organisations.

Following are our thoughts on the subject.

The Background

spam

spam has become the commonly-used term for unsolicited bulk email. The volume of such email is increasing. The goal of any measures has to be to block **spam** without rejecting legitimate business email. However, spammers are aware of blocking technologies and will attempt to circumvent them. As such, any solution will become transitory without regular refinement.

The global situation

25 – 40% messages on the Internet are **spam** (8% in 2001). It is generally regarded that 180 spammers are responsible for 80% of **spam** on the Internet. The biggest global spammers are in the US. Over the last six months there has been substantial increase in the receipt of **spam**.

The language of spammers is mainly English, although some Spanish and French **spam** has been received. The law is not much help in the fight against spammers, at present, as spammers are often speculative organisations doing things on the 'fly' using very low cost methods to gain the attention of the maximum amount of recipients.

Common **spam** subject areas

The main types of **spam** in the US relate to the sale of loans and mobile phones. In Asia and Africa it is predominately of a pornographic nature. And there are an increasing number of mails relating to drugs. High profile or household named companies such as F Hoffman la Roche, Volvo, Shell, Unilever, Royal Mail, Siemens Business Services are the worst hit.

In the UK, identified **spam** falls into the following categories:

- Financial marketing
- Product-oriented messages (general goods or services).
- Pornographic

- Health
- Spiritualist / organised religion
- Fraud
- Leisure messages (prizes, online games)
- Miscellaneous

What can users do right now?

There are various levels of **spam** protection – i.e. at the recipient's computer, the organisations server and at the organisations gateway from the Internet. Already, there are broad actions which can be taken to tackle **spam** such as:-

- **User education and deletion.** Users can take responsibility for manually deleting unsolicited email. Guidelines should be produced to help identification;
- **Writing to ABUSE@.** Emailing the ISP is likely to be more effective than contacting the bulk e-Mailer (as in many cases, the original source cannot be contacted);
- **e-Mail relay configuration.** The email relay can be configured to only allow the receipt of (fully or partially) RFC x821 compliant email;
- **Content checking solutions.** These can perform automatic header, content and lexicographical analysis of email to determine whether it is **spam**. These systems usually attribute positive and negative scores to the email (based upon known characteristics), and the total is compared to a threshold (resultant action is usually determinable);
- **Blacklists.** These can be used to reject mail from a given source. Commercial blacklists (e.g. MAPS) are compiled from complaints of **spam** receipt. It is possible that a blacklist may include sites added unfairly or accidentally;
- **Whitelists.** The antonym of a blacklist. Its application will only allow email receipt from known (listed) sources.

The Business implications

The cost of **spam**?

Business e-Mail addresses used by spammers are harvested from newsgroups, non-delivery receipts, from the web (using robots), interactive quizzes given out on behalf of people, and employees who have left and taken the organisations address list with them.

spam is a huge cost to business, and some organisations now store **spam** at the gateway so they don't have to archive it. For example, one global organisation alone stopped 66 million messages in the last year. They now stop in excess of 8 million messages per month with another 2 million messages presumed to be getting through. With **spam** message taking at least 3 – 10 seconds of time to process, this particular organisation calculated in April 2003, that 700 man days plus the transportation, storage and archiving had been saved by rejecting all **spam** before it went through the organisation's gateway. However, still the cost of managing the influx of **spam** is astronomical to any organisation.

Broader implications of **spam**

The entire development of the Internet and the use of electronic communications in a society may be affected by **spam**. Many electronic services that are considered worthwhile may be seriously hampered or even not be adopted due to **spam**. The most obvious thing is the public electronic directory of e-Mail and phone addresses. This was one of the first big ideas for a society more reliant on electron communication and commerce but in view of **spam** this is simply not going to happen.

A few legal considerations

- If **spam** gets into the system, some organisations are bound legally to archive it due to other laws and regulations, which affect the organisation.
- In Europe messages must show the senders' mail address.
- In the US, as long as a spammer gives the recipient the ability to remove him or herself from a list, then spammers can legally carry on spamming.
- Employees can sue their own company for not providing adequate protection against **spam**.
- Any organisation must consider the implications of the privacy and data protection laws in their country affecting the interception of an employee's email in their fight against **spam**

Conclusion

There are no clear guidelines, within the UK, Europe or the USA, to combat this expensive and disruptive problem. Waiting for the Internet to fix itself places the recent growth of e-Mail and associated electronic communication in jeopardy; if spamming is allowed to continue without legal and technological intervention, the future of electronic communication is seriously floundered. This is a situation EEMA views with grave concern, as it could take the industry back to where EEMA found it 16 years ago . . .