

# Hate spam as much as we do?

## What is “spam”?

Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it.

E-mail spam targets individual users with direct mail messages. E-mail spam lists are often created by scanning Usenet postings, stealing Internet mailing lists, or searching the Web for addresses.

In many cases, spam will appear merely as unwanted commercial e-mail – junk e-mail advertising – albeit at times advertising some fairly dubious products (e.g. offers to sell prescription drugs).

However more recently, a substantial volume of spam has proven to be considerably less innocuous – unsolicited e-mail frequently includes: computer viruses, attempts to defraud its recipients, extreme pornography, and other objectionable material.

Perhaps more objectionable than its content, is the volume of spam. Receiving one or two such messages a day is annoying. Receiving hundreds of them is a genuine drain on your time and resources, and one you should not have to put up with. Finding several hundred messages from idiots in your IN box every morning is a problem, no matter what they're actually trying to sell you.

Your e-mail is just that – yours. In most cases, it's a resource that you must pay for as part of the cost of connecting to the Internet. Reading and responding to your e-mail also represents an investment of your time, and as such has a value attached to it.

If someone sends you junk mail through your e-mail account, they're wasting your time and money.

## How to manage “spam”

A quick search of the Internet will reveal a wide range of ‘spam-buster’ products. In this guide we concentrate on a few that we have found to be effective.

Broadly, anti-spam products fall into one of two categories:

1. Spam Filters OR;
2. Permission based e-mail system

Each approach has its strength and weaknesses.

### Spam Filters

The traditional approach to dealing with spam has been to ‘filter’ incoming e-mail against several rules (e.g. sender, sender’s e-mail server, keywords in message subject, keywords in the body of the message) to determine whether a message is likely to be spam.

Typically points are assigned to each rule, if a message accumulates enough points then it is classified as spam.

You can add e-mail addresses to your Safe Senders List (or “whitelist”) to ensure that messages from these senders will never be treated as junk e-mail, and you can block messages from other e-mail addresses (and/or domain names) by adding the sender to your Blocked Sender List (or “blacklist”).

With spam filters all incoming mail is delivered to your inbox unless the filter determines the message to be spam. Thus a clever (or devious) spammer will try to create e-mail messages that will beat the spam filters rules and reach your inbox.

MDaemon (<http://www.altm.com>) a fully-fledged mail server that includes a spam-blocker as well as anti-virus and Outlook 2003’s Junk E-mail Filter are examples of spam filters.

## Permission-based e-mail system

ChoiceMail (<http://www.digiportal.com>) is an example of a permission-based mail system. ChoiceMail assumes that any incoming e-mail is spam unless it knows otherwise. Only approved e-mail reaches your inbox.

- ChoiceMail (CM) creates a “whitelist” of all the e-mail addresses in your address book. Every time you send a message to someone new, CM adds them to the list, so it is always up-to-date.
- CM sends e-mail from anyone on your whitelist straight to your inbox. You can also write rules to accept e-mail that you may want, even from people that are not on your whitelist. (If cycling is your passion, simply tell CM to accept any message containing the word “cycling” and it will.)
- CM contains tools that let you send obvious spam straight to the junk box. Unlike spam filters, these tools are not the whole product – just an enhancement to make your life easier. You can also write your own rules to block mail if you wish.

ChoiceMail then “holds” any remaining e-mail from unrecognised new senders and uses a challenge/response system to block spam by sending a reply e-mail to any new senders, asking them to verify their identities.

Each unknown sender is automatically sent a “registration request” that directs them to a web page where they are asked for their name, email address and their reason for contacting you. They also are asked to complete a task, which is easy for a person but impossible for a computer.

This process eliminates most junk email because spammers won't go through this process, thus ChoiceMail won't forward their spam to you.

When a sender does register, ChoiceMail alerts you with a pop-up message. You can then decide whether to allow the sender to communicate with you or not.



The challenge/response system is both ChoiceMail's strength and its weakness. Some first-time contacts may not like the extra step of having to confirm their identity before they can e-mail you, even though they will only have to do it once.

