ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. 2, Special Issue I, January 2016 in association with
KARUR VELALAR COLLEGE OF ARTS AND SCIENCE FOR WOMEN, KARUR
Conference on Emerging Trends and Functional Applications of Computer Technology - 12th January 2016

Spam Detection Tips and Technique for E-mail Users

U. Murugavel[1]
Ph.D. Research Scholar (Part-Time),
Bharathiar University,
Chennai, Tamil Nadu, India.
murugavel.research@gmail.com

Dr. Shanthi[2]
Vice Principal,
Alpha Arts and Science College,
Chennai, Tamil Nadu, India.
rshanthi.teacher@gmail.com

ABSTRACT

Despite of Advancement in Internet Technology, there are several possibilities in security vulnerability of internet Email users. Currently, Electronic mail is the effective way for communicating message among the users. Most of the transaction occurs through internet medium. So every day user inbox is filled with spam mails (unwanted Bulk Mails). Spam Mails are occupy not only more space (memory) and also irritate the internet users while handling it. Large amount of spam emails causing severe problem for internet users. So we need effective spam detection methods to deal with spam mails. In this paper, we presented various problem associated with spam and spam detection mechanism and tools.

Keywords:
Internet, Email, spams, spam mail, bulk Mail,

1. INTRODUCTION

Electronic mail is a powerful medium for fast and cheap communication way for internet users. So spammers used to send large quantity of unwanted mails to large group of internet users. Due to vast use of email users have resulted in the drastic booming of spam mails during the past few decades. Spammers can send Spam mail from any number of users and various locations across the earth where Internet facility is available. In order to avoid the spam mails, robust spam filtering technique has to be analyzed and implemented by the end users side or server side, and IT based organization. Spam filtering Tools, such as the e-mail filter gateways, corporate e-mail system, anti-spam services, and end-user training, provide a significant armoury for any organization. However, internet email users cannot evade the extreme critical issues to deal with large number of spam mails on a routine basis. So we need anti spam activities, in order to avoid spam mails from email users.

Spam messages cause lower productivity; occupy space in mail boxes; extend viruses, Trojans, and materials containing potentially harmful information for a certain category of users; destroy stability of mail servers, and as a result users spend a lot of time for sorting incoming mail and deleting undesirable correspondence. According to a report from Ferris Research, the global sum of losses from spam made about 130 billion dollars, and in the USA, 42 billion in 2009 [1]

Every day Email users get hundreds of spam messages with a new content, from new addresses which are automatically generated by robot software. In this paper, various spam email filtering methods is discussed to provide more robust solution and to provide basic knowledge about spam for Internet users.

2. UNSOLICITED E-MAIL

E-mail that is unwanted also called as "junk E-Mail", "Gray Mail "or Unsolicited Bulk E-mail (UBE)[2] it causes the denial of service at the network level [3].Unsolicited Commercial E-Mail is a split of spam that transports almost alike e-mail to several recipients. Spammers utilize the e-mail addresses collected from various Web pages, Bots, Directory harvest attacks, Free Product or Services requiring email address, News bulletins /Forums, Purchasing or Trading lists with other spammers and Internet service provider directories allows messages to be sent blindly to millions of recipients at essentially no cost. Spam messages are extremely irritating to most users, as they mess up their mail-boxes and prolong dial-up connections. Nowadays everyone using internet, email inbox filled with spam mails. The snag with spam mails is that they are not malevolent in nature, so generally don't get blocked with firewall or filters and etc.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. 2, Special Issue I, January 2016 in association with
KARUR VELALAR COLLEGE OF ARTS AND SCIENCE FOR WOMEN, KARUR
Conference on Emerging Trends and Functional Applications of Computer Technology - 12th January 2016

