

Jupiter

Information Technology

A Strategy for Dealing With Spam

27 September 2006

18 Church St
Swansea. SA4 3EA
United Kingdom

+44 (0)1792 875340
info@jup-it-er.co.uk
www.jup-it-er.co.uk

1. Summary

Spam, or unsolicited commercial e-mail, is a large and growing problem. This document presents a methodology for managing spam that should be effective for individuals and small businesses and organisations. The principles can also be applied to larger organisations. A useful by-product of this methodology is that it also provides a method for managing all received email messages. Reasons why spam should be avoided are also discussed.

2. What is spam?

Spam is generally defined as Unsolicited Commercial E-Mail. These days that is not necessarily the case, although it is certainly unsolicited and it is e-mail. Characteristically, spam is usually sent to a large number of recipients, typically thousands, and is invariably unwanted and unasked for.

In many countries spam is recognised as a nuisance and laws have been and are being drawn up to try and deal with it. However, spammers are often hard to find, so although laws exist in many countries, they are largely ineffective.

Spam is cheap to distribute. The spammers can send thousands of emails at very little cost to themselves. The costs of spam are borne by the recipient who has to pay for internet connections and bandwidth, disk space and time in dealing with the problem.

3. What is wrong with spam?

Apart from the kind of e-mail that tries to sell us something we don't want, there is a class of spam that uses trickery to get the recipient to do something they don't want to do.

This class can be further subdivided into two sub-classes, although the distinction is now becoming increasingly blurred.

Much spam either carries malicious software, or provides links to web sites where malicious software can be downloaded to a computer without the users permission or knowledge.

So the first sub-class is spam acting as a vehicle to distribute malicious software.

The second sub-class is spam that tries to induce the recipient into divulging financial or other information. So, this is spam as a vehicle for perpetrating cyber crime.

As the whole *raison d'être* for malicious software seems to have shifted away from kids 'larking about' to criminal activity, we can safely ignore the sub-classes for now.

Malicious software includes viruses, worms, Trojans, (ro)bots, etc., and these are increasingly being used, singly or collectively, to gather personal or financial information from affected computers. This information is then transmitted to the person or group who sent the spam in the first place.

Typical criminal spam includes phishing attacks and Nigerian 419 scams, amongst others.

The objective of the senders is to get your money. Further information about phishing can be found on <http://www.antiphishing.org/>, while an interesting analysis of an actual Nigerian 419 scam can be found at http://www.theregister.co.uk/2004/07/09/419_scam_anatomy/print.html.

4. Minimising the chances of getting spam

Some people seem to receive a lot more spam than others. The more spam you get, the greater your chances of getting infected with malicious software. As a side note, malicious software never infects in isolation, or singly. If you have one infection, then you also have other infections. The worst case we have seen was a computer infected by 7000 plus distinct instances of malware.

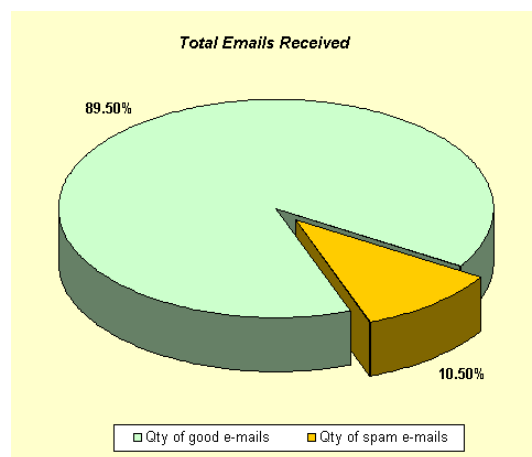
Also, the more spam you get, the more it is costing you in terms of internet bandwidth consumed, time in dealing with spam and its effects, and wasted computer resources.

As an example of how much time and resources are wasted, over a period of 498 days 10.5% of all Jupiter Information Technology's received e-mail was spam. That's a large slice, by any standards.

When you purchase goods online, you are often required to give your e-mail address.

This is useful initially, as it means that a company can send acknowledgments of your order, and notify you when your order is being despatched, etc.

However, many companies then send you a constant barrage of spam under the mistaken belief that you actually want all this stuff. After all,



you gave them your e-mail address and they construe that as consent to receive spam from them.

