interweb

Generated on 21/10/2026 17:25

KNOWLEDGE BASE · PUBLIC DOCUMENT

Someone is sending e-mail in the name of your domain: what SPF, DKIM and DMARC do about it

Security

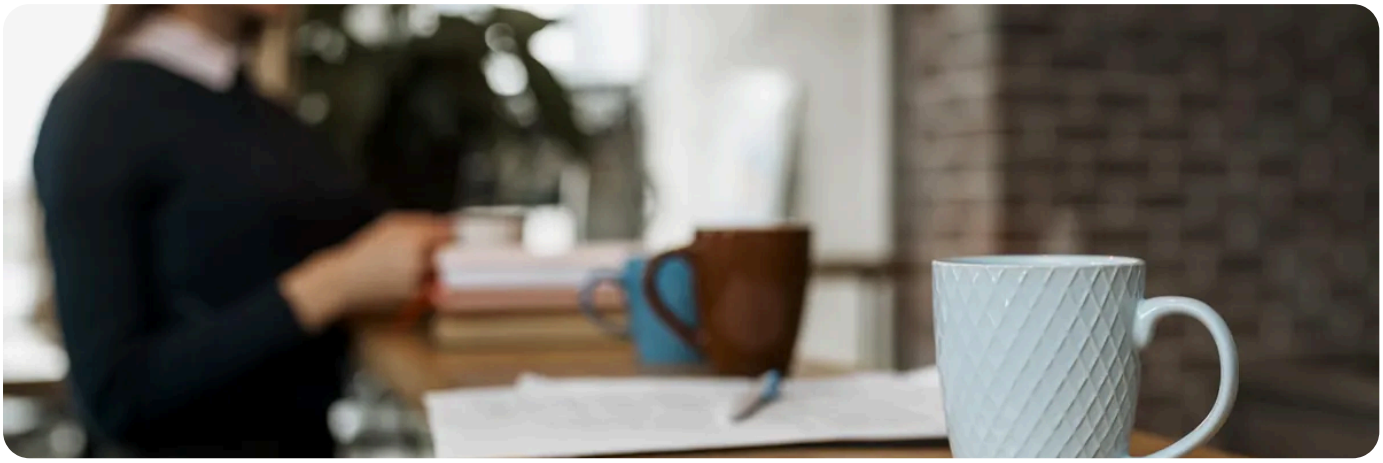
CODE	VERSION	COUNTRY · LANGUAGE
RLX-MZ-KB-1524	v2026.10.10	Mozambique · English

Interweb Mozambique
RLX Holdings, S.A. · Group RLX Holdings
Tax ID (NUIT) 401 191 607 · Legal entity no. (NUEL) 105 045 974 · Economic activity code (CAE) 62022

https://www.meu.interweb.co.mz/knowledgebase/1524

Someone is sending e-mail in the name of your domain: what SPF, DKIM and DMARC do about it

Security Created on **October 10, 2026** 3 min read



The short answer: sending an e-mail that looks as if it comes from `someone@asuaempresa.co.mz` is trivial: the sender address is written freely, like the return address on a letter. To stop that there are three records in the domain's DNS: **SPF**, **DKIM** and **DMARC**. The first two prove who may send; the third tells the world **what to do with messages that fail**. Without DMARC, the other two are only information.

What each one does

Record	The question it answers	How it works
SPF	"Is this server allowed to send for this domain?"	A list, in DNS, of the authorised servers.
DKIM	"Was the message really sent by who it says, and not altered?"	A digital signature on every message, checked against a public key in DNS.
DMARC	"What if a message fails both?"	The domain owner's policy: do nothing (`none`), quarantine (`quarantine`) or reject (`reject`), and where to send reports.

All three records live in the domain's **DNS**. If your domain uses Interweb's nameservers, you edit them in the cPanel DNS zone editor; if it uses others, it is wherever the DNS is managed. Without access to the zone there is no SPF, DKIM or DMARC, so it is worth knowing now where it is.

How to tell whether someone is using your name

1. **Signs from outside.** Customers receiving e-mails you did not send, bounces for messages that never left you, or spam complaints in your name.

2 **Read the DMARC reports.** If your record has an address for reports, you receive summaries of who sent messages using your domain, and how many passed or failed. See **creating your DMARC record, and reading what it sends back**.

3 **Run a diagnosis of the domain.** In cPanel, the deliverability tool audits SPF and DKIM: **the panel that audits your domain**.

How to close the door, in stages

1 **Get SPF and DKIM working.** The step by step is in **creating your SPF record**; the conceptual summary in **SPF, DKIM and DMARC: why your e-mail lands in spam**.

2 **Publish DMARC in `none` mode.** It blocks nothing; it just gives you the reports. Let it run for a while and confirm that your legitimate messages (from the site, the shop, the newsletter) pass.

3 **Move up to `quarantine`**, and later to `reject`, once your legitimate sources are all authorised. From then on, anyone forging your domain sees the messages rejected by the servers that respect DMARC.

! **Going straight to `reject` without reading the reports is the quickest way to lose legitimate e-mail.**

The invoicing system, the online shop or the newsletter service also send in the name of your domain. If they are not authorised in SPF or signed with DKIM, DMARC rejects them as if they were fake.

DMARC protects your *exact* domain. It does not stop someone registering a similar domain (with one letter swapped) and sending from there. Against that, only recipients' attention helps: see **how to recognise phishing**.

NEED A HAND?

Suspect your domain is being used to send e-mail? Send us an example with the full header.

Open a support ticket →

SEE ALSO

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

- **Creating your DMARC record, and reading what it sends back**
- **Creating your SPF record, step by step**
- **Email Deliverability: the panel that audits your domain**

interweb

Interweb Mozambique

RLX Holdings, S.A. · Group RLX Holdings

TAX ID (NUIT)	401 191 607
LEGAL ENTITY NO. (NUEL)	105 045 974
ECONOMIC ACTIVITY CODE (CAE)	62022
REGISTERED OFFICE	Bairro 7 de Setembro Vilankulo 1304 · CEP 0411-02, Inhambane, Mozambique
CONTACT	info@interweb.co.mz · +258 84 635 1111 · +258 86 635 1111 · www.interweb.co.mz
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

Online version of this document

RLX-MZ-KB-1524 · v2026.10.10 · Generated on 21/10/2026 17:25