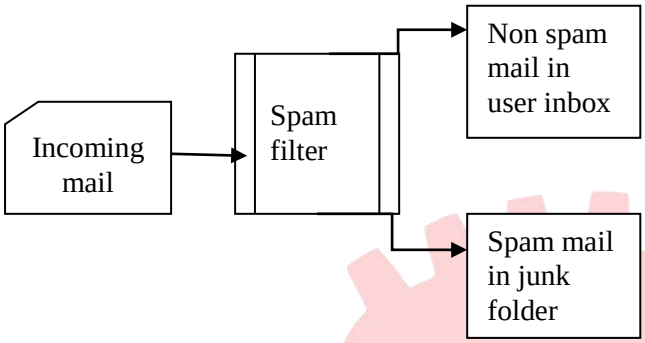

Fig2. 1Simple spam process

Fig 2.1 shows the simple spam mail process. Whenever email arrives from incoming mail server, spam filter check the mail. If the mail is suspect as spam it reach the spam folder or it will considered as ham mail.

3. TYPES OF SPAM

Spam mail can be classified into various types, the following types of spam mail are spreading into the internet world nowadays .we are mentioned some the spam types.

3.1 INSTANT MESSSAGE SPAM

IM spam also called Spam Instant Messaging (SPIM). It is used for mostly advertising purpose appearing in instant messages while open in email or online shopping. SPIM ad popup on the screen whenever it is sent. Spim is more annoying than spam emails. During internet users use a webpage instantly a popup screen will appear and irritate the user while working.

Fig 3.1.1.
IM Spam

3.2 APPEND SCHEME

If marketer has one database consists of customer names, addresses, and telephone numbers of then they can pay to have their database matched against an external database containing e-mail addresses. The company then has the measures to send an e-mail to users who have not requested e-mail, which may include persons who have cautiously withheld their e-mail address E-mail spam. It is the general type of spam. In this spammer try to send numerous spam mails to various recipients most of the internet users experienced this type of spam. It annoying the internet users and waste the memory by flooding the spam e-mail

3.3 M-SPAM

In today world everybody using mobile for communication with others. Mobile component plays a major role in human life, Due to vast usage of mobile device spammers use Short Message Service (SMS) a type of spam technique for sending. It fills the inbox unwantedly. It is also called 'mobile spam (m-spam)'

Fig 3.3.1.
Mobile SMS Spam

3.4 IMAGE SPAM

In early days, spammers used only text based mails for transport spam e-mail. They were easily filtered by the text-based spam filters. To avoid such filtration technique, spammers find new way of technique called image spam. Image spam consists the advertisement text embedded in images rather than in the body of the e-mail, because the image contents are not filtered by most spam filters.

Image spam consists of advertisement, medicine and other computer-generated text which simply annoys the user. Most of the image spam includes porn images, hair fall control, bumper car prize won and etc. Text message are stored in image format such as GIF or JPEG and displayed in the email.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. 2, Special Issue I, January 2016 in association with
KARUR VELALAR COLLEGE OF ARTS AND SCIENCE FOR WOMEN, KARUR
Conference on Emerging Trends and Functional Applications of Computer Technology - 12th January 2016

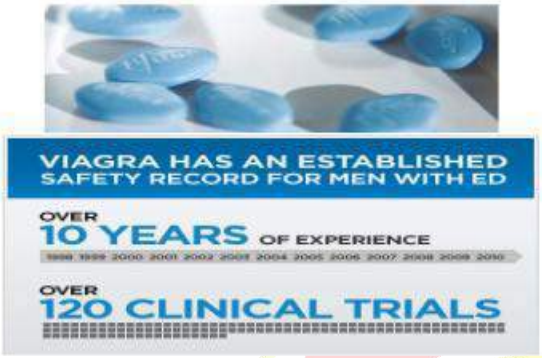

Fig 3.4.1 image spam

3.5 BACKSCATTER SPAM

Backscatter is a side-effect of e-mail spam, viruses and worms, where e-mail servers receiving spam mail and other e-mail send vault messages to naïve party. This takes place because the original message's wrapper the sender is fake include e-mail address of the victim. Because these messages were not solicited by the recipients, are substantially related to each other, and delivered in mass quantities, they qualify as unsolicited bulk e-mail or spam. As such, systems that generate e-mail backscatter can end up being listed on various DNSBLs and be in violation of internet service providers' Terms of Service