In addition, by subscribing to one set of spam you are leaving the door open to receiving spam from other companies. This is because e-mail address lists are actively marketed and sold.

Obviously, you want to purchase goods online. And why not? First, though, set up a throw away e-mail account with a free provider such as Yahoo or Hotmail. Then use this e-mail address when registering with the online store.

At the bottom of the e-mail it often invites you to unsubscribe. Do not be tempted. Never unsubscribe from unsolicited e-mails. Many are sent speculatively, and unsubscribing confirms your e-mail address is live and active.

There is only one way to deal with spam. Delete it. Do not respond to it. Do not read it, and do not click on any links.

Some people complain to the ISP where the e-mail originated from, but even if the source ISP is genuine, it would seem that many (not all) ISP's are friendly to spammers, so you end up with more spam. The cycle repeats, endlessly, until your inbox is filled with spam.

5. Simple E-Mail filtering

It is possible to filter all your incoming emails, so that all your email is organised. Most email software has a facility for creating folders and filters or rules. Once your email messages are organised, then it becomes easier to see what has just arrived, and it also becomes easier to see suspicious email. This is a good enough reason to organise, by itself.

All my email is filtered, and my objective is always to have an empty inbox. If a message stays in the inbox after filtering, then it is automatically suspect, and is treated with caution.

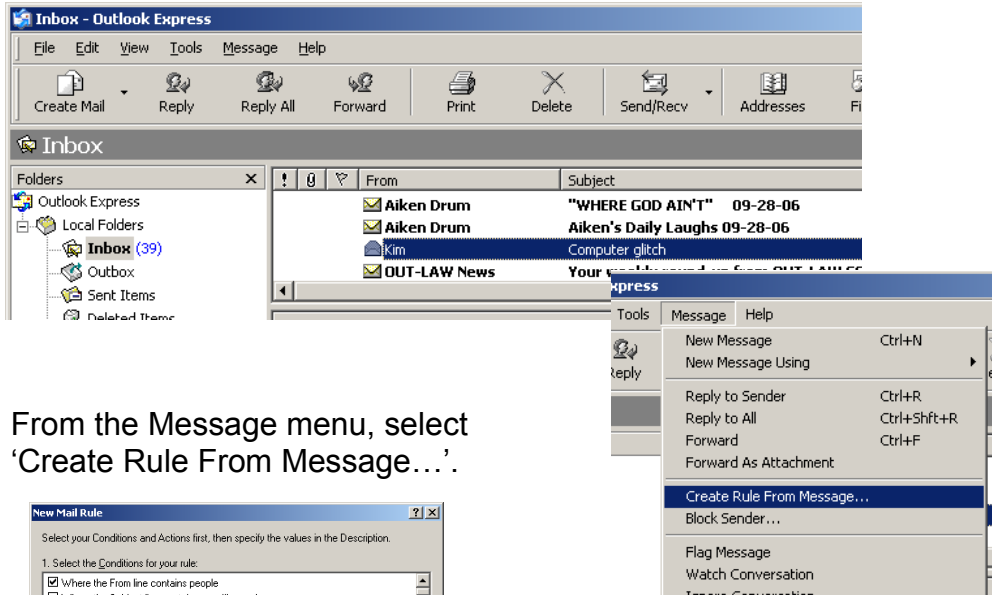
By organising and filing it is also easy to prioritise messages, according to your own preferences. If, like most people, your inbox is full of unsorted messages, how can you identify suspicious mail or prioritise your tasks?

Unfortunately, most spam is not able to be filtered in this way. This is because spammers use various tricks to bypass simple filtering. However, by filtering what we can filter, the remainder is most likely to be spam.

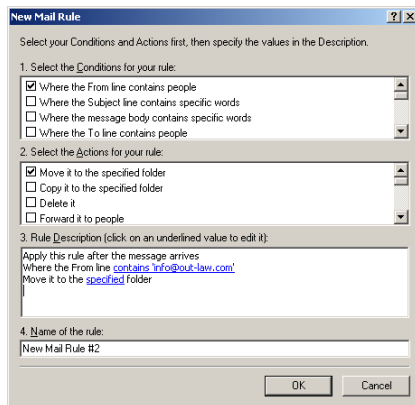
Check before deleting, though. There may be an important message there from someone who hasn't made it into your filtered list yet.

