Spam

Premium Spam Filtering

There are several articles on the subject of sending, receiving and managing spam. Please refer to the one that fits your needs best:

- **Sending Spam:** What you can and can't do.
- **Spam Prevention Tips:** What you can do about it.
- **Standard Spam Filtering:** What we do for all clients.
- **Premium Spam Filtering:** At modest additional cost. (this article)

- (this article)

For those customers who find that spam is wasting more and more of their time, we are pleased to offer an effective, sophisticated spam and virus filtering service using heuristic filtering methods, Bayesian filtering methods, rules based evaluation, white lists, black lists and other methods to define spam and eliminate it from your life.

The cost is quite reasonable for our hosted clients and a third party filtering service for those who don't host with us is available through our **spam111** service. See our **features** page for pricing details and **contact us** to sign up.

SPAM FILTERING:

Filtering Methods: We use several methods for filtering with message scoring as an evaluation tool. The system decides whether a message is spam based on the number of "points" assigned to it. If a message gets enough points, you can determine it to be spam and it can be discarded or quarantined. You have control over the Delete Value and the Quarantine Value at both the domain and individual levels. Several methods we currently use for assigning points are as follows:

- **A Rules Based Approach** that analyzes headers and message text for certain specific characteristics. Both positive and negative points are assigned based on what is found in the message.
- **A Learning Component** that builds a database of tokens from known spam and known ham (wanted messages). These tokens add extra positive or negative point assignments to messages that have the tokens, thereby increasing the certainty that they are or are not spam. The token database is continually updated based on the content of incoming messages so it keeps "learning" what the spammers are doing.
- **Collaborative Spam-tracking Databases** are used. The system reads a signature of each incoming message and compares it to known spam from several databases. Since spam is typically sent to many people, the first people to receive a spam message can add it to a database -- at which point everyone else will automatically block it.
- **Whitelists** are a lists of addresses known to be non-spam.
- **Blacklists** are a lists of addresses or IP addresses known to be used

for spam.

Custom Interface: The interface to the system allows you to set your own parameters for filtering. You have the ability to set limits on whether to totally discard messages or just quarantine them for some fixed time period. Additionally, you get statistics and graphs showing the amount of spam the system has processed for you and what happened to it.

HOW TO USE THE SYSTEM:

In order to manage your spam settings, review your usage graphs and manage what is in your quarantine, simply log into the **management system**. You can log into the system as postmaster@yourdomain.com to manage the entire domain or as yourmailboxname@yourdomain.com to manage only your own spam. The following options are available:

- **Global Settings** - As you can see from the options below, if the delete score you set is lower than or equal to the quarantine score, no messages will be quarantined.
    - Delete Score: set from 4 to 15 (8 is recommended)
    - Quarantine Score: set from 4 to 15 (5 is a good starting place)
    - Quarantine Days: set from 1 to 14
    - Blacklist Action: Quarantine or Delete
- **My Settings** - These override the global settings.
    - Username: for example jsmith@somewhere.com
    - Full Name: for example Joe Smith
    - Delete Score: 4 to 11
    - Quarantine Score: 4 to 11
    - Quarantine Days: 1 to 14
    - Blacklist Action: Quarantine or Delete
    - Mail Forward: email address to forward all incoming mail to.
    - ***Remote POP Accounts:*** As an ICG Link or Spam111 client, you can use this handy feature to filter mail from external POP accounts using your spam111.com mailbox. So, if you have an account with Comcast, BellSouth or some other ISP, there's no need to live with spam from that mailbox anymore either. When you enter your POP settings, that mail will be filtered and will show up in your spam111 mailbox.
- **White/Blacklist** - White/Blacklisting looks for particular senders or sender domains and will either delete or accept those messages regardless of their content. It is not a particularly effective method of controlling spam, but it may be useful in some pseudo-spam contexts.
    - Whitelist addresses will always pass through the filters
    - Blacklist addresses will not - Adding every spammer's address to your blacklist is probably not worth the time since spammer's will routinely change their From address.
    - Note: If you white or blacklist an entire domain, you do not

have to list any addresses at that domain since it will be covered by the domain rule.

- **Training as Spam or Good** - You have the option of training the system to learn about what's good and what's not.
    - Training and White/Blacklisting are completely separate, and should not be confused.
    - Training a messages will submit it to our training queue, which is now moderated. If you submit a message for training, we will review it and train our spam filter with it if we think it is appropriate. If not we will disregard it. This prevents the filter from getting confused... one man's ham is another man's spam.
    - Submitting quarantined messages for training as spam is not particularly effective, since the messages already scored high. The maximum score our Bayesian filter will attach is 6 points.
    - Submitting quarantined mail as Good will help prevent similar messages from scoring high, and is critical to keeping our false positives to a minimum.
    - More effective for spam training is submitting messages that eluded the quarantine. If you receive messages that you'd like to train as spam, you can send them to **spam@spam111.com** for training.
- **Quarantine**
    - Sort by sender, subject, date or score
    - Delete messages permanently from quarantine.
    - Send messages from your quarantine on to your mailbox or train the system with them.
    - View quarantined messages.
    - Add message senders to White/Blacklists.
- **Usage**
    - Provides statistics and daily & monthly graphs of deleted, quarantined and sent mail.

VIRUS SCANNING:

All incoming and outgoing email messages that pass through our servers are scanned using Clam AntiVirus. Virus definitions are updated every 4 hours. Virus definition tables are kept up to date and are based on the OpenAntiVirus database along with additional signatures including those for popular polymorphic viruses and some of our own enhancements. Any message having an attachment with the .vbs, .lnk, .scr, .wsh, .hta or .pif extensions will have the attachment stripped from the message before delivery.

HARDWARE SYSTEMS:

Spam

Multiple dual CPU servers are in place whose sole purpose in life is to perform virus and spam tagging & filtering. The system is designed in a modular fashion such that machines can be added to compensate for growth. There is always at least one more machine than is necessary to handle the load for redundancy and backup purposes.

Unique solution ID: #1008
Author: Chase
Last update: 2017-02-07 12:59