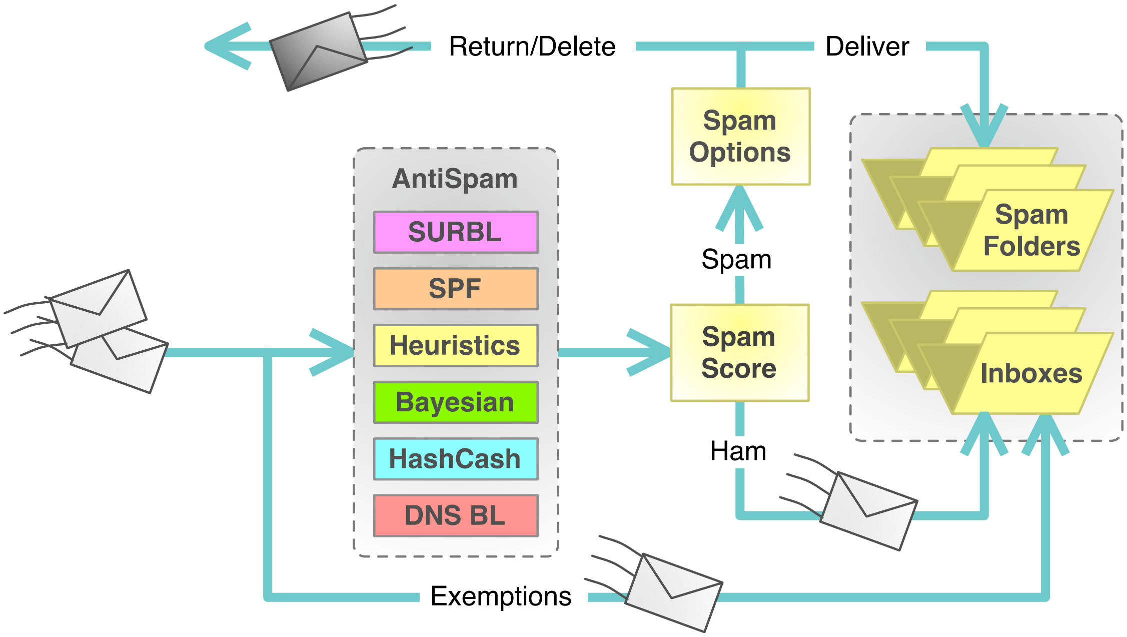
AntiSpam Tools in MDaemon

Between 50 to 60% of all Internet email traffic is spam—that is, the email messages arrive both unsolicited and unwanted.

Spam is the cholesterol of the internet. It clogs bandwidth and hinders the delivery of legitimate communications. Yet, enough recipients respond to the uninvited offers to make spamming profitable.

For the majority of people, spam brings mostly trouble, costing them billions worldwide in wasted bandwidth, lost computer processing power and consumed disk storage space. When uncontrolled, spam also devours the time needed to review and discard the messages.

If you want to avoid the wastefulness of unsolicited messages, MDaemon offers a variety of AntiSpam tools. While no single method stops spam by itself, the combined capabilities of MDaemon's AntiSpam tools can reduce unwanted messages to a trickle.



Reducing Spam Without Deleting Ham

AntiSpam Limitations and Sensible Defaults

The human mind is by far the best spam filter. You can usually pick out spam by viewing the sender name or the subject line. While no spam fighting technology can achieve that level of accuracy, MDaemon AntiSpam comes close.

Using their default settings, the AntiSpam tools can detect 80-95% of spam without falsely labeling ham—that is, legitimate messages. The point is this: an MDaemon beginner can confidently enable AntiSpam with little worry of losing valid messages.

If you later want to tweak the settings, most of the AntiSpam tools come with multiple configuration options to help detect, mark, quarantine and eliminate spam.

How Spammers Make a Profit

Spam exists because one-in-a-thousand to one-in-a-million people respond to the messages. While the replies are few, spammers can easily email to millions each day, making profits from those who buy. Financial rewards come to spammers because they pay almost nothing for sending their massive emailings. Instead, the expense of spam transmission is pushed out to the companies who run the Internet and the individuals who receive the email messages.

Spammers' Methods of Operation

Spammers send their messages through SMTP email servers the same as everyone else. However, they often use stealth to keep operating. They regularly switch email servers, using various internet service providers, local servers on their own computers, open relay servers on the Internet, free email services and hijacked personal computers.

