



This white paper
outlines SPaM
solutions and
benefits.

SPaM

SPaM	2
What is SPaM?	2
Solutions	2
Benefits	4

What is SPaM?

SPaM is unsolicited bulk email, usually advertising, on the Internet or Usenet newsgroup postings sent to a large number of people who didn't ask for it. The act of sending spam is "spamming." Someone who sends spam is a "spammer." The term "spam" probably comes from the Monty Python sketch where the name of the canned meat product is used so often that it crowds everything else out. Spam in this sense is the electronic equivalent of junk mail sent to "Occupant", except that the recipient pays the vast majority of the cost receiving the unwanted mail. It has evolved from simply being a nuisance to becoming a significant problem, especially for businesses.

Solutions

There are countless offers available to reduce the amount of Spam. Where do you begin? E-mail can be filtered at the user level through the use of a personal email program, such as Outlook or it can be blocked at the server level through the use of Blacklists. Many commercial and public blacklists, such as MAPS and ORBZ/S, follow a "guilty until proven innocent" approach, which frequently blocks email from legitimate senders, such as a client, thus resulting in loss of productivity or vitally important information.

At Fluid Consulting, Inc., we believe in an approach that removes the hassles of Spam without further inhibiting the productivity of our client. Yes, we also use blacklist, however, our blacklist contains only the addresses of the most egregious spammers on the Internet. While conservative, our blacklist can immediately block nearly 10 percent of our customer's inbound spam.

We also use a method referred to as **fingerprinting**. Messages not blocked by blacklisting are fingerprinted to detect matches with known spam message characteristics.

Fingerprinting technology leverages knowledge gained from filtering mail for our entire customer base. The fingerprinting database aggregates data from all spam blocked by our system allowing the fingerprinting process to become more intelligent and refined as more mail is processed. Messages identified as spam are fingerprinted and given a unique id based on their content. If these messages come through our system again, the fingerprint is detected and the message is marked as spam. Messages are analyzed to determine new spamming methods (i.e., base64-encoded spam). Once determined, our team modifies our scoring layer on the fly to catch spam using the same method.

Rules-based scoring is another method we choose to reduce the amount of spam. We assign scores to messages based on more than 20,000 rules that embody and define characteristics of spam and legitimate email. Points are added to the score if a message contains characteristics of spam; and points are subtracted if it contains many characteristics of legitimate email. When a message's score reaches a defined threshold, it is flagged as spam. Message characteristics we evaluate and score include:

- Phrases in the body and subject of the message
- Formation of headers (i.e., Message-ID, Received, random characters)
- Originating mail server
- Originating mail agent
- From and SMTP From address

Most customers choose to quarantine messages identified as spam outside their network. Quarantined messages are stored and deleted after 15 days. Customers can review quarantined messages and retrieve improperly blocked messages through a Web-based tool. We have a very low incidence of blocking legitimate email - less than one for every 250,000 emails received (less than 0.0004 percent). As an alternative to quarantining messages, we also allow spam to be sent through to customers. When we forward spam, it can modify the message to flag it for internal review. Modifications can include:

- Inserting an X-header for filtering inside the perimeter
- Inserting a new subject line message (i.e., < This is spam >)
- Directing spam to an internal SMTP mailbox

Benefits

Automatic spam filtering –

No user interaction is required; and it is not necessary to set up of individual accounts

Highly accurate filtering –

Legitimate business email is not blocked.

No white listing –

Highly granular and accurate spam filtering technology eliminates the need to white list approved mail senders.

Hassle-free quarantine –

Spam quarantined can be reviewed through the Web-based interface; quarantined spam automatically expires after 15 days and is deleted.

Improved network efficiency –

Eliminating spam outside your network reduces the load on mail servers and results in network usage and storage savings.