



Effective Spam Prevention

Prepared by **AGIX IT Technology & Services, February 2010**

www.agix.com.au

Copyright

Copyright 2010, AGIX IT Technology & Services. All rights reserved. This book, or part thereof, may not be reproduced in any form without permission of the publisher.

Introduction

Any business will say the most annoying aspect of Internet use is the amount of Spam they receive. Not the performance, cost or complexity of the Internet, but Spam. Spam comes with a cost, it comes with security concerns and out right annoyance to the end users.

The first Spam email was sent in 1978 by Gary Thuerk. That email intended to reached 600 Inboxes. In contrast, one hundred billion Spam emails were sent in one day during 2007.

An accepted statistic is that 97% of all emails passing over the Internet is considered Spam. The Spammer usually has a goal such as; to earn money through a scam, to gain access to your systems or 3rd party accounts, to sell you something or to trick you into visiting their site which gains them exposure. Sometimes Spam emails come from seemingly legitimate and trusted sources, they look like legitimate emails from your bank or social website and they will direct the receiver of the email to well designed fraudulent websites.

The Information Technology department of any organisation is usually charged with the responsibility of minimising the amount of Spam entering the corporate network just as they do with Virus prevention, malware and pornography.

This white-paper is intended to cover the key aspects of Spam, management guidelines and recommendations for management and system administrators.

Table of Contents

Copyright.....	2
Introduction.....	3
What is Spam.....	5
Forms of Spam.....	5
Why Spam.....	5
Spammer techniques.....	6
Stopping Spam	6
Good practices.....	7
Anti-Spam procedures.....	7
RBL services.....	7
Relay and DNS.....	8
Spam filters.....	8
Router and firewall involvement.....	8
Email server positioning.....	8
End user involvement.....	9
Email flow overview.....	9
Assessing anti-Spam effectiveness.....	10
RBLs and Reporting Spam.....	10
Spam in business.....	10
Summary.....	11

What is Spam

Each weekend I receive junk mail in my home letter box. Letters from department stores, local lawn-mowing businesses and electrician service, council letters and cable TV advertisements. None of these have my name on them and I can be sure that my neighbours have received the same mail in their letter boxes. This is the old (or snail mail) version of Spam. Old but still very much in use today.

Spam is a bulk means of advertising or scamming the public. The sender has a long and ever growing list of email addresses to which they send the same email. Over time the email content changes to satisfy new interests or to by-pass spam filter. The sender either means to sell you something, to trick you into giving out your personal information or to direct you to a waiting website.

The result is that your email Inbox receives a growing amount of unsolicited emails that will probably just take up your time to sort and remove.

Forms of Spam

Whilst most Spam is delivered via email, Spam can be delivered via a mobile phone SMS, IM (Instant Massaging chat program), Fax machine, automated phone calls, website forums, social website or blog submissions and any other mass delivery medium.

All forms of Spam rely on there being an easy, cost effective, often instant, anonymous mass submission process. Most important is the cost. Spammers use mediums that are most cost effective. SMS's cost the sender rather than the receiver which differs from email. Therefore we will see less SMS Spam when compared to email.

As technology evolves, more mediums will become available and be abused by Spammers.

Why Spam

The sender of Spam (the Spammers) only needs one in a million recipients to respond to their liking for their campaign to be a success. Consider that sending email is free for the sender but costly for the receiver, there really is no financial incentive to stop Spamming. If the Spammer gets one correct bank login user-name and password as a result of sending out one million emails, the Spammers campaign would have been a success. Given the amount of Spam we see today we can be sure that Spam does pay off.

By financial cost, I mean that generally we as consumers pay for our downloads more so than uploads. Therefore it's cheaper to send an email than to receive one. So the receiver pays, not the sender. The result of which is that Spammers have a cost effective marketing delivery strategy.

If it were free to put junk mail into my home letter box, I can expect my letter box to be full every day from unsolicited mail. But there is a cost for the paper, the delivery person's time and the cost of printing the advertisement. Email Spam doesn't come at any cost to the Spammer.

Spammer techniques

A Spammer with more email addresses on their list is more effected than one with less. Therefore they will go to great lengths to gather (or harvest) as many email addresses as possible.

Spammers will do the following to gather email addresses:

1. Crawl the Internet (web sites) for email addresses.
2. Buy, steal or trade email addresses with other Spammers.
3. Trick the public into providing their email addresses freely.
4. Guess commonly used email addresses such as info@, sales@, etc.

It's worth going into each of the above points in more details to better understand how you can protect your Inbox.

- Firstly, organisations such as Google, MSN and Yahoo crawl the Internet (websites) looking for content to list in their index. Just as they are looking for content, Spammers are looking for email addresses. They both use the same technique.
- Secondly, Spammers buy, sell or trade email addresses with each other regularly to widen their scope.
- Thirdly, Spammers will attempt to gather email addresses from the public in seemingly legitimate ways. For example, they might offer a software product or white-paper to download on the condition that you subscribe by providing your email address.
- Finally, Spammers will often guess email addresses. Most companies have email addresses like info@, sales@, helpdesk@, accounts@, etc. Using this principle, Spammers will attempt to send emails to every domain name they can get hold of with the prefix of the above example recipients.

