interweb

Generated on 15/11/2026 00:18

KNOWLEDGE BASE · PUBLIC DOCUMENT

Forwarded e-mail lands in spam or bounces: why SPF breaks and what to do

Delivery & Spam

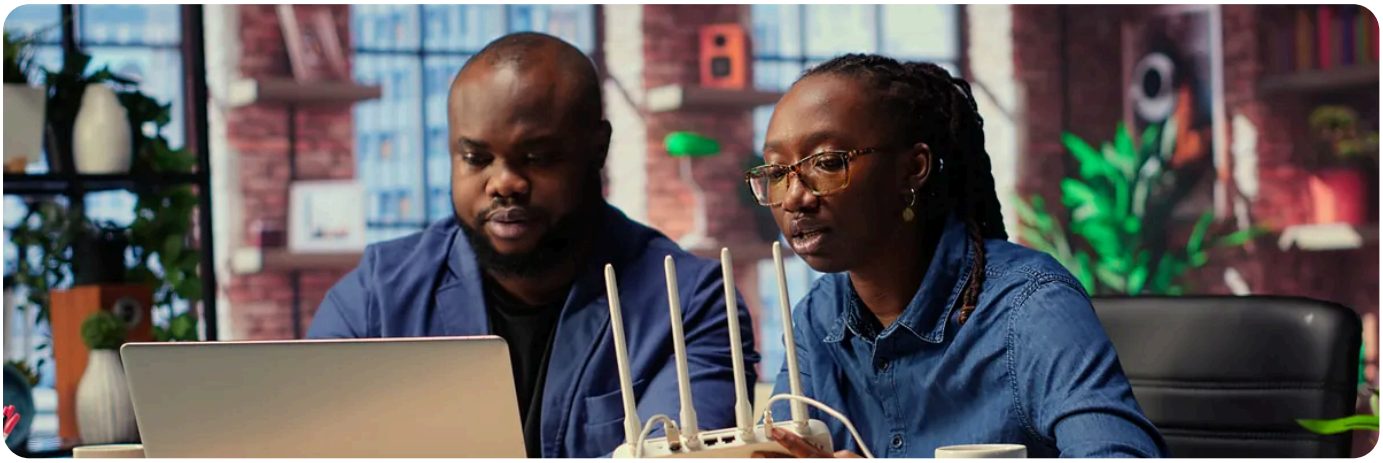
CODE	VERSION	COUNTRY · LANGUAGE
RLX-AO-KB-1908	v2026.10.15	Angola · English

Interweb Angola
RLX Angola, Lda. · Group RLX Holdings
Tax ID (NIF) 500 260 5724 · Commercial registration no. 26464-25/250724

https://www.meu.interweb.ao/knowledgebase/1908

Forwarded e-mail lands in spam or bounces: why SPF breaks and what to do

Delivery & Spam Created on **October 15, 2026** 2 min read



The short answer: when your address forwards messages to another (for example, to Gmail), the destination server sees the message arriving **from your server**, which is not on the list of who may send for the original sender. SPF fails, and the message falls into spam or is refused. There are three ways round it.

Why it happens

Step	What goes on
1. Someone writes to you	The sender (a bank, say) writes to your address on your domain.
2. Your server forwards	It hands the message to Gmail with the original sender's address, but from **your** server.
3. Gmail checks SPF	It asks the sender's domain whether your server is authorised. It is not. It fails.
4. The result	Spam, quarantine or refusal, especially if the sender has a strict policy (DMARC).
What survives	The DKIM signature, when there is one and it is not altered, passes the check even when forwarded.

What to do, in order of preference

1. **Instead of forwarding, let the other service fetch the e-mail:** Gmail, for example, can connect to your mailbox by POP or IMAP and bring the messages in. Then there is no forwarding. **POP or IMAP**.

2. **Or use the mailbox directly** on your phone or computer, with the domain's address, and skip the forwarding.

3 **If you really must forward,** the forwarding server should rewrite the sender (a technique called SRS). Ask us whether that is active in your case.

4 **Look at the header** of the affected message to confirm the cause: **Reading an e-mail header**.

5 **Get your own domain right too:** your domain's SPF, DKIM and DMARC tell others how to treat what comes from you: **SPF, DKIM and DMARC**.

! **Adding the forwarding server to the sender's SPF does not work:**
That is not in your hands (it is the other party's domain) and should not be. Those who can act are you, by changing how you receive, or the forwarder, by rewriting the sender.

Forwarders, aliases and catch-all are easily confused: **Catch-all, forwarders and aliases**. If the message came back with a code, see **Bounce message 550**.

NEED A HAND?

An important message does not arrive when forwarded? Open a ticket with that message's full header (no passwords).

Open a support ticket →

SEE ALSO

- **POP or IMAP: which to choose, and what you lose by picking wrong** →
- **Reading an e-mail header: did SPF, DKIM and DMARC pass?** →
- **SPF, DKIM and DMARC: why your e-mail lands in spam** →
- **Catch-all, forwarders and aliases: the three that get confused** →
- **Bounce message 550: user unknown, relay denied and rejected, what each one means** →

interweb

Interweb Angola

RLX Angola, Lda. · Group RLX Holdings

TAX ID (NIF)	500 260 5724
COMMERCIAL REGISTRATION NO.	26464-25/250724
REGISTERED OFFICE	Rua Direita do Patriota, Bairro Dangereux Belas, Luanda, Angola
CONTACT	info@interweb.ao · +244 942 011 191 · www.interweb.ao
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

Online version of this document

RLX-AO-KB-1908 · v2026.10.15 · Generated on 15/11/2026 00:18