Generated on 21/10/2026 16:04

KNOWLEDGE BASE · PUBLIC DOCUMENT

Your server IP on a spam blacklist: finding the source and getting off Spamhaus or SpamCop

Security

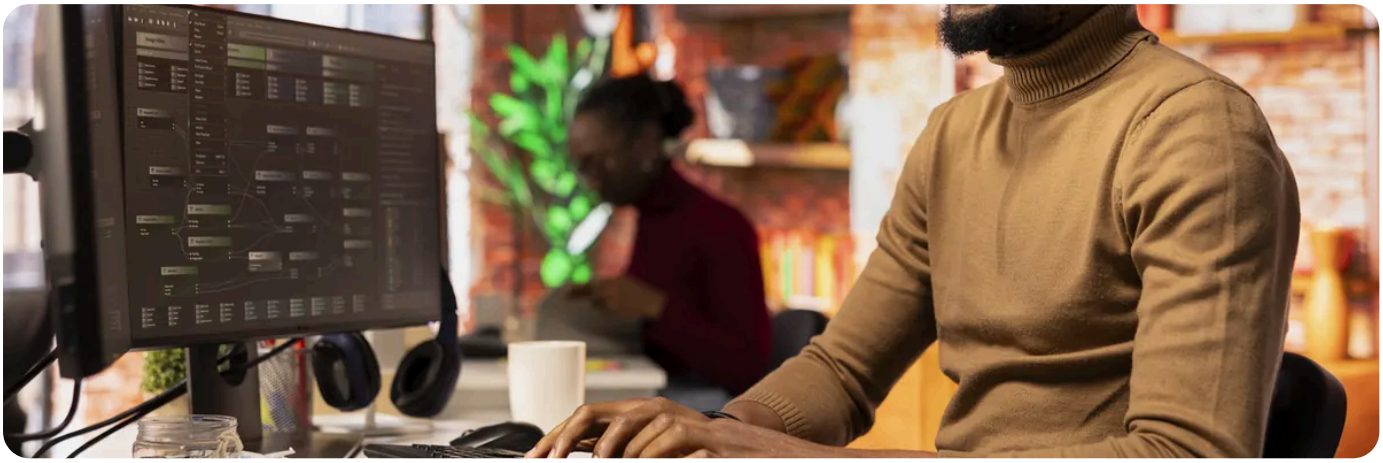
CODE	VERSION	COUNTRY · LANGUAGE
RLX-INT-KB-6876	v2026.10.21	International · English

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/6876

Your server IP on a spam blacklist: finding the source and getting off Spamhaus or SpamCop

Security Created on **October 21, 2026** 4 min read



This article is for customers with a VPS or a dedicated server, with root access. If you have a hosting plan, start with **your domain or IP is on a blacklist**. **The short answer:** your server's IP landed on a blacklist because, somewhere, someone saw spam coming from it, or traffic from an infected machine. Spamhaus and SpamCop are among the most widely used lists: with your IP on them, many mail servers refuse what you send. Sometimes a notice also comes from our network provider, with a short deadline, often a single day. The order never changes: **find the source, stop it, and only then ask for removal**.

The common lists, and what they mean

List	What it usually means	How to get off it
Spamhaus SBL	The IP was seen sending spam, or tied to a spam or phishing operation.	Fix the cause and ask for removal in the Spamhaus removal centre, explaining what you did.
Spamhaus XBL	An infected machine, or a program sending mail directly without going through a mail server.	Clean the server and ask for removal in the same centre. The lookup page tells you the step for your case.
Spamhaus PBL	Not a penalty: a list of IPs that should not send mail directly.	If you run a real mail server with reverse DNS, the Spamhaus page explains how to request an exclusion.
SpamCop	People who received spam from your IP and reported it.	It drops off by itself once the reports stop. SpamCop's lookup page tells you what applies to your IP.
Other lists	There are many smaller ones. Some charge for "express removal".	Do not pay: on the serious lists, removal is free.

Finding the source and getting off the list

1. **Confirm the list and the reason.** Look the IP up on the Spamhaus page (check.spamhaus.org) and on SpamCop's. Note the list, the date and the reason: it is your lead for the rest.

2. **Look at the mail queue.** A huge queue addressed to people you do not know is spam going out through the mail server: `mailq | tail -n 1`
`postqueue -p | head -50 # Postfix`
`exim -bpc # Exim (servers with cPanel/WHM)`

3. **Find out who is sending.** A mailbox with a stolen password shows up in the log by its user name; a website script shows up with the folder it runs from: `grep "sasl_username" /var/log/mail.log | tail -50 # Postfix (Debian/Ubuntu)`
`grep "sasl_username" /var/log/maillog | tail -50 # AlmaLinux/Rocky`
`grep "cwd=" /var/log/exim_mainlog | sort | uniq -c | sort -rn | head` If it is a hijacked mailbox, see **your e-mail account has been hacked**.

4. **Look for direct connections to port 25.** If a process shows up that is not your mail server (Postfix, Exim), it is malware sending spam on its own: `ss -tnp state established '( dport = :25 )'` In that case, follow **botnet activity reported from your server**.

5. **Stop the source.** Change the mailbox password, switch off the abused form or script, remove the malware. Then clear only the spam from the queue, message by message, with `postsuper -d MESSAGE_ID`. `postsuper -d ALL` also deletes legitimate mail that is waiting.

6. **Stop it happening again.** If the server does not need to send mail directly, close outgoing port 25 and send what you need through a **smarthost**: `ufw deny out 25/tcp` If you really run a mail server, check its **reverse DNS (PTR)** and **SPF, DKIM and DMARC**.

7. **Ask for removal and reply to us.** On Spamhaus, use the removal centre and explain in a few lines what you found and fixed. In the support ticket, send the report: **writing the reply to an abuse notice**.

Asking for removal before stopping the source is wasted effort.
The spam goes on, the IP is listed again, and lists are harder on repeat offenders. If sending continues after a notice, the server may be switched off to protect the network: **why the server was switched off or locked**.

If the IP was already listed before you started using the server,
open a support ticket with the lookup result: a new server with no mail going out is easy to explain in the removal request.

NEED A HAND?

Your IP is listed and you cannot find the source? Send us the list name, what the lookup shows and the output of the commands above.

Open a support ticket →

SEE ALSO

- Your domain or IP is on a blacklist: how to check and how to get off it
- An abuse notice about your server: what it means, the deadline and what we need from you
- Writing the reply to an abuse notice: cause, what you removed and how it will not happen again
- SMTP relay through a smarthost: sending mail from a VPS or from an application
- PTR and reverse DNS: why your e-mail depends on it
- Is my VPS compromised? Checking processes, cron jobs, users, SSH keys and temporary folders

mozout

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-6876 · v2026.10.21 · Generated on 21/10/2026 16:04