3.6 BLANK SPAM

Blank spam is spamming deficient a payload advertisement. Often the message body is omitted altogether and also the subject line. Even though it falls in the form of spam because of its nature as bulk. Blank spam may be originated in different ways, either intentional or unintentionally:

4. Worldwide distribution of SPAM?

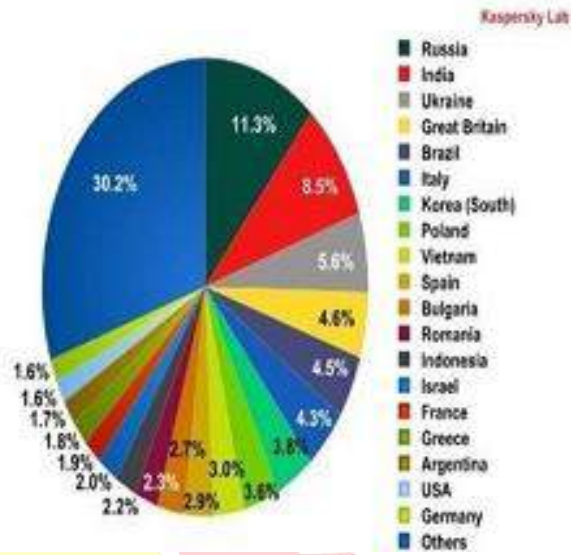

Fig 4.1 Chart shows worldwide distribution of SPAM

5. SPAMMING METHODS

5.1DIRECT SPAMMING

In direct spamming method Spammers purchase upstream connection from spam friendly ISPs They buy connectivity from non spam-friendly ISP and behind spamming, change to other ISP. They sometimes obtain a group of dispensable dialup IP addresses, proxy server traffic during those connections Open Relays and proxies. They use mail servers which allow unauthenticated internet hosts to send emails through them. Open relays and proxy servers that permit illegitimate Internet hosts to connect and relay mail through them.

5.2 BOTNETS

Electronic device (computer) is used to send large quantity of spam emails in the form of Software Robots. Robot act as centralized system for controlling the spam.

5.3 INTERNET PROTOCOL HIJACKING TECHNIQUES

IP address are hijacked to send spam range is briefly advertised via BGP and used to send spam mail are sent, they withdraw the route from the network

6. HOW SPAMMERS SEND SPAMS

6. Collecting Email address

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. 2, Special Issue I, January 2016 in association with
KARUR VELALAR COLLEGE OF ARTS AND SCIENCE FOR WOMEN, KARUR
Conference on Emerging Trends and Functional Applications of Computer Technology - 12th January 2016

In this method spammers used to collect email address. It is also called e-mail address harvesting. Huge quantity of e-mail addresses are collected without the knowledge of the address owner. Spreading of spam mails can be done using the following ways

(1) Web mail services
(2) Computer (robot)
(3) Open relays
(4) Open proxies

6.1SPAM FRAUD

Spammers may engage in purposeful fraud to send out their messages. Spammers often use of fake names, IP addresses, phone nos, and other information to set up "throwaway" accounts at various Internet service providers. They also sometime use falsified or theft credit card numbers to pay for these accounts. This allows them to move rapidly from one account to the next account as the host ISPs discover and shut down each one.

Some Other spammers engage in spoofing of e-mail addresses (much easier than IP address spoofing). The e-mail protocol simple mail transfer protocol [SMTP] has no authentication by default, so the spammer can pretend to originate a message apparently from any e-mail address. To avoid this, few ISPs and domains need the use of SMTP-AUTH, Spammers frequently look for vulnerable third-party systems like open mail relays and open proxy servers. Spammers use networks of malware affected PC called zombies to send the spam. Zombie system known as Botnets.

7. SPAM FILTERING PROCESS

7.1 TYPE OF MESSAGE

Spam filter look for the type of message being sent. If the message is spam it sent to spam folder else it is considered as ham.

