



# ANTI-SPAM FILTERING

## WELCOME

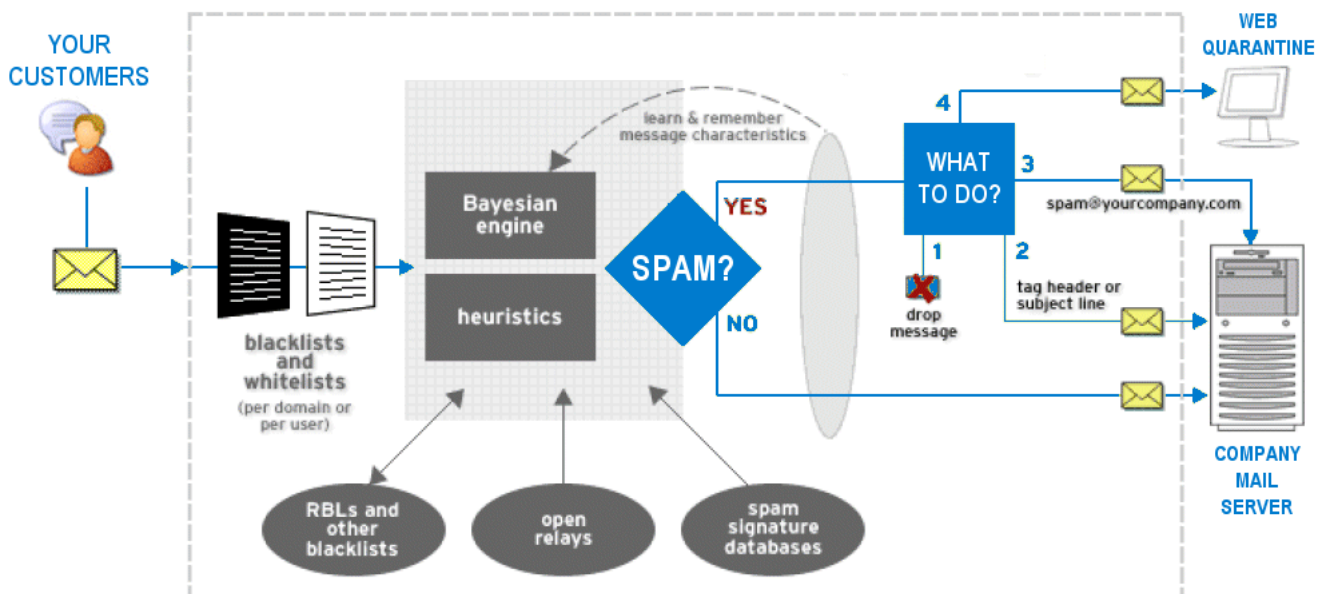
Thank you for choosing Edgewood Hosting as your ANTI-SPAM filtering solution. We are committed to providing a uniquely effective solution to help you dramatically reduce junk email. This document contains frequently asked questions regarding the use of our service. While the service is designed to be easy to use, we hope that this guide may serve as a reference for you during the initial setup of the service and as you experience the benefits of our filtering solution.

## HOW DOES THIS WORK?

You can manage your junk mail handling preferences via our Anti-Spam Control Center:

[HTTPS://ANTISPAM.EWHOST.COM](https://antispam.ewhost.com)

It's simple to login—just use your standard email address and email password you normally use! Once logged in, you will see a variety of tools and options available for managing your junk mail. This Guide explains these options and provides you with some background on how our system works.



Incoming email to your company is routed through our ANTI-SPAM servers located at a secure data center before it arrives at your company's email server. For each inbound message, we automatically run a series of tests to detect which messages are junk and which messages are legitimate. No software needs to be installed on your workstation at all!

---

## WHAT DETERMINES WHICH MESSAGES ARE JUNK?

---

Our system employs a multi-faceted set of tests on incoming messages to detect spam. Using our leading *Bayesian* engine, we compare incoming messages to millions of known SPAM message signatures to detect junk email. We also incorporate what's known as "whitelists" and "blacklists" as well as a database of web addresses advertised by spammers. As a final step, we have an extensive set of heuristic rules, which analyze:

- **MESSAGE HEADERS** – most junk email messages employ one of many possible techniques to mask their identities and to fool recipients into thinking that a message is valid; we recognize these techniques, and respond accordingly!
- **BODY TEXT** – while the millions of commercial spam messages are constantly changing, they often have a characteristic "style" to them. We can recognize these elements as well as messages that have previously been identified as spam.
- **MESSAGE SIGNATURE** – Our system builds upon the leading collaborative spam-tracking databases, which assign digital signatures to common messages and are continuously updated via the contribution of many thousands of users.
- **BLACKLISTS** – We incorporate many of the available "blacklists" of known spammers or spam relays, including the databases at [mail-abuse.org](http://mail-abuse.org), [ordb.org](http://ordb.org) as well as others.
- **URI LISTS** – Our system incorporates third-party and our own lists of web addresses, phone numbers, and other unique identifying elements advertised by spammers.

