Spam

By Govind Rammurthy – MD and CEO – MicroWorld Technologies Inc.

Spam is the vilest manifestation of e-mail abuse. This white paper provides information about Spam, losses caused by Spam, how Spam works and suggests key features that a good Anti-Spam software should have.

What is Spam

Spam is unsolicited junk mail sent to you or your mail server. People who indulge in such activities are called Spammers. These are sent by commercial advertisers who may offer dubious products, get rich schemes, products that do not suit your life style, promote illegal activities, etc. The intent here is to make you spend money. Almost 60% - to 70% of Spam is related to Porn.

There is another type of spammer who sends large number of e-mails that flood your mailbox or mail server. The intent here is to cripple your e-mail service to such an extent that you cannot receive genuine mails. This is termed as Denial-of-Service (DOS) attack.

Why Spamming happens

As technology advances, people find new ways to subvert it. The rapid spread of Internet and the easy availability of free e-mail service has given a cheap and easy means to send and receive messages. The flip side is Spam. Spamming provides a very cheap and 'cost effective' means to reach a wide audience. It costs the Spammer almost nothing to send mails and invariably get an eyeball count.

Losses caused by Spam

Some of the losses caused by Spam are listed below:

- Spam is received through e-mails and may have alluring subject line like: Free offer, Chance of a lifetime, etc. Invariably you try to open the mail and read it. That is what the Spammer wants you to do. Opening the mail, reading it and then deleting it, consumes your Internet access time and costs you money. The mail servers that have delivered the mail through a series of servers have spent money and used bandwidth to deliver junk you did not want. Probably the junk mail was ahead in the queue for mails to be delivered and was given precedence over an urgent mail.

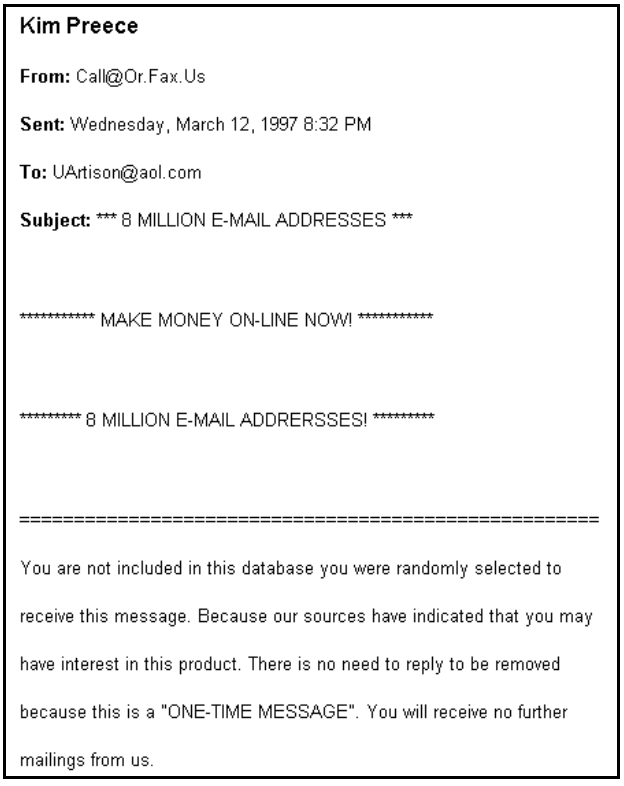
- Some Spam mails have attachments and the mail asks you to open it. If you do so, you risk running a virus that may be hidden in the mail. The costs involved in removing a virus from your system are massive.
- Some Spam mails after enclosing an alluring description of products or services, ask you to click on a link for further information. These links may open porn or other sites that you had no business visiting. But details of the visit are recorded in your server and you may have a lot of explaining to do.
- Products advertised through Spam mails require that you provide your credit card number and other personal information. Besides getting your account billed for junk items, you also open yourself to more Spam.

Are there any Anti-Spam Laws

The US Congress has introduced Bills, which should deter Spam authors. These laws make illegal, the act of sending unsolicited mails, bulk mails, mails with forged headers and sender name. If any such mails are sent, they should carry the author's physical address, e-mails ID and opt-out instructions.

For laws regarding Spamming, refer http://www.spamlaws.com/

Figure 1 shows a Spam example.



Kim Preece

From: Call@Or.Fax.Us

Sent: Wednesday, March 12, 1997 8:32 PM

To: UArtison@aol.com

Subject: *** 8 MILLION E-MAIL ADDRESSES ***

********** MAKE MONEY ON-LINE NOW! **********

********* 8 MILLION E-MAIL ADDRERSSES! *********

==========

You are not included in this database you were randomly selected to receive this message. Because our sources have indicated that you may have interest in this product. There is no need to reply to be removed because this is a "ONE-TIME MESSAGE". You will receive no further mailings from us.

Figure 1. Spam Example

How Spam Works

Spams are sent through e-mails, which is why you are reading this white paper. There are two entities: sender and receiver. Intermediaries like ISPs, and mail servers unwillingly or willingly pick up Spam and send them to you. Now how does a Spammer living in another country, manage to get your e-mail ID?

