

KNOWLEDGE BASE · PUBLIC DOCUMENT

Reading an e-mail header: did SPF, DKIM and DMARC pass?

E-mail

CODE

RLX-INT-KB-3204

VERSION

v2026.10.10

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/3204>



Every e-mail carries, hidden, a **header**: a technical report of where it passed through and how it was judged. It is the most direct proof for answering “why did it land in spam?” and “is this message really from who it says?”. You need no networking knowledge: just know where it is and which three lines to read.

How to open the header

Where you read the e-mail	What to do
Gmail	Open the message, the three-dots menu, Show original . The top already summarises SPF, DKIM and DMARC with PASS or FAIL.
Webmail (Roundcube)	Open the message and look for Headers or, in the More menu, View source .
Classic Outlook	Open the message, File , Properties , the Internet headers box.
Apple Mail	View menu, Message , All Headers (or Raw Source).
Thunderbird	View menu, Message Source .

The lines that matter

Line	What it says
Authentication-Results	The result of the three checks, written by the server that received the message. It is the main line.
Return-Path and From	The “technical” return address and the one shown as sender. If they belong to different domains, note which domain DMARC judges: the From one.
Received	Each server it passed through adds one. They are read from the bottom up: the bottom one is the first.
Message-ID	A unique identifier. It is what support asks for to find the message in the logs.

An example of what you look for, in the **Authentication-Results** line:

```
spf=pass smtp.mailfrom=yourcompany.com
dkim=pass header.d=yourcompany.com
dmarc=pass header.from=yourcompany.com
```

If the line is missing, the message did not pass through a server that writes them (rare at the big services). Always compare the domain shown in each check with the domain of the sender’s address.

What each result means

Result	Meaning and what to do
pass	The check succeeded. Nothing to do.
fail or softfail (SPF)	The message came from a server the domain did not authorise. See creating your SPF record .
dkim=none	The message did not leave signed. Check the key in Email Deliverability: the panel that audits your domain .
dkim=fail	The signature does not match: the message was altered on the way, or the published key is another one.
dmarc=fail	For DMARC to pass, SPF or DKIM must pass and match the From domain. See creating your DMARC record .

The header contains IP addresses and e-mail addresses. Do not post it on forums or social networks; send it only to whoever will read it, such as support. If you paste an excerpt, remove what is private.

The quickest test: send a message from your address to a Gmail of yours and open **Show original**. In two minutes you see whether SPF, DKIM and DMARC pass, with no third-party tools. The overview is in **SPF, DKIM and DMARC**.

Want us to look at the header with you? Send us the complete header, without the body of the message.

[Open a support ticket](#)

SEE ALSO

[SPF, DKIM and DMARC: why your e-mail lands in spam](#)

[Email Deliverability: the panel that audits your domain](#)

[Creating your SPF record, step by step](#)

[Creating your DMARC record, and reading what it sends back](#)



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