

KNOWLEDGE BASE · PUBLIC DOCUMENT

How to write an e-mail that does not land in spam: behaviour, recipients and limits

E-mail

CODE

RLX-INT-KB-746

VERSION

v2026.10.04

COUNTRY · LANGUAGE

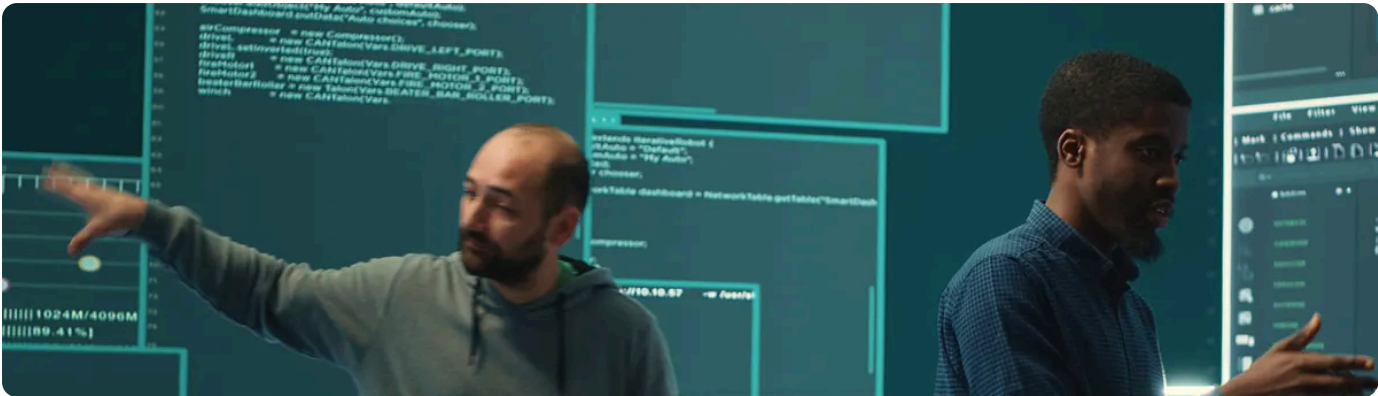
International · English

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/746>



An e-mail lands in spam for three kinds of reason: the domain is not authenticated, the message looks like spam, or the sending behaviour looks like a spammer's. The first is solved once and stays solved. The other two are habits.

The foundation: before touching wording or lists, make sure the domain has **SPF, DKIM and DMARC** in place. Without them nothing else saves the message - it is explained in **SPF, DKIM and DMARC**.

Behaviour: what the receiving server is judging

Do	Avoid
Send from a real address on your domain	Putting an address that is not yours in the From, or a Gmail pretending to be the domain
Keep a steady rhythm	Going quiet for months then firing 400 messages in one afternoon - the classic compromised-account pattern
Reply within existing conversations	Starting every contact from scratch to addresses that never wrote to you
Clean out addresses that bounce	Keeping on at addresses that no longer exist - repeated bounces wreck a domain's reputation
Sign with name, company and contact	Messages with no signature at all, which is how spam usually arrives

Recipients: where it goes wrong fastest

1

Write to people who know you. A bought list is the quickest way to burn a new domain, and there is no undoing it afterwards.

2

Never put dozens of people in To or Cc. Besides exposing everyone's address to everyone else, it is a strong bulk-sending signal. Use **Bcc** - or better, send one message per person.

3

If it is a newsletter, treat it as one. It needs a visible, working unsubscribe, and it should only go to people who asked for it.

4

Check the addresses before sending. Typos cause bounces, and too many bounces make you look like a machine guessing addresses.

The message: what makes a filter suspicious

Signal	How to fix it
Subject in ALL CAPS or with !!!	Write the subject as you would in a letter: clear, without shouting
Hard-sell words	"FREE", "URGENT", "CLICK NOW", "MAKE MONEY" - exactly the spam vocabulary. Say the same thing differently
The message is one big image	An e-mail with no real text, just a poster, is a spam signature. Put the essentials in text
Many links, or shortened links	Few links, all to your own domain. Shorteners hide the destination - and filters know it
Executable or compressed attachments	No .exe files, and avoid .zip. Put the file behind a link instead of attaching it
Written in a language the recipient does not use	Write in the reader's language - out-of-context text scores badly

Limits: ours, and the ones that actually count

On our side we do not impose a hard ceiling of messages per hour, and that is **not a licence for bulk sending**. The limit that decides whether your message arrives is not ours: it is the receiving server's, and that one is published nowhere - it adapts to your domain's reputation, day by day.

Limit	What to bear in mind
Messages per hour	No fixed ceiling on our side. But a sudden spike from shared hosting makes the whole server look suspicious - which hurts your neighbours and you
Recipients per message	Technically many fit; in practice, more than a few dozen in Bcc already looks like bulk mail. Split it up
Attachment size	Our server accepts large messages, but the recipient decides - most services cut off near 25 MB. For heavy files, send a link
Sending from your own mailbox	Fine for conversations. For campaigns, use a proper bulk-mail tool that handles unsubscribes and reputation

Something that protects everyone: we also scan the mail that **leaves** the server. It is not to police you - it is because one compromised account firing out spam is enough to put the whole server on blacklists, and then nobody's mail arrives. If an account of yours is used that way, we tell you.

For internal lists: cPanel includes **Mailing Lists**, which works well for closed groups (your team, the partners, a class). It is not a marketing-campaign tool - for that, a dedicated platform pays for itself.

Test before sending for real

1 Send the message to an address of yours **at another provider** (a Gmail, an Outlook.com) and see where it lands.

2 If it lands in spam, open it and look for whether the service states a reason - many do.

3 Fix one thing at a time and repeat. Changing five things at once tells you nothing about which was the problem.

If it still lands in spam after that, **write to us** - we can read the outbound log and tell you what the other side replied. And if your problem is the reverse, spam arriving in your mailbox, see **how to stop spam reaching your mailbox**.

Your messages still landing in customers' spam?

[Talk to us](#)

SEE ALSO

How to stop spam in Outlook: the filter on your computer and the one on the server

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

SPF, DKIM and DMARC: why your e-mail lands in spam

Need e-mail on your domain? See the Professional E-mail plans.

PROFESSIONAL E-MAIL

Your e-mail should carry your company name.

Mailboxes on your own domain, with webmail, antis spam and automatic setup on phone and desktop.

See e-mail plans

Works in Outlook, on your phone and in the browser



Online version of this document

MozOut is a leading internet services company, with a mission to help businesses to be born and prosper through technology.

2020

FOUNDED

37,000+

CLIENTS

130+

SIGN-UPS A DAY

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