- When you register for a free e-mail service, fill in forms, register with a news group or mailing list, you may have entered information related to your personal life style. Spammers manage to hack this information, or they register as genuine users to these sites and get access to your e-mail ID.
- **Spiders**: These are special software programs that run through the Internet. They search for code in WebPages that looks like e-mail IDs and when such data is found, they copy it into a database. Spam authors use the data to Spam.
- **E-mail extraction software**: These are commercially available software's that allow you to search for target e-mails IDs. They have a search engine and if you enter key words like Vacations, e-mail IDs of companies that provide services for Vacations and people interested in Vacations is generated.
- **On-line Ad Tracking Tools**: These tools allow a Spammer to find how 'successful' the Spam was. Details of how many people opened the mail, how many responded, which Ad brought the best results, etc. are generated as a 'report'. This allows Spammer to offer a pay-per-click system.

Now comes the question of how Spam is relayed. There are many ways in which this is done. The commonly used ones are: Rogue ISPs, One-Shot Accounts and Blind Relayers.

- **Rogue ISPs**: Spammers who have enough cash to fund their illegal activities run these. Rogue ISPs obtain their own network numbering and multiple domain names from the InterNIC. Spammers use multiple domain names and manage to get across Spam blocks. While it is possible to block a domain, it is not possible to block an ISP provider.
- '**On-the-fly' Spammers**: Such type of Spammers, register as multiple genuine users for trial accounts with ISPs. Forged identity or stolen credit cards are used to establish identities. They then use these accounts to start their Spam hits. By the time the ISP realizes that they are hosting a Spam run, the Spammer uses another account.
- **Blind Relayers**: Some innocent servers allow Blind Relaying – relaying messages without authentication. Spammers route their mails using these servers. The relay sends the mail and it appears as genuine.

How Spammers beat Anti-Spam software

Spam authors have become smart. They know that the target audience has Anti-Spam software in place. They still manage to deliver Spam using a variety of techniques:

- **Subject Line**: Subject line of Spam e-mail will start with **Re:** or **Fw:.** The Anti-Spam software you have installed will assume that the Spam is a genuine reply to your mail. Such mails are allowed into your mailbox.
- **Images**: The whole Spam message is enclosed as an image in the mail. Anti-Spam software will allow the mails thinking it is a genuine mail.

Features of Anti-Spam Software

The ideal software uses a combination of Filters, that check for restricted words and allows you to add known Spam IP address or e-mail IDs to block lists. While it is important that your network does not receive Spam, the software should ensure that your network is not used to send Spam.

False Positive: E-mails from genuine senders that carry information you need are sometimes falsely identified by the Anti-Spam software as Spam. Such errors are termed as false positive. Anti-Spam software should be intelligent enough to identify Spam and genuine mails.

The following features are recommended in an Anti-Spam Software:

RESTRICTED PHRASE CHECKING:

Spam mails have an enticing subject line like: deal of a lifetime; free your debts, etc. These words may occur in the body, header, and HTML tags.

- The software should have a list of such words and phrases. Any mail with the words as the subject, should be automatically deleted or Quarantined.
- You should be able to add or delete words and phrases to the block list.
- The software should detect such phrases in e-mail body and HTML tags.
- The software should allow you to enable or disable this feature.

Figure 2 shows a screen with Restricted Phrase Checking feature, from eScan, the top selling Anti-Virus and Content Security software.

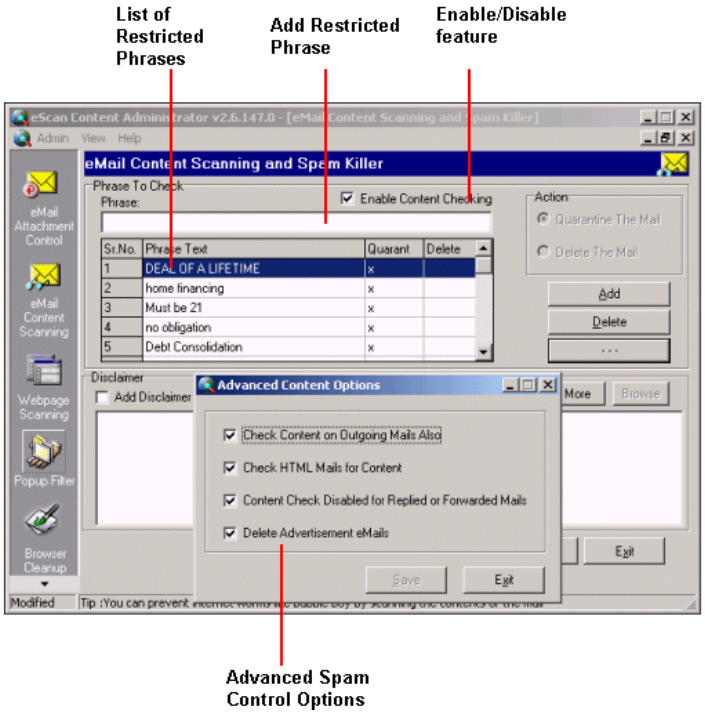


Figure 2 Restricted Phrase Checking

BLOCK SPAMMER

Another way to beat a Spam is to refuse entry to e-mail IDs that are known Spammers. Software with the following features effectively combats Spam.

