Do you use any anti spam methods?

Author:
Your-Site.com

Created On: 06 May 2005 09:22 AM

Greylisting is the first level of anti-spam measure we use.

It works like this:

Our mailservers keep a database of ip/server/email addresses that have sent emails to the servers.

If an incoming email server/address is not in the database, the server sends a "message refused - please try again later" message to the sending server, then adds the sending server and email address to the database.

The sending server is supposed to accept the return error code as a "soft" error, and resend the message at some point in the near future. When it does, the server finds the ip/host/email addresses in the database, and accepts the message as it normally would. Properly configured sending servers will resend the message in 5 to 30 minutes. Our mail servers remember the incoming ip/server/email addresses for 30 days - after 30 days of no messages, the ip/server/email addresses entry is deleted, and the next time a message comes in from that server/address, the process is repeated. If messages come at less than 30 day intervals and all 3 fields (ip/server/email addresses) are the same, it should never expire.

The basic idea is that spammers ignore all error responses, since they know they're sending to tons of invalid addresses, and won't take the time to resend on soft errors. Thus, a lot of spam will never get through. Properly configured mail servers will resend the message, at the expense of a short delay on the first message.

Some legitimate email servers are not properly configured, and fail to resend messages they are requested to or delay the message by a large amount of time.

We also use other methods, such as keeping blacklists of known spammers, as well as scanning emails and assigning likely hood of spam numbers to them and virus scanning all incoming attachments.