

## Junk Mail Primer

Junk mail, unsolicited e-mail, or Spam, are words every Internet user knows. There are legal interpretations of what and what may not be constituted as junk mail. Should the e-mail sent by your friend without permission, be considered, a junk e-mail? All the unsolicited e-mails are not necessarily bad. For example, I did purchase a foreign language learning CD after I read about it through an unsolicited e-mail. On the same token, breast enlargement e-mail will definitely go into my trash bin, for many reasons (One of them being that I am a male). These types of questions make the distinctions very hard. Yet, somehow, we have a look at the subject line and we know what it is. No one can argue that the junk e-mailers have every right to send what they send. There is this issue of responsibility, which fades away in the virtual world of e-mail. If a business or a person sends the junk mail using U.S. mail, it incurs some expense. The expense makes them responsible. They target the segment only what they think will work. However, the cost of sending e-mails is nothing more than your monthly charges to your ISP. This has made some of these folks very irresponsible. As a result, yours and my mailboxes are flooded with messages we don't want to wish to see. Folks are so scared with the junk e-mails that they are changing e-mail addresses every so often. I consider my email address like my phone number and I don't think that I have to change my phone number every month just because I am getting too many unwanted phone calls. You have as much right to stop the Spam as the spammers do to send them.

### How do they do it?

Spam has become a big business. There is technology behind it. A spammer has to make sure the following:

1. Hide their foot prints  
This usually means use a phony return address or sometimes a valid return address, belonging to someone else.
2. Don't make use of your ISP's mail server, because most ISPs, like normal people don't want to be bothered with irate recipients.

The Internet e-mail uses a protocol called SMTP. The SMTP stands for Simple Mail Transfer Protocol. As the name implies, the SMTP protocol is really simple and straight forward. The designers of the protocol were looking for functionality at that time. An SMTP server is much like a U.S. Post office mailbox. Consider the e-mail, a letter, which anyone can drop in the mailbox, and U.S. Mail will deliver the letter to where it is intended to go. In the e-mail world, you don't have to put stamps on the letter. Like the mailbox analogy, it does not matter to the SMTP server, who you are and where the message is going. In the earlier days of the Internet, the spammers use any mail server, which will accept their bulk messages. Soon, the ISPs and the mail administrators realized this conspiracy, and took actions. Their actions were analogues to moving the post office mailbox inside the building. This way, only the authorized people are allowed to drop the letter in the mailbox. Any mail server, which is left out in the open these days, is termed as "open relay", and is black listed by many watchdog agencies.

These excerpts were taken from SMTP Trap user guide.

Eventually, the spammers felt the squeeze, and went back to the drawing boards. The mechanism they came up, is still used by most of the bulk e-mail programs.

To understand their method we must first understand how the e-mails get routed on the Internet. Everything at the Internet level works with IP addresses. Similar to human analogy, an IP address is a unique address for a computer. Without an IP address a message could not be delivered. Since the IP addresses are just numbers and we humans are not very good at remembering large numbers, we have delegated this task of converting the names to IP addresses to computers. These computers are called DNS (Domain Name Servers). A domain is a name we can relate to, like yahoo.com etc. The domains are registered by many agencies. These agencies (also known as registrars) maintain the owners' information as well as the IP addresses of the DNS', which contain information about the domain. Whenever a request originates to contact a server under a domain (www.yahoo.com for example), the request first goes to its registrar. The registrar says, I do not where this server is, however, I could tell you who has the information about this server. So, the registrar points the request to the DNS server(s) for the domain. The DNS for the domain converts www into an IP address and informs the sender of this address. This mechanism is called name resolution (Conversion of name into an IP address). Apart from name resolution, the DNS servers contain a special entry in their tables for the mail servers responsible for the domain. This special entry or record is called Mail Exchange (MX) record. When queried for an MX record, a DNS server usually returns the IP address(s) of the mail server(s) responsible for a domain.

Sophisticated bulk e-mail programs actually query the DNS for every recipient's domain and deliver the message to the mail server responsible for the recipient's domain. Since the mail message is designated for a recipient within it's domain, the mail server gladly accepts the message. Note that the same mechanism is used when you use your ISP's mail server to send a mail to anyone outside your domain. In other words, the recipient's mail server does not really differentiate whether a valid mail server, or a bulk e-mail program is sending a message. The spammers, all around the world use this little loophole and exploit it.

### **Junk Mail Filters**

It is actually not hard to eliminate the junk e-mails. The problem is that as soon as you implement the rules, the good guys get eliminated too. As a result most administrators do not bother implementing them or keep them rather loose.

The following section covers different mechanism you can adopt and their pit falls:

1. Block the sender by IP address. This is a very ineffective way of suppressing junk email. The good spam artist tries to hide his footprints. Most of them use dial-up connections with dynamic Ips. Blocking those Ips permanently is not fair to the people who may get those addresses subsequently. I have also seen when overzealous system administrators block the whole class C of addresses, when the spam originates from fixed IP collocated servers. This is also unfair to other companies who may be collocating at the same location and sharing the same class C. There are websites who claim to be watch dog for spams and maintain

These excerpts were taken from SMTP Trap user guide.

list of blocked IP addresses. If this technique is used, it should be used with caution and with fairness to everyone.

2. Do not accept any email, if it does not come from a valid mail server.  
This is easy. Check the name of the sending server. From the name, derive the domain. Determine the IP addresses of all the mail servers for that domain, if this server's IP address is one of those IP addresses then allow, else reject the message. Most of the small domains will be able to come in using this technique. However, big domains like hotmail, yahoo etc. use outbound servers, which are not listed as valid mail servers under their domains. Being large domains, they have so many of them.
3. Do not allow anyone who cannot be reverse resolved.  
The mechanism of reverse resolution is just the opposite of name resolution. A reverse resolution is conversion of an IP address to a name. Many spammers disguise themselves as someone else by putting a bogus name for the mail server. Many mail servers will look at the name and allow them in because they think they are valid (based upon a name they trust). However, performing a reverse resolution will reveal that the sender is not who it claims to be. The pit fall for this check is that many administrators are either too lazy to do it or are simply ignorant about it. As a result, **good guys** get eliminated again.
4. Eliminate by sender, subject, and the contents.  
This is probably the most used, yet most ineffective way to eliminate the spam. Most spammers use changing return addresses. Most likely, they will never use the same identity to send the same spam. Eliminating spam by subject and contents has the risk of eliminating e-mails, which are valid and genuine.

A good strategy to fight the Spam is to utilize a combination of the techniques above and find the one, which works for you.