Stopping Spam

It's no easy task to stop Spam but there is plenty we can do to minimise it. The I.T administrator has a variety of tools at their disposal to minimise Spam from entering their email server. Preventing Spam can only be achieved when we understand the underling problems.

As stated earlier in this book, we can't stop the sender from sending us Spam given that anyone can send an email if they choose. But we can filter our incoming emails, we can assure our systems are part of the solution and not part of the problem and we can be sure no Spam originates from systems that we are responsible for.

A fundamental problem with Spam prevention is that emails are easily forged and completely lack security. For example, emails can easily be sent as though they had come from source A when in fact they came from source B.

This is a common technique used by Spammers to hide the true origin of their emails. By

changing their origin, they can bypass simple RBLs (real-time black lists) more of the time.

This can but often isn't checked while email traverses the Internet. The name at the bottom of the email can be anything, the senders (source) email address can be anything. Many aspects of email can be forged.

Incorrectly configured email servers contribute to the problem and are the first to be abused. Properly configured email server help to prevent Spam. This is because as an email attempts to travel from one email server to the next, the receiving server should check that the sender has certain characteristics such as a real domain name, a clean (not black listed) IP address and domain name, proper hand-shaking between servers, the correct system time and the format of the email.

Spammers are quickly discovered and RBL organisations will add them to a long list of known Spammers. Email servers can use this as a resource to assist in blocking Spam.

Another technique is to use a Spam filter. These exist for servers and desktop computers. The practice is to check email for Spam-like characteristics such as key words and phrases. An incoming email is be put through a scoring system which will assign a cumulative score to an email depending on how many key words, phrases and specific characteristics are discovered. For example, if an email contains the words “viagra” and “best prices” you can be fairly sure this email is Spam and therefore it will have a high score. On the other hand, if the email contains the work “viagra” and no other Spam-like words, it is likely to be a social email and it's score will appropriately reflect this. The Spam filter therefore cannot rely on a single factor but many factors when examining and scoring an email. The resulting score associated with an email that has passed through the filter is compared to a threshold score and determined to be Spam or Ham.

The remainder of this book aims to assist the administrator with Spam prevention through high level server configuration and filters, network structure and end user involvement.

Good practices

This chapter discusses what the administrator can do to assure the systems they are responsible for are not being abused by Spammers, they are properly configured to take advantage of all anti-Spam services, that their company router or firewall are properly configure and they have a strategy involving end users.

Anti-Spam procedures

RBL services

Assure that your email server uses RBLs to block Spam. As en email enters your email server, the server checks with an online RBL services to see if it originated from a known Spam source. If it does, it's rejected immediately. If not, it will continue on it's path.

As noted before, Spammers will attempt to hide or change their origins in an attempt to by-pass RBLs. However, a considerable amount of Spam is sent from incorrectly configured email

servers (open relays) that are abusable by Spammers. Those email servers are added to RBLs over time. Therefore it makes sense to use RBLs as part of your anti-Spam processes.

Relay and DNS

Assure that your email server requires proper DNS of the sending server, that the sender has a proper DNS MX record and that your email server is the final destination for that email.

Email servers need to have a registered domain name but it can be anything. Receiving email server should do a reverse lookup of the IP address of the sending server and receive a result. No result means the sending server doesn't have a real DNS name and therefore is likely to be a Spam source.

Assure that your email server is configured to only relay from internal (or other well thought, specific) hosts. Open relays are one of the biggest allies to Spammers. Monitoring a servers logs over time will indicate if it is being used as an open relay.

Spam filters

Assure your email server has a Spam filter configured such as Spamassassin. Such a filter will be applied to each email passing through your email server and assign a score. This has been previously discussed in an earlier chapter. However, it's pertinent to this section too. The score depends on the characteristics of the email. The higher the score, the more likely the email is Spam. Filters generally don't stop or reject emails but will modify the email header or subject line with an indication of it's score thereby allowing the recipient to sort their emails based on the outcome. For example, the end user receiving an email that has a Spam tag (as a result of the filter) may choose to have that email automatically sent to their Spam or Junk email folder for later review.

Router and firewall involvement

It's one thing to prevent Spam from entering your network of computers, but another to prevent it from leaving. Spam can originate from anywhere including computers that you are responsible for. Therefore you as the responsible I.T administrator should assure that end user computers have anti-virus programs installed and that your company router or firewall is configured to only allow emails to pass out (and in) of your network via your email server.

Desktop computers can send emails out directly as though they were an email server. Using appropriate network ports and protocols, desktop computers can pretend to be email servers and send an email to another email server expecting that the email will pass on as intended. To prevent such a practice, the router or firewall should only allow emails to pass out where the source IP address is the company email server.