7.2 HEADER SECTION

Take a look in your spam folders and scan the subject lines. If the subject lines found suspicious then the mail reach the spam folder

7.3 BODY SECTION

Your message is compared to millions of email messages the ISP receives. If your messages contains identical to OTHER types of messages are considered as spam, then your message may be blocked-up as well. For instance, if you use Gmail, look at the spam folder. It has spam messages. Domains inside your email messages could be causing issues as well. URLs in Content Destination URLs, URLs in Message Headers, URLs in Unsubscribed links, etc

7.4 USER FEEDBACK

This can be either specific to your mails or feedback for all mails received by the ISP

7.5 ADDRESSES PART

From Address use domains as well as specific e-mail addresses at those domains.

8. DEALING WITH SPAM

Currently, various spam laundering techniques are used to deal with the spam e-mail in your inbox. Avoid sharing of personal email address to unknown. The use of caution while opening new email. Avoid unsubscribing.
The use of spam Filters

9. SPAM FILTERING METHODS

Spam filtering method can be categorized in to mainly two methods, namely list based and content based filters.

9.1 LIST BASED FILTERS

BlackList

In BlackList technique is the most popular filtering methods to stop unwanted mails by jamming the messages from a predefined record of senders to end user organization's system admin create blacklist profile. If an incoming message arrives it check the blacklist profile. If the mail is not in the list will reach the users inbox else it move to spam folder.

.

Whitelist

This Method act precisely opposite a blacklist. White list allows you to specify which senders to allow the mail from. Sender addresses are stored on a trusted users list. Only legitimate sender mail received to inbox else moved to spam folder.

Real-Time Blackhole List

It works almost similar to a conventional blacklist but need less hands on maintenance. Because real time blackhole lists are maintained by third parties, who take the time to build comprehensive blacklists on the behalf of subscribers

Greylist

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. 2, Special Issue I, January 2016 in association with
KARUR VELALAR COLLEGE OF ARTS AND SCIENCE FOR WOMEN, KARUR
Conference on Emerging Trends and Functional Applications of Computer Technology - 12th January 2016

A modern technique, Greylist rejects the message from anonymous users and sends a failure message to the originating server. If the mail server tries to send the message for second time servers will assumes the message is ham and lets it proceed to the recipient's inbox

9.2 CONTENT BASED FILTERS

Word Based Filters

Word Based spam filter is the easiest method of content-based filter. In general a word-based filter simply blocks any e-mail that contains certain restricted terms.

Bayesian Filters

Bayesian filters are text based filter method and the most popular, advanced form of content-based filtering, this filter use the laws of mathematical probability to find which messages are ham and which are spam. In Bayesian filter method, to efficiently detect spam, the end users must be trained by manually feeding message as either junk or ham.

Heuristic Filters

Heuristic filter also called Rule based filter Heuristic filters works on the basis of take multiple repeating terms found in an email. Suspicious words that are commonly found in spam messages, such as 'Lottery' or 'Rolex' receive higher points, while terms frequently found in normal emails receive lower scores.

9.3 OTHER FILTERING TECHNIQUES

Challenge/Response System

In challenge/response system used to block unwanted emails by forcing the sender to perform a task before their message can be delivered. For example, if a person sends an email to someone who's using a challenge/response filter, you will receive an email right back that asks you to visit a Web page and enter the code displayed. If you successfully complete this task, your e-mail will be delivered to the recipients you're your message is rejected.

Collaborative Filters

In this method, collecting input from the millions of email users around the world. Users can flag the incoming emails as ham or spam and these notations are informed to a central database. If various users mark a particular email as spam then the filter automatically blocks it from reaching users inboxes.

DNS Lookup Systems

Various anti spam methods use the domain name system (DNS). In which all mail servers on the Internet use to identify themselves and to identify spammers [9].

10. ANTISPAM TECHNIQUES

End user side

Even though if spammers send spam mails to internet email users. It's the responsibility of users to prevent from spam mails. Users have to take precautionary steps to avoid spam by enable robust firewall or internet security antivirus software.

Admin side

Spam mails can be avoided from admin side by monitoring user's activity / system activity

Cyber law

By enforcing cyber law and strict action we can avoid spreading spam emails unnecessarily.