- Add e-mail ID of known Spammer to the block list. Any mails received from an ID, included in the list are automatically deleted, without being downloaded into your server.
- If required, the software should remove an e-mail ID from the block list and allow in mails from it.
- Software should allow a notification to be sent to the intended recipient and system administrator. The notification should provide details of: who the mail came from and who it is for, subject, reason why the mail was deleted.

Figure 3 shows a screen with Block Spammer ID, from eScan, the top selling Anti-Virus and Content Security software.

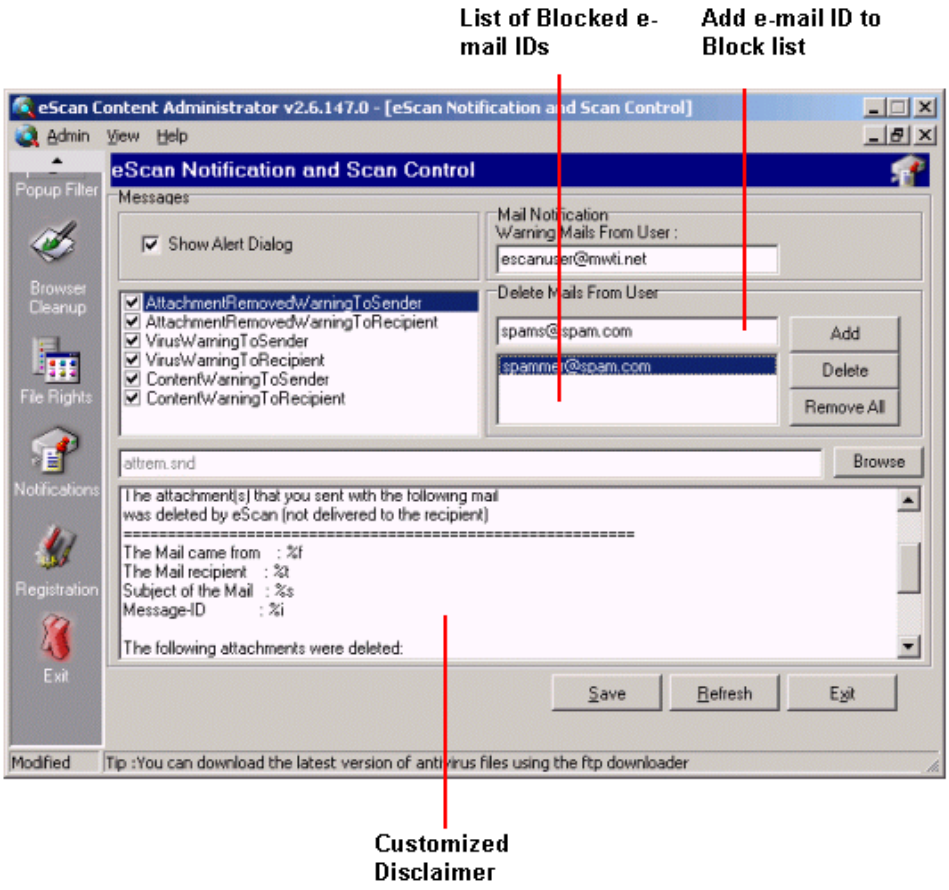


Figure 3 Add e-mail ID to Block List

What to do when you are Spammed

Spams have become quite common and are a nuisance. When the number of Spam mails you receive increases from one or two, to many, then the nuisance turns to a threat. If you use free e-mail service providers and do not check your mail regularly, then the junk mails soon choke up your mailbox capacity and genuine mails bounce. Here is what you need to do:

- For short-term results, open the mail and click **Block** in your e-mail account. The Spammer is blocked and will have to use another e-mail ID to Spam.
- For long-term results, you need to install intelligent software that recognizes Spam and automatically blocks it, before it reaches your mailbox. Refer Features of Anti-Spam Software for more details.
- Report Spam to your ISP. Enclose a copy of the Spam mail.
- **MAPS** (Mail Abuse Prevention System) is an autonomous body that maintains a **Blackhole** list of known domains, indulging in Spam. Write to them about your problem. For details refer http://mail-abuse.org/

- What was a search query yesterday turns out to be a Spam today! As an example, yesterday, you were searching for building material to construct a fence, so you found an online store, filled in the enquiry form and ticked the check box for 'do you want to receive offers for new products'. Today, you have changed your mind about the fence. But you keep getting mails about building materials. This is not Spam. Search for the unsubscribe link in the mailer and remove yourself from the list.
- The first line of defense in the fight against Spam is you. Don't be naïve and do not fall for on-line scams. We have enough of off-line ones.

About the Author

Govind Rammurthy is a hard core 'techie' with keen business acumen. He founded MicroWorld Technologies Inc. in 1995 and has been in the forefront in the fight against Viruses and other threats. He leads the team of programmers and QA who have developed world-class product suites, **eScan** and **MailScan**. These products offer the greatest control in the areas of Anti-Virus and Content-Security.

To find out how MicroWorld can help you control Spam, visit http://www.mwti.net/