

Geton Anti-Spam - FAQ

Will I need to make any changes to my mail client POP or SMTP settings?

No! All changes in regards to our service are seamless to the end user's mail client.

I have signed up for your Advanced Spam Protection service, but I have not received any user account information.

User accounts are created automatically when a message is quarantined for the first time. You may also create your account automatically by entering your email address on the administration login page (<https://admin.getonantispam.com>), without a password and then click on the "Create New Password" button. An email with your account info will be sent to that email address. You must use a valid email address for your domain.

What user level controls does your service make available?

- **Quarantine Enable/Disable Ability** - Controls the user's ability to enable/disable their personal quarantine inbox.
- **Spam Scan Enable/Disable Ability** - Controls the user's ability to modify their personal spam settings.
- **Notification Change Ability** - Controls the user's ability to change the frequency and language of their quarantine summary notifications.
- **Scoring Change Ability** - Controls the user's ability to change the spam scores at which their emails are tagged, quarantined, and blocked.
- **Use Bayesian Ability** - Controls the user's ability to manage their personal Bayesian database. the spam scores at which their emails are tagged, quarantined, and blocked.
- **Whitelist/Blacklist Ability** - Controls the user's ability to add email addresses and domains into their personal whitelist and blacklist.

What happens to my email if my mail server is unavailable?

Your mail will be stored on the firewall, then delivered once your server becomes available.

How do I know my email will remain private?

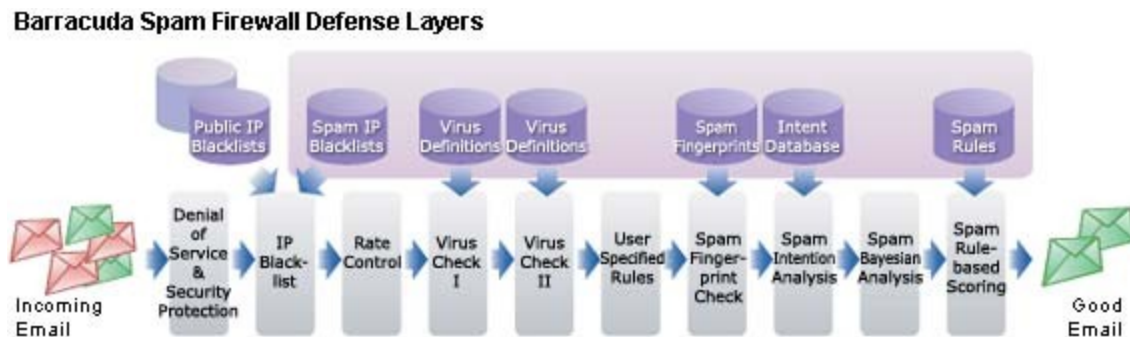
Email is processed inside the hardware. Further privacy is configured in the Spam Firewall. The administrator can specify who can access the machine and it is password protected. All administration interfaces are also protected by a 256 bit high encryption SSL certificate.

How often are your Spam and Virus definition databases updated?

At Barracuda Central, a team of security experts work around the clock searching for new threats and trends circulating throughout the Internet. Spam rules and virus definitions are updated on central databases and made available to our Spam Firewall through an Automated Subscription Service. These updates run on an hourly bases minimizing response time to new threats.

How is Spam filtered?

Incoming email is routed through the Barracuda Spam Firewall. Spam is tagged, quarantined or blocked based on preferences. Legitimate email is allowed through to the destination mail server and recipient mailbox.



Will I receive “False Positives”?

The Barracuda Spam Firewall is tuned to minimize false positives and has one of the lowest false positive ratings in the industry. Per user allow and block lists will further reduce the occurrence of false positives. **NOTE:** The more aggressive your Spam score setting, the higher the likelihood of false positives.

What happens to quarantined email?

If you have selected the “Advanced Spam Protection” program, all quarantined messages are stored on the firewall on a per account bases. You will receive notifications at intervals you select in the administration interface for your account. The default notification interval is daily. If you have selected the “Basic Spam Protection” program, no emails will be quarantined. All suspect messages will be tagged “[BULK]” and delivered to your inbox for further evaluation and action.

I use my mail client to redirect tagged messages to a designated folder. My current anti-spam solution uses *SPAM* or some other keyword to tag messages. How do you tag suspected Spam messages?

Not all mass emails are Spam. We prefer to use [BULK] to tag suspected messages.

I marked a message to “Deliver”, “Whitelist”, “Whitelist/Not Spam” or “Classify as Not Spam”, but I can not see it in my inbox.

All messages that have been quarantined will be delivered to your inbox with the original time and date of the email. You may need to scroll or change view settings in your mail client. You may also need to check any rules you may have set up in your mail client.

What level(s) of redundancy does your service provide?

- Our servers are located in a Class A Data Center with multiple fibre channel connections to the Internet.
- We run daily backups on our mail servers.
- If our mail server becomes unavailable, the Spam Firewall will store mail until it is available again.
- Our Spam Firewall is equipped with redundant disks (Mirrored Drives) should one of them fail.
- All Spam Firewall configurations including user account settings and Bayesian databases are backed up at daily intervals.
- If our Spam Firewall becomes unavailable, we have a backup MX server that will receive your mail and store it until it becomes available again. The backup MX will then forward all mail to the Spam Firewall were it will be filtered before final delivery. This is to ensure you are still protected in the event of a service interruption.

NOTE: We have a 24 hour replacement service agreement with Barracuda Networks in the event of a non-recoverable hardware failure of the Spam Firewall.

How do I troubleshoot lost mail?

Lost mail can result for a variety of reasons including of course, the use of Anti-Spam and Virus protection services.

1. Have there been any recent changes to the mail server? Has it been moved? Has domain and account information been remove for the old server? Has the domain changed DNS servers? Have the records for the domain been remove from the old DNS servers?
2. Search your mail server's log file for recent occurrences of the email address, domain or the IP address of the sending mail server. You can do an MX lookup for the domain to retrieve the IP address. Ask your service provider or domain administrator to search the logs if you do not have access.
3. Send an email, with the address in question, to postmaster@getonantispam.com with the subject line "Lost Mail". We will search our log to see if it was filtered through our system and respond with the results and any suggestions.

I am still receiving Spam. How can I stop it?

The nature of UCE (unsolicited commercial email) is that once a way has been found to defeat one method, another method is found to avoid detection. We can only try to minimize the Spam that reaches the inbox, but this also requires action on the part of the user.

1. If you are on the "Basic Spam Protection" program, we highly recommend you upgrade to the "Advanced Spam Protection" program. This will provide you with more tools and control.
2. Make sure that port 25 (SMTP) on your mail server will only accept inbound connections from mx1.getonantispam.com.
3. If you notice certain sender patterns, you can use your block list in the admin interface of our Spam Firewall. Blocking may be performed by full email address ("user@domain.com"), domain only ("domain.com"), or domain portion ("com"). For example, you notice that a lot of Spam has a source domain of somehost.somedomain.ru and you know you never receive legitimate email from Russia. Put "ru" (without the quotes) in your block list.
4. All email filtered through our Spam Firewall will have a "X-ASG-Debug-ID" string in the header of the email. Set your mail client to view all header information. Look for a string that looks similar to "X-ASG-Debug-ID: 1172391343-32e400100000-JqMYgr" and send this ID to abuse@getonantispam.com. We can examine the email and take further action to try blocking similar messages. If the message does not have a "X-ASG-Debug-ID", then it did not flow through our service.