Customizing your mailbox.org spam filter settings

Important note to our business customers: these settings need to be enabled via your administrator via the setup panel first.

The spam protection module of mailbox.org comes with pre-configured settings that are optimal for most users. If you would like to change the configuration and deactivate particular features, please read this article first to get more information about how the individual mechanisms work.

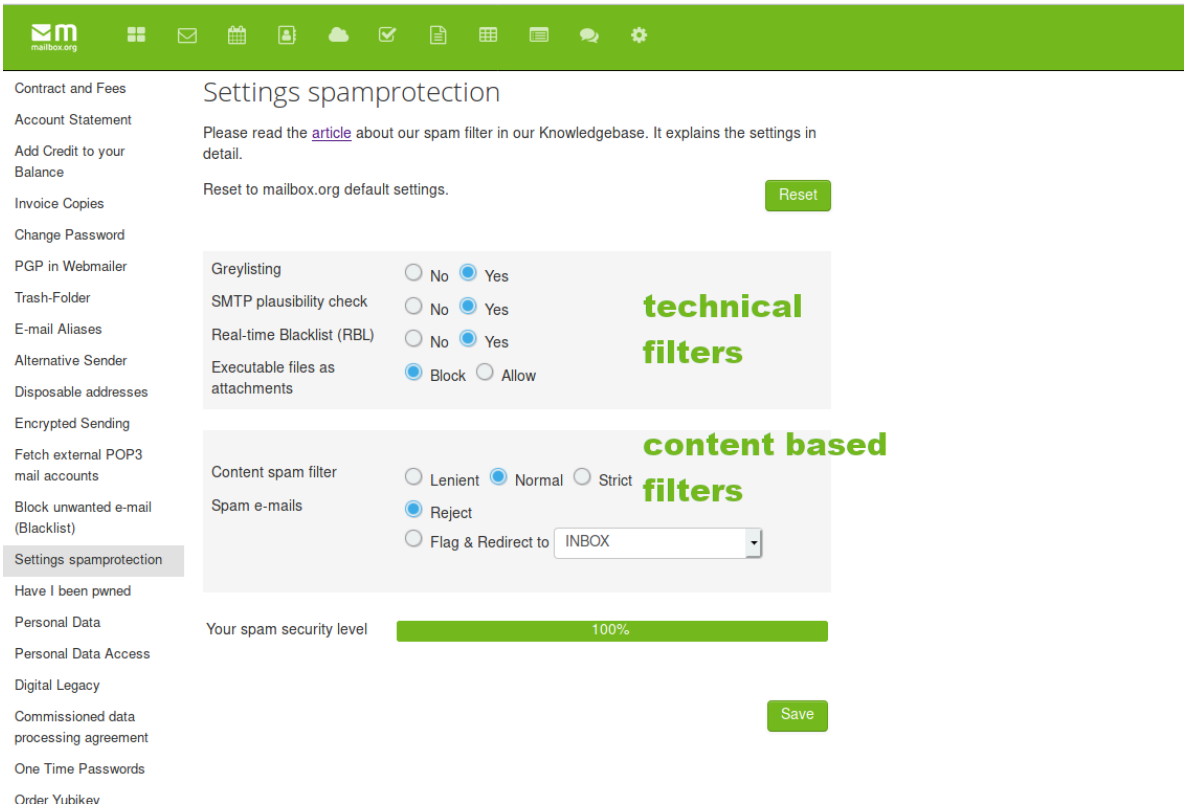
You can find the spam filter configuration page in the web frontend under Settings mailbox.org Spam filter

Please take note of the following definitions, which we are going to use in the following:

- **Client:** This is the system that wants to connect to our servers and deliver an e-mail, normally another mail server or, sometimes, a spam server or evil botnet.
- **False positive:** A regular e-mail, which was flagged as spam even though it is not spam.
- **False negative:** A spam e-mail, which the system failed to recognize as such.

Whenever an e-mail has been flagged as spam by our systems, it will be rejected. That means our server will deny accepting the e-mail message and the system at the other end (the client) will issue a delivery failure notice to the sender (the message „bounces“). So, the sender will be notified by their own provider if there was a problem with delivering the message. It is the same bounce mechanism commonly in place to deal with situations where someone tries to send an e-mail to an address that doesn't exist, for instance when there has been a spelling mistake.

The setup has mainly two sections:



technical filters: shows the options for filtering at protocol level. Filtering is done before the server "sees" the real message.

content based filters: is the area of content filtering. Filtering is done by various techniques, which check for known patterns in the e-mail. You may choose, whether detected spam should get rejected or get moved into the "Junk"-folder for instance.

Important: The options in teh technical filters area always reject messages (except greylisting, this only rejects temporary), if a message matches there (independantly of the settings in the content filter section).

Spam protection through greylisting

Greylisting is a technique where a mail server will temporarily reject initial connection attempts made by clients that are currently unknown to the server, i.e. those that have never made a connection before. Our mail server will react to such connection attempts by sending the

equivalent of what would be a „busy“ signal on a telephone line. After five minutes have passed, the client is then automatically permitted to try again to deliver the e-mail message. Once this happens, the message will be accepted and relayed to the recipient. Hence, greylisting means that a message won't be blocked or returned indefinitely – regular messages will always arrive eventually.

So, what is the rationale behind imposing this delay? The greylisting technique exploits a behavior commonly shown by spam senders and bot-nets, which for various reasons tend not to try and deliver a message repeatedly if rejected once. On the other hand, in regular mail server operation clients will frequently meet „busy“ servers on the opposite end and then automatically attempt to deliver a message again. Since any systems who have made a successful connection previously are no longer greylisted, more than 98% of all mail traffic will usually pass through without delay.