---

## WHAT % OF SPAM IS CAUGHT?

---

Our success rate fluctuates depending on the mailbox we are filtering. Different people have different mail patterns, and some customers choose a more aggressive posture against spam than other customers. Industry standards for spam detection range from 90% - 98%. Our goal is to correctly identify upwards of 98% of junk email.

---

## WHY CAN'T YOU STOP 100% OF SPAM?

---

Despite an occasional claim to the contrary, 100% is not feasible. Due to the enormous quantity and constant evolution of junk email, combined with the different communications patterns of different companies, no automated tool could block all spam without also blocking a significant number of legitimate email messages. Our system blocks a large percentage of junk email and is unlikely to block legitimate email.

---

## CAN I CHANGE HOW AGGRESSIVE THE FILTER IS?

---

Yes! Our system can take a more or less aggressive posture towards spam detection, in accordance with the type of email you receive. With a very aggressive posture – in which a very high percentage of spam is detected – there is a greater likelihood of legitimate messages that are mistakenly considered spam. Conversely, with a less aggressive posture, a higher number of spam messages may not be detected as such, but there is a lower chance of flagging legitimate messages as spam. We offer six settings for how aggressive we are in determining whether a message is spam:



## WHAT HAPPENS TO MESSAGES THAT ARE SPAM?

---

You have several options for handling spam messages detected by our system:

- **DROPPED** — The first option is to simply drop the message. This reduces the bandwidth requirements for your network, reduces the load on your company's mail server, and reduces the time that would otherwise be spent by you dealing with junk mail. The downside, of course, is that if a legitimate message is identified as SPAM, it is gone forever.
- **SUBJECT TAG** — The second option is to modify the subject line of messages that are detected as spam, and then deliver the messages to you. We simply add **\*\*SPAM\*\*** to the beginning of the subject line for detected spam messages. You can setup a simple filter in your email program that automatically places these messages in a "SPAM" folder which you can review periodically.
- **REDIRECT** — Our system can redirect all suspected junk mail to a single e-mail address at your company (like receptionist@yourcompany.com). This allows for one person to be in charge of reviewing the suspected SPAM.
- **QUARANTINE** — The most popular option is to send SPAM to your own password-protected Web Quarantine area that you can review periodically. Messages are stored in the quarantine for ten days and then are deleted. You can setup a notification email so that every day you get a summary of SPAM that you received. This way you spend your valuable time reviewing just one summary email instead of hundreds of SPAM emails.

## HOW DO I CHANGE MY SETTINGS?

---

You can manage your junk mail handling preferences or access your Web Quarantine via our Anti-Spam Control Center:

[HTTPS://ANTISPAM.EWHOST.COM](https://antispam.ewhost.com)

It's simple to login—just use your standard email address and email password you normally use! This site allows you to change the aggressiveness of the junk mail filter, view statistics about your email, manage your whitelists and blacklists, and access your Junk Mail Quarantine. To change how your junk messages are handled, click "Change Spam Handling".

## WHAT ARE WHITELISTS AND BLACKLISTS?

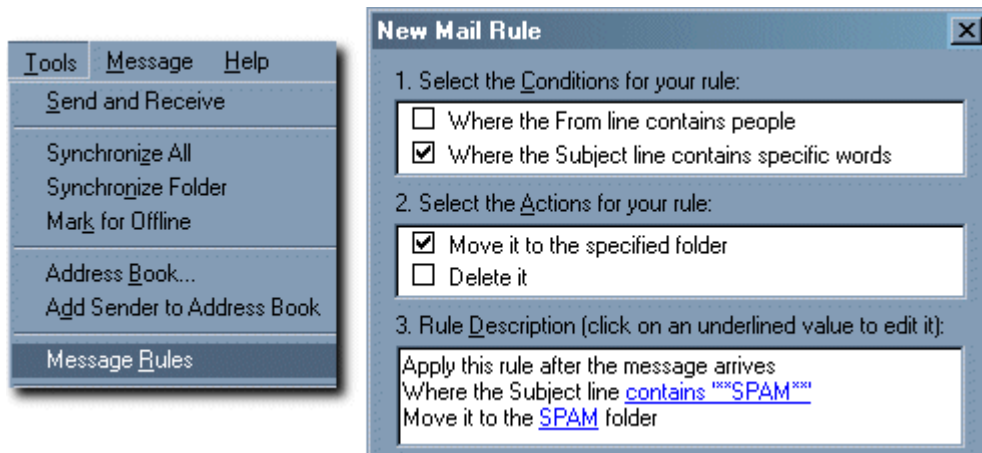
---

Whitelists are rules that allow messages to be delivered based on their FROM email address or domain name, regardless of how SPAM-like the message may be. If you find that messages from yourcustomer.com routinely get mistaken for junk email, you can add that domain to your whitelist. This will ensure that it is never flagged as SPAM. Conversely, blacklists are rules that block messages based on their email address or domain name, regardless of content. An email from an annoying spammer that continually gets through our system but is truly SPAM can be added to the blacklist to prevent future message delivery.