Examples could be an online order notification, or a friend who has changed their e-mail address.

In Outlook Express highlight a message header.



From the Message menu, select 'Create Rule From Message...'.



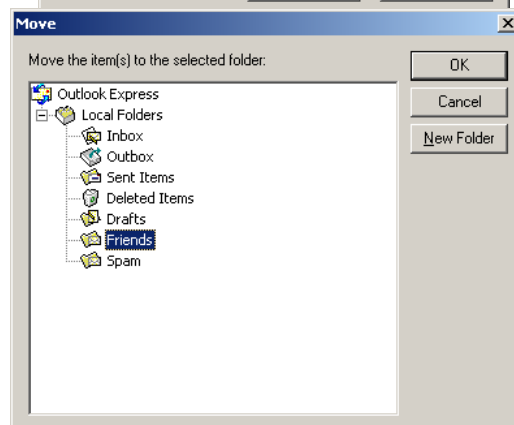
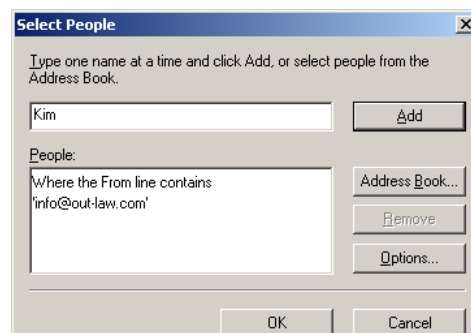
The 'New Mail Rule' dialog box will be displayed. Specify the condition for the rule. For example, if the sender is someone you know, select the first option, 'Where the From line contains people'.

Now, if it's a friend then we probably want to move it to a 'Friends' folder, so tick 'Move it to the specified folder' in the 'Actions' window.

As we build up the rule, we see a description being formed in the 'Description' window. If you click on the blue underlined text, you can further edit each part of the rule.

Type the name of the person you want to add to the rule, then click 'Add'.

Repeat the process for the other parts of the rule as desired.



Now whenever mail from this person is received it will automatically be moved to the Friends folder.

It's as easy as that, and will reap great benefits by itself.

6. Further filtering using third party tools

One of the great problems with simple filtering to trap spam, is that there is always a hard core of spam messages that will defy any attempt to filter in this way. This is because the spammers have become very good at bypassing filters. With a simple filter you can only deal with messages you already know something about, such as messages from friends and family, or messages from a newsletter that you have signed up to. It is very difficult to create rules that catch apparently unique messages.

This is where spam filtering software comes in. Spam filtering software use a few different methods to trap spam. Some use 'whitelists' and 'blacklists' to identify spam. A 'blacklist' is a list of senders from whom we do not want to receive e-mail messages, and a 'whitelist' is a list of senders from whom we do want to receive messages.

The list concept is not too different from the simple filtering that we employed above, and if you have a web mail account that offers spam filtering, then it will probably use 'blacklists' and 'whitelists'.

Other spam filtering software will use statistical analysis of each message to decide whether it is spam or not. After analysis the message is given a probability score to determine whether it is spam or not. This method is called Bayesian filtering and works very well. Usually, there is a small amount of time before the software becomes fully effective, as it has to 'learn' what you consider to be spam. The more it is used, the greater the effectiveness.

It's the Bayesian type of spam filter software that I will concentrate on, as I consider them to be most effective and convenient in use.

There are two main contenders. These are K9 (<http://keir.net>) and Mailwasher (<http://www.mailwasher.net/>).

Both are easy to setup and use, and each has different strengths and weaknesses. K9 is completely free. Mailwasher is downloaded as a free 30 day trial, and is feature limited. To take advantage of it's other features you need to upgrade to the Pro version.

K9 has the ability to automatically configure itself to work with Outlook Express. Just click the appropriate button under 'Advanced' settings tab and it will do all the hard work.

URL's

Anti Phishing Working Group

<http://www.antiphishing.org/>

Anatomy of a Nigerian 419 scam

http://www.theregister.co.uk/2004/07/09/419_scam_anatomy/print.html

K9 Software

<http://keir.net>

Mailwasher Software

<http://www.mailwasher.net/>