Mozout

Generated on 15/11/2026 00:35

KNOWLEDGE BASE · PUBLIC DOCUMENT

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

Delivery & Spam

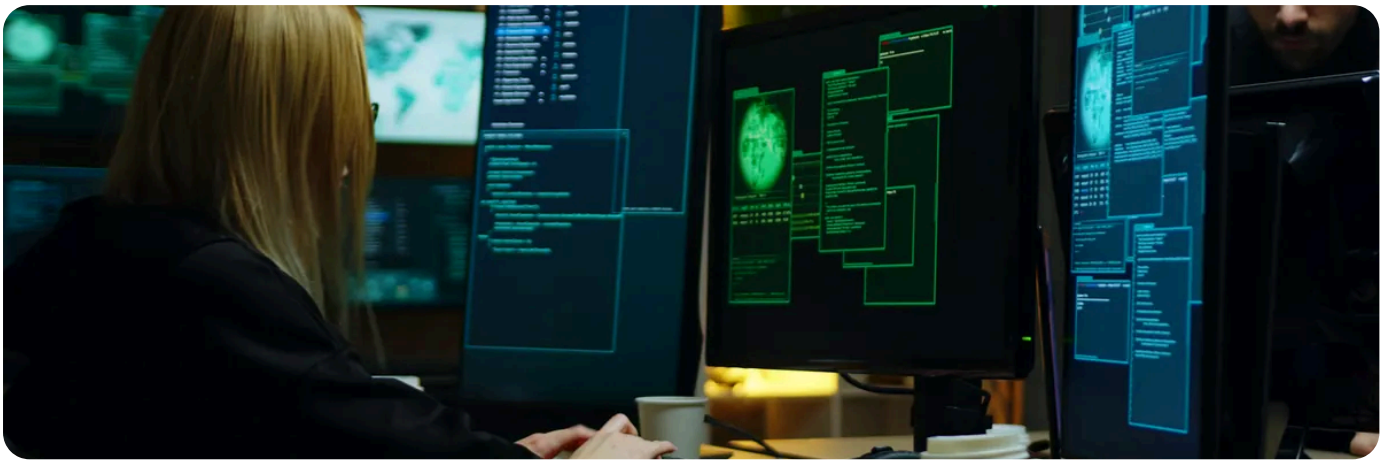
CODE	VERSION	COUNTRY · LANGUAGE
RLX-INT-KB-594	v2026.10.04	International · English

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/594

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

Delivery & Spam Created on **August 16, 2026** Updated on **October 4, 2026** 3 min read



E-mail was designed at a time when nobody lied about who they were. Today anyone can write a message pretending to come from your domain - and these three records are what prove yours is genuine.

Record	What it proves
SPF	The list of servers **allowed to send** on behalf of your domain. The receiver checks the message came from one of them.
DKIM	A **digital signature** on every message. It proves the message really left your system and nobody altered it on the way.
DMARC	The **instruction** for what to do when a message fails the other two: let it through, mark it as spam, or reject it.

Why this actually matters to you

Without these records, Gmail and Outlook.com have two choices - take a risk, or put it in spam. In doubt, they choose spam. That explains the overwhelming majority of *"they say they never got it"* cases. It is also what stops someone sending fake invoices in your company's name.

How it works with us

1. If the domain uses **our nameservers** , **SPF and DKIM are created automatically** when the account is opened. You need do nothing.

2. If the DNS is at another provider, the records exist on our side but **have to be copied there**. This is the silent cause of a lot of mail in spam folders - ask us for the values and we will send them.

3. **DMARC is not automatic**, and rightly so: a strict policy before everything else is in place will reject your own e-mail. You start by observing, and tighten later.

Checking it without leaving cPanel

You do not need an external site to find out whether these records are right: cPanel itself has a tool that runs the check and tells you what is missing.

1. In cPanel, search the bar for `Email Deliverability` and open the option it finds.

2. The list shows the account's domains. Beside each one it says **«No problems exist on this domain»** - all good - or **«Problems Exist»**.

3. If there are problems, click **Manage the Domain**. The page shows the state of **DKIM**, **SPF** and reverse DNS, and offers the suggested record for each one missing or wrong.

4. With the domain's DNS here, the fix can be applied from that page. If the DNS sits with another provider, copy the suggested value and create the record there - that is the most common cause of mail landing in spam for no apparent reason.

DMARC does not appear in this tool.
It checks DKIM, SPF and reverse DNS - DMARC is created separately, in the *Zone Editor*, as a TXT record named `_dmarc` on your domain. Always start with `p=none`, which only observes and sends reports; tightening to *quarantine* or *reject* before SPF and DKIM are right rejects your own mail.

If you send e-mail from other places

An invoicing system, an online shop, a campaign platform or the website contact form also send in your domain's name. Each of them has to be **included in the SPF**, or the messages leaving through them fail the check.

There can be only one SPF record.
When adding a new service you **merge** it into the existing SPF - you do not create a second one. Two SPF records cancel each other out, and that is worse than having none.

Before blaming the server
send yourself a test from **webmail** . If it reaches a Gmail address cleanly, domain reputation is not the problem - see **why your e-mail is not sending or receiving** .

NEED A HAND?

Is your e-mail landing in spam? We will check all three records for you.

Open a support ticket →

SEE ALSO

With the domain authenticated, the rest follows:

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

PROFESSIONAL E-MAIL

Your e-mail should carry your company name.

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

See e-mail plans →

Works in Outlook, on your phone and in the browser

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-594 · v2026.10.04 · Generated on 15/11/2026 00:35