Please note that you may add individual email addresses (john@example.com) or entire domains (example.com) to you whitelist or blacklist. The latter example would affect emails from every user @example.com, so be careful when using that.

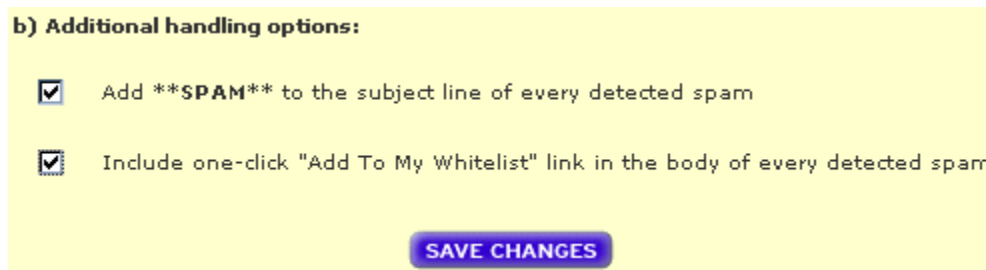
## FILTERING MESSAGES WITH **\*\*SPAM\*\*** IN SUBJECT

Are you receiving hundreds of messages in your mailbox with **\*\*SPAM\*\*** at the beginning of the subject line? This is an indication that our filtering service is working! You (or your administrator) has elected to handle suspected SPAM messages by placing the phrase **\*\*SPAM\*\*** in front of the subject line. Some folks like this and others hate it. The nice part of having the subject line “tag” is that you can setup a simple filter in your email software to automatically forward these messages to a separate folder from your inbox. You can then review the messages at your convenience. This is very simple to implement with many email software programs, including Outlook, Outlook Express, Entourage, Netscape Mail, Thunderbird, Eudora and others. Since different programs have slightly different procedures for this, please consult your system administrator.



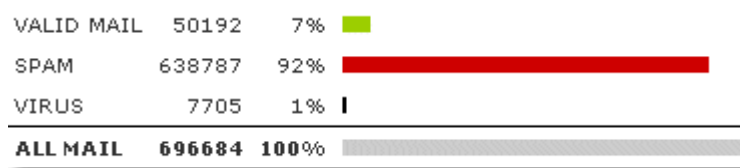
## SPAM NOTIFICATIONS WITH WHITELIST LINKS

Do some of your incoming messages now start off with something like “SPAM notification: This message was detected as probable spam?” This is an optional feature of our filtering service, which your system administrator may have enabled. Because a small percentage of email messages identified as spam may be legitimate email, this feature allows you to easily “whitelist” addresses so that future emails from the same address will be automatically considered as legitimate messages. With this feature, if a detected spam message is not spam, and you want to receive future emails from that sender, simply click on the link within the message, and the sender will be automatically added to your whitelist. This feature can be enabled or disabled within your Anti-Spam Control Center by enabling the “Add To My Whitelist” option:



## HOW MANY OF MY MESSAGES ARE SPAM?

You can view statistics on the messages you've received on your Anti-Spam Control Center. Click on "Message Volume" to see an overview of how many valid messages, junk messages, and virus-infected messages were sent to you.



## DAILY SPAM SUMMARY EMAIL

You can enable a daily summary of messages (called a "digest") that were detected as either SPAM or viruses. From your Anti-Spam Control Center, click on "Email Notifications." You can also have email statistics sent to you on a daily basis.

A message digest is a listing--emailed to you periodically--of all spam messages caught by the system. It contains a brief summary of each message, including sender address and subject line. If your **spam handling settings** are currently configured to redirect your spam messages to webmail quarantine, you may find this digest helpful.

I do NOT want to receive a message digest.  
 YES, I would like to receive a message digest.

Send the digest every:  SUN  MON  TUE  WED  THU  FRI  SAT

## WHAT IF MY MAIL SERVER GOES DOWN?

Normally, our servers process all inbound messages instantaneously and deliver them to your mail server without storing the messages. However, if your mail server is down or inaccessible, our system will act as a message queue, and will temporarily hold inbound messages for your company, forwarding the stored messages to your server once it is back online. Thus, our filtering service effectively adds reliability to your email system, but it does not retain any messages once those emails have been delivered to your mail server.

## FEEDBACK AND IMPROVEMENT

What should I do with spam that is not detected properly? Similarly, what should I do about any legitimate mail that is detected as spam? Our staff reviews undetected spam (called **false negatives**) and legitimate mail erroneously detected as spam (called **false positives**) on a regular basis. To assist with this process, please:

- forward false negatives (undetected spam) to [spam@ewhost.com](mailto:spam@ewhost.com)
- forward false positives (legitimate mail tagged as spam) to [notspam@ewhost.com](mailto:notspam@ewhost.com)