White Paper: Eliminating the Spam Scourge

Andrew Gilhooley
6th July, 2007

Spam, or unsolicited e-Mail has become a real problem over the last two years. At the time of writing, over 95% of all e-Mails we handle are identified as unsolicited. Despite the best efforts of various governments to control the problem through legislation, the level of undesireable e-Mails remains relatively constant.

If your e-Mail inbox is overwhelmed each morning, read on!

Why do they do it?

At the end of the day, it's a simple numbers game. Sending a single e-Mail costs nothing. Sending a million e-Mails costs nothing. If only 0.01% of recipients act on the e-Mail, that's 100 new customers. It isn't ethical, but that 0.01% make it worthwhile for the spammer, whilst giving the rest of us a headache.

How do they operate?

The first thing a spammer must do is obtain a list of e-Mail addresses. These are traded over the internet, and are not difficult to obtain. Remember that sending an e-Mail costs nothing? If a spammer has a list of a million e-Mail addresses, and only half of those work, that's still 500,000 working e-Mail addresses, so even at a 0.01% conversion rate, that's still 50 new customers.

It's not a good idea for a spammer to send a million junk e-Mails through their internet service provider. That kind of behaviour gets noticed. Spammers use "bot-nets" to do the work for them. These are collections of compromised computers, which unbeknown to their owners have become infected with something similar to a virus. The "bot" software is remote-controlled by the spammer, and can be programmed to perform whatever tasks are required. These methods render the spammer essentially untraceable.

Bespoke Software • Custom **Databases** • Stock Control • Invoicing • Payroll • **Technical** Applications • Legacy Application Support • Training
On-Site **Support** • Telephone Support • **Remote** Support • **Maintenance** Contracts • **Pro-Active** Services • **Repairs** & **Upgrades** • **Security** • Firewalls
Anti-**Virus** • Anti-**Malware** • **Spam** Filtering • Web **Design** • **Dynamic** Content • Web Hosting • Domain Registrations • **Internet** Access
Broadband • Modems • Shared **Fax** • **Printing** & Imaging • File **Servers** • Print Servers • **e-Mail** Servers • Web Servers • **Linux**
Microsoft • Small Business Server • **Exchange** Server • Windows Vista • **Windows** 2003 • Windows XP • Windows 2000
Windows NT • Windows 95/98/ME • Windows 3.1 • MS-DOS • **Novell** Netware • Sage Accounts • **Sage** Payroll
Desktop PCs • Workstations • **Mobile** Computing • **Network** Cabling • Hubs & Switches • Routers • **Wireless** • VPNs
VoIP • Tape Drives & **Backup** • Disaster **Recovery** • Business Continuity • Off-Site Media Storage

Registered in England and Wales Number 4259976 VAT Registration Number 789 1096 77

1T Solutions Limited
Haselton House, 3 The Crescent
Doncaster Road, ROTHERHAM
South Yorkshire S65 1NL

www.1t-s.com

Can it be stopped?

The first thing to understand is that there is no way to eliminate every single item of junk e-Mail without also eliminating some legitimate mail. The best that can be done is to reduce the problem down to a level which is easily manageable.

Unfortunately, once your e-Mail address is on a list, there is very little that can be done to remove it. The only options are to deal with the spam, or change your e-Mail address, although this is usually the very last resort.

Dealing with the Spam

Never under any circumstances reply to a message asking them to remove you, or click any link marked "Remove" within any e-Mail unless you are completely comfortable that the sender is legitimate. Responding to unsolicited e-Mail is a sure-fire way of identifying your e-Mail address as being active to the spammer. All that will be achieved is the delivery of yet more unsolicited e-Mail to your inbox.

A certain degree of paranoia can be quite healthy when dealing with e-Mail. Things can often be more than they appear, and it can take a great deal of skill and experience to determine if an e-Mail is legitimate or not. Spammers are becoming more creative, and even the most hardended IT guru can still be hoodwinked.

