Mozout

Generated on 15/11/2026 00:36

KNOWLEDGE BASE · PUBLIC DOCUMENT

How to stop spam reaching your mailbox: what we filter and what you can do

Delivery & Spam

CODE	VERSION	COUNTRY · LANGUAGE
RLX-INT-KB-738	v2026.10.04	International · English

MozOut International
RLX Holdings (Pty) Ltd. · Group RLX Holdings
Tax no. (SARS) 943 907 6234 · Registration no. (CIPC) 2025/667953/07

https://www.my.mozout.com/knowledgebase/738

How to stop spam reaching your mailbox: what we filter and what you can do

Delivery & Spam Created on **August 17, 2026** Updated on **October 4, 2026** 6 min read



There is no way to end spam, and anyone promising that is selling you a fiction. There is a way to cut it down a great deal - and most of that work is already done before the message reaches you. This article covers what the server filters on its own, what you can switch on in your account in five minutes, and the habits that make more difference than any filter.

First, a clarification:
This article is about **receiving** spam. If your problem is the opposite - *your* messages landing in other people's spam folder - the fix is a different one and it lives in **SPF, DKIM and DMARC**.

What we already do before the message reaches you

None of this needs switching on by you: it is active on the server for every account.

Protection	What it does in practice
Content analysis	Every message is analysed and given a spam score before delivery
Identification checks	Whoever connects must identify itself properly - forged or malformed identification is refused at the door
Dictionary attack blocking	Anyone guessing addresses on your domain at random (info@, sales@, contact@...) is cut off
Rate limiting	Servers dumping messages at machine speed are throttled
Repeat-failure blocking	Senders that keep failing delivery stop being served for a while
Scanning on the backup server too	Spam cannot slip in through a side door while the main server is busy

We also filter what **leaves** the server. That does not protect you directly, but it protects something you depend on: if a neighbouring account were compromised and started firing out spam, the whole server would land on blacklists and *your* messages would stop arriving anywhere.

Switching on the spam filter in your account

The analysis always happens, but it is your account that decides what to do with flagged messages. Five minutes well spent:

1. Log in to cPanel and open **Spam Filters** (in the Email section).
2. Turn on the **Apache SpamAssassin spam filter**. From then on, messages over the threshold carry *****SPAM***** in the subject - easy to see and easy to filter.
3. Turn on **Spam Box**. It is the most important option on that page: instead of mixing spam in with everything else, it delivers it to a separate **Spam** folder you can glance at now and then. Nothing is lost.
4. To be stricter or more relaxed, adjust the **score**. It starts at 5. Dropping to 4 catches more spam *and* more legitimate mail by mistake; raising it to 6 or 7 does the reverse. Move it **half a point at a time** and watch for a week.
5. Use the **Allow** and **Block** lists for specific cases: the accountant whose mail keeps landing in spam, the nuisance sender who keeps not landing there.

! **Do not turn on auto-delete straight away:**
There is an option to **delete** spam instead of keeping it. A message deleted that way **goes nowhere** - there is no folder to retrieve it from, and we cannot recover it either. If you ever use it, set it to delete only very high scores, and only after months of confirming that your Spam folder holds nothing worth keeping.

The habits that beat any filter

Do this	Why
Do not publish the address as text on your site	It is the single biggest source of spam: programs crawl websites all day harvesting addresses. Use a contact form instead of printing sales@ on the page
Never reply to spam	A reply confirms the address exists and is read by a human - which makes it worth more on the lists that get sold on
Do not click "unsubscribe" from strangers	On a newsletter you asked for, it works. On spam it does exactly what replying does: confirms you are alive

Do this	Why
Mark as spam instead of deleting	Deleting teaches the filter nothing. Marking teaches it, and the next similar message gets caught
Use separate addresses	One address for customers, another for sign-ups and website registrations. When the second fills with junk, you throw it away with no consequences
Be wary of anything asking for details	The spam worth blocking is not the advertising: it is the message pretending to be your bank, or us, to get your password

The mistake that fills mailboxes: the default address

cPanel has a setting called the **Default Address**, also known as *catch-all*. When it is set to forward, **anything sent to any made-up name on your domain lands in a mailbox of yours** - including the thousands of random guesses robots make every day.

It is one of the most common causes of a mailbox that "will not stop receiving junk". The fix is simple: in **cPanel → Default Address**, choose **discard** instead of forwarding. Anyone writing to an address that does not exist gets told it does not exist - which is the correct behaviour.

If you genuinely need to catch everything:
Create accounts or forwarders for the addresses you actually use (info@, sales@, support@) and leave the default set to discard. Same result, without the tap left running.

Your own rules, for what the filter misses

When the nuisance always has the same shape - a repeated subject, an entire domain, one word - a rule works better than lowering the overall score. You can create them in **cPanel → Email Filters**, for one account or the whole domain, or straight from webmail: **how to create e-mail filters in Roundcube**.

One thing to avoid:
CPanel includes a tool called **BoxTrapper**, which replies to every unknown sender asking them to confirm. It sounds sensible and is not: spam almost always carries a forged sender, so those confirmations end up bothering innocent people - and legitimate customers who never answer the challenge have their messages lost. We do not recommend it.

What if a good message ends up in spam?

It happens, and you fix it in this order: take the message out of the Spam folder and mark it as legitimate; add the address to the **Allow** list in Spam Filters; and only then, if it keeps happening with different senders, raise the score by half a point. If it is a message you really need and it is nowhere to be found, **talk to us** - we can see in the server log what happened to it.

If the problem is broader than spam - messages simply not arriving or not going out - start with **why your e-mail is not sending or receiving**.

NEED A HAND?

Still getting too much spam after all this?

Talk to us →

SEE ALSO

If you use Outlook, there is a second filter to consider:
How to stop spam in Outlook: the filter on your computer and the one on the server

For the reverse problem, your own messages landing in other people's spam:
How to write an e-mail that does not land in spam: behaviour, recipients and limits

WEB HOSTING

Looking for hosting that stays out of your way?

cPanel, a free SSL certificate, backups every night before dawn kept for a year, and support that answers in your language.

See hosting plans →

Free migration of your current site · no lock-in

MozOut International

RLX Holdings (Pty) Ltd. · Group RLX Holdings

TAX NO. (SARS)	943 907 6234
REGISTRATION NO. (CIPC)	2025/667953/07
REGISTERED OFFICE	1111 Olive Street Saint Louis 63101, Missouri, United States
CONTACT	info@mozout.com · +27 78 823 3325 · www.mozout.com
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

Online version of this document

RLX-INT-KB-738 · v2026.10.04 · Generated on 15/11/2026 00:36