Because they are constantly on the move, spammers are difficult to track down and stop at their source.

Spam Scores and Spam Processing Options

In operation, MDaemon AntiSpam assigns spam scores to each incoming message. Each AntiSpam tool can either add to or subtract from the score of each email. When the spam score of an email reaches a threshold level, AntiSpam marks the message as spam.

Once a message is designated as spam, it can be bounced back to the sender, deleted, sent to a public spam folder or processed as normal through the content filter and on to the recipient.

The content filter can perform multiple functions on spam, such as adding a warning to the subject line. For email users with IMAP and webmail capabilities, the spam can be placed in account-specific spam folders.

DNS Black Lists

One of the primary ways to help detect spam is by comparing the email sender addresses against publicly-available black lists of known spammers or open relay servers. (An open relay allows email transmission from any sender to any recipient with no security checks.)

Several web sites maintain these types of lists, known as DNS Black Lists. The lists contain IP addresses of offending email servers. DNS black listing matches the server addresses of incoming messages to the addresses in the black lists. If they match, the messages can be marked as possible spam by raising their spam scores.

The public black listing tool in MDaemon can check multiple lists. Each list uses different criteria for adding and removing email servers. The default black lists supplied with MDaemon have proven themselves to be reliable.

Detecting Spam-Supporting Web Sites

Spammers who use the world wide web to sell their products often change their sending email addresses. They seldom, if ever, change the web sites they use for making sales. A new antispam technology capitalizes on this behavior to help detect spam messages.

The technology is called SURBL, or Spam URI Realtime Blocklists. As implemented in MDaemon, SURBL searches the contents of incoming messages for Uniform Resource Identifiers (URIs). It then compares these with a list of Internet addresses—mostly web sites—known to support spammers.

When an address in an email is associated with spamming, MDaemon can mark the message as possible spam.

Users of SURBL report at least a 20 to 60% reduction in spam by using just this one tool.

Detecting False Identities

Spoofing is the unauthorized use of an email address or domain name. It enables email senders to hide their true identities.

When sending their messages, spammers often spoof their identities by using the names and return addresses of other people. This tactic attempts to trick recipients into opening and responding to emails.

One of the most damaging uses of spoofing is *phishing*. Phishing messages claim to originate from trusted sources such as online payment services, banks, ISPs, government agencies and corporate IT departments, as examples. With identity theft as the goal, the messages ask recipients to update or confirm personal and financial information via email or on official-looking, but fake, web sites.

To help unmask spoofed email addresses, MDaemon uses the Sender Policy Framework (SPF).

SPF is an industry-wide security tool for validating sender addresses. If a sending address appears to be spoofed, the message can be marked as possible spam.

As it becomes more widely implemented, SPF is reducing the amount of spoofing. It has been put in use by thousands of Internet enterprises, including Amazon, AOL, Earthlink, eBay, Google, Hotmail, Microsoft and Symantec.

Checking Messages for Spam-Like Content

MDaemon uses the heuristic technology of *SpamAssassin* to help identify unwanted email messages. Heuristic detection compares emails to multiple pattern-matching rules developed by analyzing millions of spam messages. The rules apply to various parts of an email, including its server address, sender, subject and message. For example, a email message with red HTML text may point to spam.

Heuristic matching applies each rule to each message. Every time a message matches one of the rules, the email receives a score indicating it may be spam. When the score reaches a threshold level, MDaemon can mark the message as possible spam.

MDaemon stays current with changing spam styles by regularly updating its heuristic rules with the newest SpamAssassin content.

During the past several years, heuristic technology has become very reliable in detecting spam without falsely labeling valid messages.

Defining Spam for Yourself

Spam detection becomes even more accurate when the AntiSpam technology can discern the difference between legitimate and unwanted email for individual email servers. In MDaemon, Bayesian classification supplies this type of service.

Locally defining spam by its content is important because spam for one enterprise may be ham for another.

Bayesian classification works by completely analyzing known samples of both types of messages—spam and ham. With this system, authorized users or administrators or both supply the Bayesian software with real-world examples of wanted and unwanted emails.

The Bayesian tool analyzes the complete content of each spam and ham example, then compares this information to new incoming messages. By adding examples everyday, you make the Bayesian software more accurate over time. Given several hundred local examples of each type of message, Bayesian classification is more than 90% accurate on spam, with virtually zero mistakes for ham—the email messages you want to keep.

