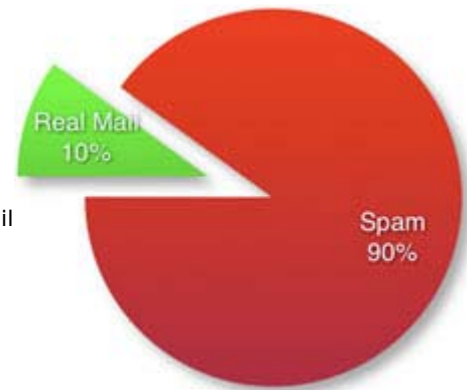


## Effective Spam Filtering

For most average Internet Service Providers and networks in North America, Europe or Australasia, today's incoming email traffic consists of approximately 90% spam and 10% normal legitimate email. [1]

The main problem for mail system administrators is how to filter out the spam while not losing legitimate email, and how to keep mail queues flowing without spam-filter processes slowing the mail queue.

The main problem for ISP executives is also how to do this cost-effectively.

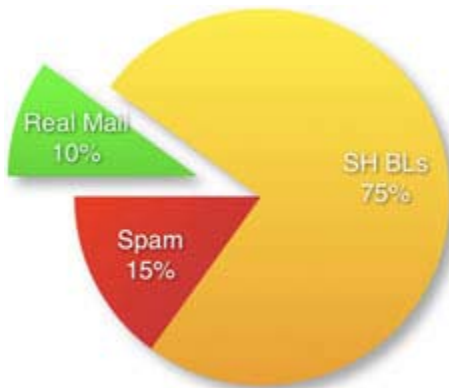


### 2-Stage Filtering

Using only the Spamhaus DNS-based Blocklists (SBL, XBL and PBL) ISPs and internet networks can very safely reject 75% of inbound mail traffic outright, rejecting the vast majority of spam at SMTP connect time and before mail servers are burdened with it, or have to process or accept the messages.

Remaining spam that gets past the Spamhaus blocklist checks at SMTP connect time, should then be filtered by checking the IP addresses of web sites advertised in the spam against the SBL in a second stage called "URI SBL". [2]

Using the setup described below, UK ISP uxn.com achieves a catch rate of 299 out of every 300 spams (99.6%) with zero false positives.



#### 1st Stage

The first stage is to install the Spamhaus [ZEN](#) blocklist on your incoming mail relay(s). ZEN, which is a combination of Spamhaus's SBL, XBL and PBL blocklists, will identify and reject 75% of a normal mail relay's incoming mail traffic.

Incoming mail from servers listed on SBL, XBL or PBL at this first stage should be rejected at the RCPT TO command, terminating the SMTP transaction before the message body is accepted, sent or received.

This is cost effective - more than halving your incoming mail bandwidth and the subsequent mail queue - and is the safe way to handle message filtering, because in the event a legitimate Sender is ever blocked in error

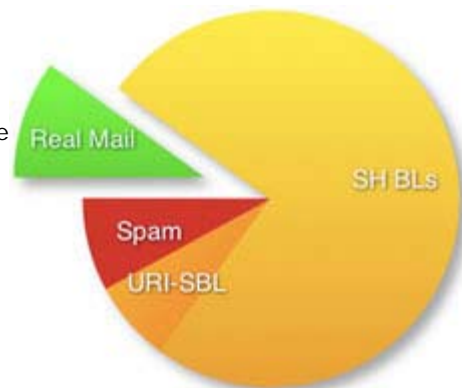
they are immediately notified by the reject notice of the reason why their message could not be delivered as well as what to do and who to contact about it. [3]

## 2nd Stage

Over 60% of spam contains URLs of spammer web sites whose webserver IPs are listed on the Spamhaus SBL. [4] Therefore the second stage is to scan the 25% of mail which gets past first stage IP filtering, looking for URIs (web site addresses) in the message body and testing their host IPs against the SBL.

This is done by installing an application capable of scanning message bodies for URLs and checking them against the SBL.

There are a number of free/open source applications - such as SpamAssassin, SpamBouncer, and there is also a free Sendmail filter with this feature.



If using SpamAssassin, we recommend you increase the value of SpamAssassin's SBL-check feature, **URIBL\_SBL** to at least 5 or 6 (by default it's set to 1 which in most cases is too low to trigger the spam flag).

Spamhaus lists the IPs of spammers' web servers and DNS servers, in addition to spam sources in the SBL for this purpose. Spammers may find fresh sources not yet on our DNSBLs, but they in most cases need to advertize a web site hosted somewhere.

Remaining spam, which should now be reduced to less than 7% of your total incoming email traffic, is taken care of easily by SpamAssassin's other filter components, including SURBL, with the result that the total spam catch rate should now average 99.6%, or 299 in every 300 spams.

---

1] Many large providers report the numbers are greater than 90% spam, some as high as 95%.

[2] URIBL\_SBL ref: [http://spamassassin.apache.org/full/3.0.x/dist/rules/25\\_uribl.cf](http://spamassassin.apache.org/full/3.0.x/dist/rules/25_uribl.cf)

[3] The Spamhaus DNSBLs return a text message (TXT) on a positive hit, giving the URL to the precise record page explaining why the IP is listed and who to contact to get the issue resolved. The Spamhaus XBL and PBL DNSBLs allow end-users to remove their own addresses from the blocklist.

[4] URL on SBL: Out of a sample of 860 spams tested by Spamhaus in March 2007 using the "URIBL\_SBL" feature in SpamAssassin 3.0, 612 (equal to 71%) contained urls of spammer web sites whose IPs were listed on the SBL.

## About Spamhaus

Spamhaus is an international non-profit organization whose mission is to track the Internet's Spam Gangs, to provide dependable realtime anti-spam protection for Internet networks, to work with Law Enforcement Agencies to identify and pursue spammers worldwide, and to lobby governments for effective anti-spam legislation. Founded in 1998, Spamhaus is based in Geneva, Switzerland and London, UK and is run by a dedicated team of 25 investigators and forensics specialists located in 10 countries.

## About MX Tools

MX Tools, provides reliable, fully-supported e-mail anti-abuse tools - including sales and dedicated technical support for the world's most widely used and highly regarded blocklists - Spamhaus and SURBL. Our direct access to the backline technical teams and our interaction with key customers globally, enable us with a global best practices view into how email tools and solutions are designed and deployed for all email platforms. Thousands of customers across the globe - including the world's leading organizations - rely on the solutions and support delivered by MX Tools. [www.mxtools.com](http://www.mxtools.com)