- Risk that any legit e-mails get blocked (False positives): Virtually zero.
- Recommendation: Leave enabled.

SMTP plausibility check

This mechanism compares the host name submitted by the sending mail system („I am host ABC“) with the hostname mapped to the IP address used by that system („Reverse Lookup“). According to official RFC guidelines, mail servers should make sure these two pieces of information match exactly. If they don't, then there is an increased likelihood the client is a spam sender or bot-net trying to hide its true identity.

In practice, one may experience problems with legit yet poorly configured mail servers, where hostnames and IP addresses don't match. Depending on further parameters, e-mails coming from these kinds of servers might get blocked.

We believe the SMTP plausibility check is the only spam protection measure that might actually produce false positives on occasion. Whenever our users have reported a problem with the receiving of e-mail, it was usually because of this mechanism.

- Risk of false positives: Low.
- Recommendation: Consider disabling only if you are experiencing problems.

Realtime Blacklists (RBL)

RBL blacklists are global databases that contain up-to-date information about clients that have been recognized as a source of spam. Providers can check these databases in real-time to protect their customers. Clients that make it on these lists may have been infected by viruses, or compromised through hacking of their system software or of the mail accounts on the system, and will then keep sending spam messages on a massive scale as a result. Any e-mails coming from these sources will consequentially be blocked and not delivered.

RBL blacklists are not centralised and there are many of them, and they are all using somewhat different policies. For this reason, mailbox.org does not employ all of the lists but only a few that are particularly reputable and in use by many other providers as well. What these lists have in common is that they operate extremely cautiously and will only “blacklist” a client if there is clear evidence of abnormal behavior. If a system appears on one of these lists, we can be sure this happened for a good reason. Sometimes, ordinary mail servers can be affected as well but only if they actually pose a danger to other systems (which may be temporary).

- Risk of false positives: Very, very low.
- Recommendation: Leave enabled at all times.

Content spam filter

For content filtering, we use the well-known “Spam Assassin” software, which determines the spam probability of a message based on different technical characteristics. If a message has a high probability of being spam, it will be either rejected directly, or redirected to a special mail folder.

- **Careful:** The risk of false positives is infinitesimal but as a consequence, some spam messages may remain undetected („False negatives“).
- **Normal:** This is the optimal setting, where the detection parameters have been adjusted based on years of experience, yielding a minimal risk of false positives. We have not had any issues reported yet from customers who use this setting - definitely recommended.
- **Strict:** The number of e-mails recognized as spam increases, which will block almost all spam e-mails but at the same time, the risk of experiencing false positives increases as well.

Recommendation: Use the „Normal“ setting.

Block executable attachments

By default, our servers will block messages containing files with suspicious characteristics that are almost always out of the ordinary and likely dangerous (e.g., double indices on Windows files). Further, executable files will be blocked if attached directly to a message. The danger of catching a virus is simply to large with these e-mails. If an executable file is wrapped into a ZIP archive and then attached, then it will usually pass through without problems as the risk of an immediate infection is lower.

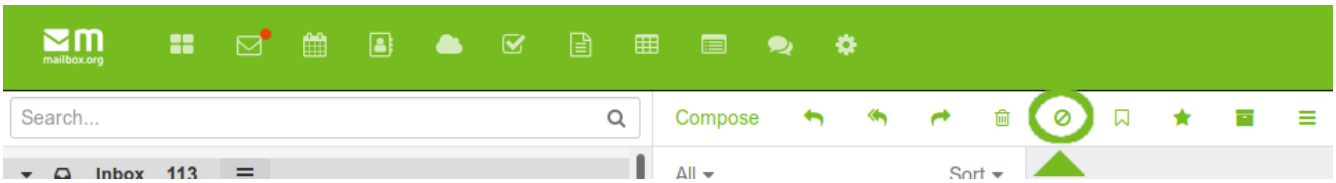
If this option is disabled, all file attachments will be passed on, no matter the file type.

Please note: Any file attachments that our virus scanners recognize as infected will still be blocked.

- Risk of false positives: Very low, as most e-mail are not affected by this.
- Recommendation: Leave enabled at all times to avoid virus infections.

Trainable spam filter

If you still receive spam despite all these measures, you can easily train a personal filter.
To do this, first select the message in question. Now click on the "Spam" icon:



Alternatively, you can simply move the message to the spam folder, which will also trigger the learning process. If you moved a message to the spam folder by mistake, just move the message
from the spam folder back to your inbox.

Learning success: the filter trained here probably needs a certain number of examples, in order to reliably recognize the messages as Spam. The learning success also depends directly on
the content of the messages.

Summary:

In our opinion, the only spam protection measure that might occasionally cause problems with receiving e-mails is the SMTP plausibility check. None of the other techniques has ever been at the heart of any support tickets we had.

We understand that some people might want to disable the SMTP plausibility check but we also strongly recommend to leave all other mechanisms enabled.

Please note: Successful spam protection requires a combination of different mechanisms. Only this combination minimises the risk that e-mails get flagged as spam by mistake („False positives“). *We ask for your understanding that we cannot accept any complaints about insufficient spam protection if a user has manually disabled any of the components that are enabled by default.*

Related Articles

- Why am I getting spam in my mailbox
- Customizing your mailbox.org spam filter settings
- My sieve mail filter does not work
- Can I use sieve mail filtering
- Should I forward virus warnings