If you're in a sales role (for instance Real Estate) you would expect to receive 'unsolicited' e-mail from new clients looking to either purchase or sell property. You may not want these people to receive a "challenge" from ChoiceMail. There are a couple of options:

1. Create rules with keywords (e.g. 'buy', 'sell' and other words that frequently appear in e-mails from new clients) to allow any messages with those keywords to automatically be accepted.
2. At any time you can review the e-mail messages that ChoiceMail is "holding" as unknown. You can manually accept messages that are from new clients even though they may not have responded to ChoiceMail's challenge (by default ChoiceMail holds unknown messages for 4 days – but you can change this period).
3. If you don't want new clients to receive a "challenge" under any circumstance, then ChoiceMail is not the right solution for you. Instead you should rely on a Spam Filter such as MDAemon to manage your spam.

ChoiceMail does a great job of blocking unwanted spam, although new correspondents will have to take an extra step before they can e-mail you for the first time.

## Implementation

ChoiceMail has different versions depending on your mail environment:

Version	Price
▪ ChoiceMail Free	<b>FREE</b>
Recommended for single users with one POP3 e-mail account (that's right it is FREE – an excellent choice for use at home).	
Can be installed by the end user.	
▪ ChoiceMail One	<b>\$60ex per copy</b>
Recommended for single users with multiple e-mail accounts or who want to protect AOL, Yahoo, MSN, or Hotmail accounts).	
Can be installed by the end user.	
▪ ChoiceMail SmallBusiness	<b>Depends on the number of users</b>
Provides protection for organisations that do not operate their own mail server (typically worth considering when you have more than 5 users).	
Depends on the number of users, typically ½ - 1 day to implement.	
▪ ChoiceMail Enterprise	<b>Depends on the number of users</b>
Works with Exchange, GroupWise, Domino and more.	
Depends on the number of users, typically ½ - 1 day to implement.	



MDaemon is a fully-fledged mail server, but because it includes anti-virus and spam-blocker features we frequently implement MDaemon in conjunction with other mail servers (e.g. Exchange) to provide two levels of protection against e-mail borne viruses which in recent times have become very prevalent (and destructive if they are not detected).

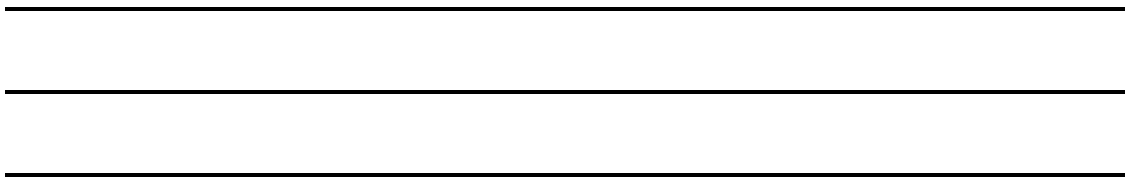
MDaemon with Anti-virus **\$650ex**

(includes 12 months virus definition updates)

Installation and configuration will be completed in ½ day.

MDaemon with Anti-virus and Spam Blocker **\$1,150ex**

Initial installation and configuration will be completed in 1 day, typically there is then tailoring of the spam filters to “suit” the spam of the organisation on an ad-hoc basis post-implementation.



Zero Effort Networking (ZEN) is experienced in accurately identifying computer network problems and acting swiftly to fix them. Since 1996 we have helped clients implement stable, reliable computer networks that take the worry out of network management. For further information you are welcome to contact us.

Zero Effort Networking Pty Ltd  
ABN: 38 082 434 446  
Telephone: 02 9676 3541  
Facsimile: 02 8569 2012  
E-mail: [info@zeroeffortnetworking.com.au](mailto:info@zeroeffortnetworking.com.au)  
Web: [www.zeroeffortnetworking.com.au](http://www.zeroeffortnetworking.com.au)  
Office: Suite 15, 18 Third Avenue, Blacktown NSW 2148

No part of this publication may be reproduced without written permission of the authors. Copying and distribution by any means is strictly forbidden. Additional copies may be obtained for free by contacting Zero Effort Networking.