

Firespring offers an e-mail filtering service which scans for and flags potential spam so that it can be efficiently located and eliminated. Additionally, this service removes viruses from inbound e-mail. With a monthly subscription fee, all e-mail messages addressed to your domain(s) are screened.

How does it work?

Once activated, your inbound mail is diverted to our spam filtering servers where each incoming message goes through a 10-step screening process. At the end, a decision is made as to the status of the message and one of four possible outcomes takes place. The message may be Allowed, Tagged, Quarantined or Blocked. See below for detailed descriptions of each.

1. **Allowed:** This means that the message is, by our best judgment, not likely to be spam. When we "allow" a message, we are letting it go through the system to be delivered directly to your inbox.
2. **Tagged:** When, based on our calculations, an incoming e-mail is suspected to be spam yet we are not entirely sure, we let the message through to you, but we alter the message by adding "[SPAM]" to the beginning of the subject line. We do this for two reasons. First, we're not sure that it is spam, so we don't want to delay the message; we'd rather let you make the final decision. Secondly, we want to make it easier for you to see that it may be spam. If you prefer, you can also use this tag to set up mail rules in your e-mail client so that these messages are moved to a folder of your choosing, to be sorted through as time permits.
3. **Quarantined:** When we determine that a message is very likely to be spam, we stop the message from being delivered and hold it on the server. We then send a Quarantine Summary to you. Since we're pretty sure that the message is spam, the delay shouldn't be a problem. If you see a message in your Quarantine Summary that you would like to be delivered to your inbox, you can choose that message for delivery and, optionally, whitelist the recipient so that their messages aren't stopped in the future. Alternatively, you can always manage your settings and preferences via a direct access URL (See "How do I access the firewall settings and preferences?" below).
4. **Blocked:** When we are very sure that the message is spam, we block the message altogether. These would be messages from blacklisted senders and known sources of spam. These messages aren't reported to you; they are just rejected altogether. We do this to make the rest of your content more relevant. You're much more likely to check for legitimate messages in your Quarantine Inbox if we keep the most egregious mail out of the mix. We have seen no instances in our review of this blocked mail being anything other than spam. However, if you feel this could cause an issue, you can whitelist every domain name and specific e-mail address from which you need to receive e-mail. We cannot make global adjustments because it is very important for all of our end users to have the ability to manage their spam filtering in their own way.

Are all spam messages at least Tagged?

Spammers are constantly coming up with new ways to "beat the system". Our filtering software is constantly updated to fight spammers' newest tactics, however it is possible that a spam message will come through without being tagged. The reverse is also true, once in awhile a legitimate message might be tagged as spam when it is not.

Will I miss any real messages?

If, due to its characteristics, a message is tagged as "[SPAM]" you will still receive it. If it is contained in your Quarantine Summary, you will be able to release it for delivery and add the domain to your whitelist for your e-mail address to prevent messages from this sender from being tagged or quarantined in the future.

How do I access the firewall settings and preferences?

You will receive a Spam Quarantine Summary for each of your e-mail addresses. In the body of this e-mail of your Quarantine Summary you will be able to Deliver, Whitelist and Delete.

At the bottom of the Spam Quarantine Summary e-mail notification you will see a direct "click here" link to access the Firespring Spam Firewall administrative tool. This link will expire three days from when the e-mail was delivered, but you can always access this administrative tool directly, via this URL: <http://filter01.digitalims.net:8000> u: account@example.com (your e-mail address) p: password.

Each individual e-mail account in your organization will have its own login to access his/her own settings and preferences. Each user will enter his/her own e-mail address and e-mail password.

Quarantine Inbox

Preferences: The Whitelist/Blacklist tool within the Firespring Spam Firewall administrative tool allows you to whitelist or blacklist individual e-mail addresses or entire domain names. No wildcards are necessary. Simply enter "example.com" to whitelist or blacklist an entire domain name.

Quarantine Settings allow you to disable the quarantine and allow the messages that would ordinarily be quarantined to be delivered with "[QUARANTINE]" in the subject line. Please remember to enable the quarantine when you are finished. You may also wish to define the notification interval. "Daily" is recommended and is the default interval setting. Additionally, you can change the notification e-mail address, if perhaps you want your quarantine notifications to be sent to a different e-mail address.

Spam Settings allow you to disable the spam filtering. This is not recommended.

When I add a new account, will it automatically be protected?

Once your domain is set up to be screened, all accounts current and future are protected, unless you decide differently. You will be able to opt an account out of the screening by contacting the support services team.

Do I still need my anti-virus software?

Yes. We recommend you continue to run anti-virus software on your local system. E-mail is only one way viruses are transmitted.

How do I get started?

Add the spam & virus protection service by completing the form in your website Administration Area > Manage Your Account > E-mail Accounts section. We'll add just \$15/month to your monthly subscription fee.

Don't have a website Administration Area? Download the order form found at http://www.firespring.com/clients/spam_virus_protection.html, complete and fax it back to us. We'll add just \$15 per month to your hosting fee.