Email server positioning

It's good practice to (wherever possible) separate the email responsibilities into two servers. Each server having a different responsibility. Server A is responsible for end user communications such as providing SMTP and POP/IMAP services. This server hold the end

user mailboxes and is possibly located in the end users LAN (or a server LAN if one exists). Server B is responsible for passing emails between server A and the Internet. This server performs the anti-Spam functions described in this book. Server B is possibly located in the DMZ.

End user involvement

It's the end users who are affected by Spam so it makes sense that those effected have some input into the filtering process. Consider allowing end users to make amendments to their personal black-list and white-list. Thereby giving them (the employees) some control over who can and cannot send emails to them.

Consider implementing a learning Spam filter that will make future decisions influenced by how they are taught before hand. Such systems work by having two factors to learn from; Spam and Ham. Spam is the junk email and Ham is the genuine email. By providing the leaning system with an equal amount of both Spam and Ham, the filter system can make better judgement on later emails over time.

Email flow overview

This section explains the flow or movement of email through a typical email server. This is in respect to your Spam prevention and filtering system, not the SMTP protocol or agent.

1. The first stage is the email server it's self – the program that sends and receives email over the Internet. The server will check that the email is in the correct format, sent using the correct protocol, a proper hand-shake was used, checked for matches against the RBL(s), checked against legitimate and illegitimate destinations and checked for legitimate and illegitimate attachments.
2. The email is passed to a filter system where it is assessed for Spam-like-characteristics. Such characteristics include; black and white lists (a white list is the opposite of a black list. A white list assigns a negative score to the email forcing it to be legitimate regardless of its Spam-like-characteristics), common Spam words and phrase matches, time variances and header checks (destination and source).
 1. Before or after Spam characteristics are assessed, the email server may also pass the incoming email through an anti-virus process. Generally, if a virus is detected, the email is simply removed. Depending on the configuration of the anti-virus process, the intended recipient and/or the sender may be notified of the occurrence.
3. Finally the email is passed to the Inbox of the recipient ready to be collected by the recipients email program. At this point the recipient may apply their own filter (on collection of the new email) to this email using their local email applications filter features. For example, Microsoft Outlook and Mozilla Thunderbird both allow for filtering email based on header fields and file the filtered email into an appropriate folder.
 1. If a learning system is being used, the received email can be forwarded back to the email server from the recipient as either Spam or Ham. This is a process that will help

the servers filter system compare legitimate email to illegitimate email and thereby influencing future Spam detection.

Assessing anti-Spam effectiveness

Effective Spam prevention relies on tracking, monitoring and assessing email logs and thereby assessing the effectiveness of your strategy. Email servers will log all passing emails and what action was applied to them.

There are plenty of log analysis tools that will show you what percentage of emails passing through your email server is marked as Spam, Ham and rejected.

Assess the statistics of your email server before applying the practices of this book. Do the same periodically to assess the effectiveness of your strategy.

Consider that around 97% of email passing over the Internet is Spam. You should therefore expect to reject 97% of emails coming into your email server. A realistic view is to expect to reject between 50% and 75% of your incoming email.

Between 10% and 20% of emails will be filtered with a Spam match. Hopefully the result will be within 5% false-positive either side of perfect.

RBLs and Reporting Spam

You have options to report Spam to RBL organisations. Those same RBL organisations are available for you to subscribe to in your attempt to reject Spam emails as detailed earlier in this book.

RBLs do change and you should be vigilant of such changes. Subscribe to at least three RBLs. A rule of thumb is to require a match from at least two RBLs before a rejection takes place. It's not unusual to block valid domains based on an RBL error. Therefore requiring at least two RBL matches before a rejection is good practice.

Spam in business

Businesses can do plenty to lower their incoming Spam before having to deal with servers, firewalls and spam filters. Such practices include:

1. Replacing email addresses on websites with submission or contact forms. Those submission forms should use human-verification features.
2. Replacing email address on websites with images.
3. Replacing traditional email address formatting on websites with alternatives such as “info at mybusiness dot com” to replace “info@mybusiness.com”.
4. Avoidance of common email prefixes such as sales@, info@, etc.

These are all valid in the attempt to hide or conceal true email addresses from spammers. However, they do suggest a change in business practice which may not be acceptable to the

business in question. For example, a Marketing or Sales department do not necessarily want to hide their email addresses as they rely on the greatest possible exposure to maximise sales. Those same people may accept a higher level of incoming Spam when compared to the accounting department.

For this reason we should accept that the above considerations are for business managers more so than the technician who is there to support the business rather than dictate it.

Summary

There is plenty the I.T administrator can do to minimise Spam passing through email servers which they are responsible for. The tools are there, the best practices are known and promoted and the I.T administrator must realise that end users should be involved in the process.

Combining all of the techniques in this white-paper will give you a great position in the fight against Spam. In fact there are firewall devices that will assist in the process by blocking and filtering Spam which will make your life (as the I.T administrator) much simpler. However, these systems only work as well as they are taught. That is, a good anti-Spam strategy must include a learning system and the best learning system is a combination of the end user and automated systems based on professionally designed learning techniques.