As part of the Bayesian process, MDaemon sets up separate folders to receive the samples of spam and ham email. The authorized users can add the samples by dragging and dropping them into designated folders. The samples can also be emailed to the Bayesian classifier. Some examples of legitimate messages can be added through totally automated processes.

HashCash Stamps

Because of the very limited response to their offers, spammers need to send their email messages in massive quantities. The faster spammers can send their messages, the more sales they can make.

The emerging technology of *HashCash* inserts electronic “postage stamps” into legitimate email messages. The stamp shows the amount of extra processor work and time put into creating the stamp and sending the message. HashCash slows down the sending of messages, something spammers cannot afford to do.

If widely adapted, HashCashing could add legitimacy to non-spam emails. The higher the HashCash value of the stamp, the more effort that went into sending it, making it more likely to be a legitimate email message.

MDaemon can both create HashCash stamps for sending messages and read the stamps for incoming messages.

Local Black Lists, White Lists and Exclusions

MDaemon’s spam fighting functions have locally controlled black lists, white lists and exemptions.

For the DNS Black List function, addresses included in the white list exempt any incoming messages from processing.

Black list entries for Spam Filtering identify email addresses more likely to be spam sources. Being on a black list does not block messages from that address. Instead, black listing raises the spam score of all messages to block most of them. Only messages with extremely low spam ratings are not marked as spam.

The opposite applies to Spam Filtering white lists. These identify email addresses less likely to be spam sources or destinations. Being on a white list does not exempt an address from AntiSpam processing. Instead white listing adjusts the spam score of all messages to allow most of them to pass. Only messages with extremely high spam ratings are marked a spam.

Exclusions for Spam Filtering designate email addresses exempt from processing. Optionally, emails from addresses stored in local user address books can be exempted from AntiSpam processing.

AntiSpam Tools in MDaemon Features Digest

DNS Black Lists

- Enable DNS Blacking List checking.
- Mark messages from black listed site, but still accept them.
- Check 'received headers' for SMTP or POP collected messages.
- Skip 'received headers' from white listed sites.
- Add, change and delete DNS Black List hosts.
- Cache DNS Black List results for specified durations.
- Exempt white listed sites from processing.

Sender Policy Framework (SPF)

- Enable SPF lookups.
- Process 'from' headers.
- Insert 'received-spf' header into messages.
- Set 'fail' results options.
- Set spam scores for various SPF lookup results.
- Exempt authenticated sessions from SPF lookups.
- Exempt trusted IPs from SPF lookups.
- Cache SPF lookup results.

Spam Filtering

- Set processing options for messages marked as spam.
- Exempt local, trusted and authenticated addresses.
- Skip messages larger than specified size, up to 2 megabytes.
- Don't forward messages marked as spam.
- Automatically place messages in users' IMAP spam folders.
- Set spam score adjustments for black lists and white lists.

Heuristic Analysis

- Enable spam scoring for heuristic processing.
- Set spam threshold for spam scoring.
- Set spam score threshold for rejecting SMTP messages, show heuristic results in SMTP log.
- Edit spam warning subject line for messages marked as spam.

Bayesian Classification

- Apply Bayesian knowledge to heuristic scoring system.
- Enable Bayesian scheduled learning.
- Run Bayesian learning now.
- Set up folders for samples of known spam and know ham.
- Set up reporting options for messages marked as spam.

Reporting Options

- Set up reporting options for messages marked as spam.
- Insert report in headers of original messages.
- Create new message, with original as message/rfc882 MIME attachment.
- Create new message, with original as text/plain MIME attachment.

HashCash

- Mint and insert HashCash stamp into outbound mail.
- Limit HashCash stamping to authenticated SMTP sessions.
- Add, change and delete addresses in Mint List.
- Set mint stamp size.
- Check inbound mail for HashCash stamps.

Black Lists, White Lists, Exclusions

- Add, change and delete addresses for Black Lists, White Lists(to) and White Lists (from)
- Enable address book white listing.
- Enable automatic address updating
- Add white-listed messages to Bayesian ham samples folder.
- Enable white list forwarding address

Alt-N Technologies, Ltd.
2201 East Lamar Blvd, Suite 270
Arlington, Texas 76006
Phone: (817) 525-2005
Fax: (817) 525-2019
http://www.altn.com