10.1 ACTIONS BY INDIVIDUAL:

Detecting spam

Detecting the spam found on the contents of the email, either by detecting the keywords such or by statistical means, is very popular end user techniques. There are a number of techniques and individuals can use to filter the availability of their e-mail addresses, reducing or preventing their attractiveness to spam.

11. SPAM FILTER TOOLS

Several spam filter tools are available in market today for dealing with spam and prevent from receiving it. Users have good knowledge about handling the spam mails. The following tools are most familiar in market.

SPAM FILTER TOOLS	
S.NO	**SOFTWARE NAME**
1	Symantec Mail Security for SMTP
2	MailCleaner
3	SpamAssassin
4	Bogo filter
5	Allume SpamCatcher
6	Mail Washer Pro

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. 2, Special Issue I, January 2016 in association with
KARUR VELALAR COLLEGE OF ARTS AND SCIENCE FOR WOMEN, KARUR
Conference on Emerging Trends and Functional Applications of Computer Technology - 12th January 2016

7	POP File
8	Spami hilator
9	Spam Pal

Table 11.1 shows the various spam filter tools and its official website address [10]

12. CONCLUSION

In this paper we discussed about several types of spam, filtering methods and its background process, tools to provide basic idea about spam and how to avoid spam emails for internet users. Spam can be detected and avoided by necessary tools and precaution from both end user side and server side. Every internet users must have sound knowledge about spam email and software tools used for spam filtering. Installing spam filters from end user side will prevent spam email flooding in to inbox.

13. REFERENCES

[1] Ferris Research, "Cost of spam is flattening–our 2009 predictions,"
[2] Symantec, "State of spam and phishing. A monthly report 2010,"
[3]E-mail Classification Using Genetic Algorithm with Heuristic Fitness Function
Jitendra Nath Shrivastava#1, Maringanti Hima Bindu*2
[4] Trends in Combating Image Spam E-mails
Mohammadi Akheela Khanum a, Lamia Mohammed Ketari
[5]M. Prilepok, T. Jezowicz, J. Platos and V. Snasel, "Spam Detection Using Data Compression and PSO", Proceedings of 4th International Conference on Computational Aspects of Social Networks, (2012) November 21-23, Sao, Carlos.
[6] N. Pérez-Díaz, D. Ruano-Ordas, F. Fdez-Riverola and J. R. Méndez, "Wirebrush4SPAM: A novel framework for improving efficiency on spam filtering services", Software - Practice and Experience, vol. 43, no. 11, (2013) November, pp. 1299-1318.
[7] D. Ruano-Ordas, J. Fdez-Glez and F. Fdez-Riverola, "Effective scheduling strategies for boosting performance on rule-based spam filtering frameworks", Journal of systems and software, vol. 86, no. 12, (2013) December, pp. 3151-3161.
[8] X. Ma and Y. Shen, "Combining Naive Bayes and tri-gram language model for spam filtering", Advances in Intelligent and Soft Computing, vol. 123, (2011) December, pp. 509-520.
[9] Christina V, Karpagavalli S, Suganya G
A Study on Email Spam Filtering Techniques
[10] R. Anirudh, F. Nick and V. Santosh, "Filtering spam with behavioral blacklisting", Proceedings of the 7th ACM Conference on Computer and Communications Security, (2007) October 2 – November 2, pp. 342-351, Alexandria, USA.
[11] Husna, H. Phithakkitnukoon, S. Palla, S. Dantu, R., "Behavior analysis of spam botnets" in IEEE xplore, ISBN 978-1-4244-1796-4 , Issue date 6-10 Jan. 2008.
[12] I. Androutsopoulos, G. Paliouras, and E. Michelakis. Learning to filter unsolicited commercial e-mail. Technical report, National Centre for Scienti_c Research Demokritos",
[13] Mohammadi Akheela Khanum a, Lamia Mohammed Ketari b,Trends in Combating Image Spam E-mails
[14] Brian Satterfield, November 30, 2006
Ten Spam-Filtering Methods Explained
Learn how different spam-fighting techniques work
[15]W. Gangsterer.M.Ilger,P.Lechner,R.Neumar,J.Straub
Anti spam Methods – state of the Art