Software is available to help deal with the problem. Elimination of unsolicited e-Mail follows two main techniques:

- **Passive Filtering**
  This is by far the most effective method, and bizzarely it is the least widely used. It operates on the principle that the "bot" software is required to send out as many e-Mails as possible, ignoring any error states which may be generated. The passive filter operates by generating a false error, forcing the sender to try again. A legitimate e-Mail coming from a real person will handle any error conditions, exhaustively trying a number of different methods to deliver the message. The "bot" software simply moves onto the next recipient in it's list.

- **Active Filtering**
  This involves examining each e-Mail in detail, checking it against a database of known unsolicited messages. Matching e-Mails are tagged as "Junk" and filed according to whatever rules are configured.
  More advanced filters use distributed databases, scoring systems, and automated pattern matching to identify unsolicited e-Mails.

Unsolicited e-Mail can be filtered at a number of different levels:

- **Client-Based Filtering**
  This is the simplest method, only making use of Active Filtering methods. Software is installed on your PC, which hooks into your e-Mail client software (eg. Outlook Express, Mozilla Thunderbird, etc.). This method requires some time and effort on the part of the end-user to "train" the filtering software, but spammers have a number of methods at their disposal to bypass these identification methods.
  Despite this drawback, Client-Based Filtering is still the best option for organisations only operating a small number of PCs, and where the volume of unsolicited e-Mail has not become totally out of control.

- **Host-Based Filtering**
  Most internet service providers apply some kind of host-based filtering on their e-Mail servers. Unfortunately, due to the nature of their business they cannot be too aggressive in dealing with the unsolicited e-Mail for fear of blocking legitimate messages.
  As a business, if you operate your own e-Mail server, filtering software can be installed, similar to Client-Based Filtering, although more advanced facilities are available on an e-Mail server. The level of protection depends very much on the methods employed by the filtering software.
  The major problem with this method comes from the denial-of-service attack, where the spammer targets your e-Mail server with such a huge volume of messages that it is unable to cope, and performance slows to a crawl.

- **Remote Filtering**
  This method removes all responsibility for unsolicited e-Mail filtering away from the core business systems. e-Mail filtering is handled by a system which is designed to eliminate spam and remove viruses.
  As with Host-Based Filtering, the level of protection depends very much on the methods employed by the filtering software, but the denial-of-service threat is greatly reduced as the system is designed to cope with such threats.
  Operationally, a business can host their own spam filtering system, subscribing to an update service. Alternatively a managed service can be purchased from a shared facility.

What can 1T Solutions do to help?

We have a number of offerings to help eliminate unsolicited e-Mail.

Our primary product is ***Gatekeeper***, a Remote Filtering system, which uses two distinct methods of passive filtering in combination with active filtering and anti-virus to eliminate the vast majority of unsolicited e-Mail. ***Gatekeeper***'s Active

Filtering component integrates several distributed databases, and contains over 2,200 individual rules. At the time of writing, the ***Gatekeeper*** system has blocked over **6.6 million** unsolicited e-Mails.

Gatekeeper can be purchased as a shared managed service, or a ***Gatekeeper Server*** can be deployed at your premises, with a subscription to the updates.

Due to denial-of-service issues, we generally do not recommend Host-Based Filtering unless there are strong technical reasons to do so. For customers operating their own e-Mail server, the ***Gatekeeper*** service is usually the most effective option.

For Client-Based Filtering, we recommend

** WHO ARE WE GOING TO GO WITH FOR CLIENT AND HOST PROTECTION?

NOT SYMANTEC/NORTON OR MCAFEE!!!
Not too happy with AVG either – that broke at Stuma.
Sophos is too expensive
F-Secure is more of a corporate thing

That leaves us with:

http://www.avira.com
Premium Security Suite AV / firewall / antispam / antiphishing
£30 / 1 year (£4.50)
£45 / 2 year (£6.75)
15% commission

http://www.kaspersky.com
Internet Security 6.0 AV / firewall / antispam / antiphishing
£40 / 1 year (£8.00)
£55 / 2 year (£11.00)
20% commssion