Enabling Junk Filter

We turn ON the Junk Filter for all our clients when their hosting is set up.

Accessing your Junk Mail

To protect legitimate mail, novice users can follow these three basic steps:

1.

   - Go to https://webmail.YOURDOMAIN.com/ (.net .org, etc.) for the secure version of your Webmail (replacing, of course, "yourdomain" with your own domain name). Enter only the first part of your e-mail address (the part before the "@" symbol) and your password.
   - Users are recommended to bookmark their Webmail URL.
   - To access a non-secure version , remove the "s" from the "http" in the Webmail URL: http://webmail.YOURDOMAIN.com/

2.

3.

   - To read any of these messages, you have to move them to your inbox. If you're not sure about a message, choose just the "Move to INBOX" option to read it. If clearly legitimate e-mail is found, you'll want to choose the option "Move to INBOX + Add Sender to Whitelist." A Whitelist is a list of e-mail addresses you always want to get through the filter.

Notes

- It's a good idea to delete the *real* junk, because it will lessen the amount of mail to sort through the next time you check the folder.

- Note that these messages are **not** listed according to date, but in the order of their "Spam factor" scores, from lowest to highest. This means that if legit messages have been caught here, they will probably be near the top of the list.
- **Every weekday**, between 4:00 and 5:00 pm, you'll get an e-mail titled "Junk Mail Report" that lists any messages you currently have in your Junk Mail folder. Be sure to read this message to see if anything legit has been blocked. (You can, of course, check this any time you like by going to Webmail.)
- If you have questions about any of this, or would like your settings changed, please read on.

Changing the Junk Mail Settings

(For more tech-savvy users)

In Webmail, you can modify your settings in *Options → SpamAssassin Configuration*

- Set up whitelists and blacklists, using individual email addresses or full domains. You'll see examples there too. Please note: when adding addresses and domains to these lists, be sure to check the full header of the email they sent, and use the 'return path' address, not the 'from' address. Spam Assassin filters based on the 'return path' value. When an address is whitelisted, it will bypass the filters and goes directly to the inbox. When it's blacklisted, it goes directly to the junk folder, regardless of how much it may score.

- Change the tag and quarantine value. Spam Assassin analyzes the email and places a score at the bottom of the header. Your tag and quarantine numbers will be compared to that score, and the mail will be handled accordingly: delivered to inbox or placed in the junk folder.

The default tag/quarantine level is 999/4. That means that the messages are never getting tagged (it's highly unlikely to score a 999...) and anything that scores a 4 or above will be moved to the junk folder. The lower you set your quarantine number, the higher the chance to catch the junk. However, if you go too low, you may end up with a lot of false positives. It's good to experiment a little before settling with a number. A good way to do that is setting your quarantine number to high-ish, like 10, and set your tag level to 1. That will tag all messages that score at least 1 with DHSPAM in the subject. Do that for a couple of days, and it will give you a good idea how Spam Assassin scores the messages.

Once you settle with a low quarantine number, don't forget to check the junk mail folder from time to time, and add to your white- and blacklist, to make the filter better suit your needs. Oh, and once you're done with the 'training' I described above, set your tag level high again - a tag level that is lower than the quarantine level won't do any good: anything that is quarantined won't get tagged as well.

Tip: if your email address is on a filtered domain, but you'd rather not mess with filtering and checking it through webmail, just set your tag and quarantine numbers to 999/999 - they will be left alone.

- You can also set the frequency of junk reports delivered and how often will our own sweeper clean out your junk mail folder.

NOTE: once the mail is deleted from your junk folder, it's not recoverable any more! Please be sure to customize your settings, and check the junk folder from time to time to check for false positives.

How Junk Mail works on primary addresses and forwards

OK, I admit, this can get a bit confusing. I'll try to be as graphical and straightforward as possible, but if you still have questions, don't hesitate to submit a support request, and we'll be happy to further explain.

Primary email address: Fairly simple - if the domain is being filtered, the email will be delivered based on the junk settings for that primary address. Reminder: make sure your domain is either pointed to our name servers or you have updated your name server provider for that domain with the new filter MX records.

Forwarding email address:

- If the domain is being filtered, and the address is being forwarded to another WebLiteDesigns email address which is also filtered: email gets sorted based on the junk mail settings of the original forwarding address (NOT by where it ends up).
- If the domain is being filtered, and the address is being forwarded to another WebLiteDesigns email that is not filtered or is being forwarded to an outside address only (like @gmail), then the settings you created in webmail for that email address will not apply, and the tag and quarantine numbers will reset to 999/999. It can be confusing, as you may even see a junk folder when you log in (if the forward is to another DH email address), but the mail coming to this forwarding address will not get filtered. The reason for that is that you would be unable to check any quarantined messages. Please note: even if you are forwarding the mail to a mailbox that is filtered, if you have at least one outside forward, that will prevail and your settings will go back to 999/999.
- If the domain is NOT being filtered and it forwards to a DH email address that is on a filtered domain, the mail will not get filtered. The way our junk filter works, it checks the email addresses against the mail database on our filtering mail machines. If the address is not there, it sends it to a regular mail machine. Once the mail enters our system, it will not go out again to be filtered: once the mail hits our system through the non-filtered email address, it will not get filtered, even if the end of the forward is filtered address. Makes sense?

Removing Junk Filter from your domain

Please email WLD your request: info@weblitedesigns.com. Please note, the DNS propagation rules apply; it can take up to 4 hrs. Again, if you have outside name servers, don't forget to update them with the new MX records.

Once the junk filter is off your domain (and propagation has finished), your mail will no longer get filtered. However, if you still have mail left in your junk folder, you will need to clear that out, or you'll be receiving junk reports - note, only with old messages - until you do so. Your junk folder will also remain on your webmail. If it bothers you, let us know your email address, and we'll manually remove it for you. If it's a whole domain, please still try and send the list of email addresses for easier processing. We'll work on making that automated in the future, but for now it has to be done by hand.

Using keyword filters with Junk Filter

You can still use the keyword filters even if the domain is set up with the junk filters. Mail will come in through the filter machines first, then gets routed to the regular mail machines where your keyword filters will apply. Email WLD with your list of Keywords to be added to your hosting account to be filtered.

Inaccessible from alternative webmail clients

For now, the junk mail spam folder is inaccessible from any webmail app other than WebLiteDesigns's copy of SquirrelMail.