

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Ler o cabeçalho de um e-mail: o SPF, o DKIM e o DMARC passaram?

E-mail

CÓDIGO

RLX-MZ-KB-3204

VERSÃO

v2026.10.18

PAÍS · IDIOMA

Moçambique · Português

MozOut Moçambique

RLX Holdings, S.A. · Grupo RLX Holdings

NUIT 401 191 607 · NUEL 105 045 974 · CAE 62022

<https://www.my.mozout.com/knowledgebase/3204>



Cada e-mail traz, escondido, um **cabeçalho** (header): um relatório técnico de por onde passou e de como foi avaliado. É a prova mais directa para responder a “porque foi parar ao spam?” e “esta mensagem é mesmo de quem diz?”. Não precisa de saber de redes: basta saber onde está e quais as três linhas a ler.

Como abrir o cabeçalho

Onde lê o e-mail	O que fazer
Gmail	Abra a mensagem, o menu dos três pontos, Show original . O topo já resume SPF, DKIM e DMARC com PASS ou FAIL.
Webmail (Roundcube)	Abra a mensagem e procure Headers ou, no menu More , View source .
Outlook clássico	Abra a mensagem, File , Properties , caixa Internet headers .
Apple Mail	Menu View , Message , All Headers (ou Raw Source).
Thunderbird	Menu View , Message Source .

As linhas que interessam

Linha	O que diz
Authentication-Results	O resultado das três verificações, escrito pelo servidor que recebeu a mensagem. É a linha principal.
Return-Path e From	O endereço “técnico” de retorno e o que aparece como remetente. Se forem de domínios diferentes, repare qual domínio o DMARC avalia: o do From.
Received	Cada servidor por onde passou acrescenta uma. Leem-se de baixo para cima: a de baixo é a primeira.
Message-ID	Um identificador único. É o que nos pede o suporte para procurar a mensagem nos registos.

Um exemplo do que procura, na linha **Authentication-Results** :

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

Se a linha não existir, a mensagem não passou por um servidor que as faça (é raro nos grandes serviços). Compare sempre o domínio que aparece em cada verificação com o domínio do endereço do remetente.

O que cada resultado quer dizer

Resultado	Significado e o que fazer
pass	Verificação bem-sucedida. Nada a fazer.
fail ou softfail (SPF)	A mensagem veio de um servidor que o domínio não autorizou. Veja criar o registo SPF .
dkim=none	A mensagem não saiu assinada. Confirme a chave no Email Deliverability: o painel que audita o domínio .
dkim=fail	A assinatura não bate certo: a mensagem foi alterada no caminho, ou a chave publicada é outra.
dmarc=fail	Para o DMARC passar, o SPF ou o DKIM têm de passar e corresponder ao domínio do From. Veja criar o registo DMARC .

O cabeçalho tem endereços IP e endereços de e-mail. Não o publique em fóruns nem em redes sociais; mande-o só a quem o vai ler, como o suporte. Se cola um excerto, retire o que é privado.

O ensaio mais rápido: envie uma mensagem do seu endereço para um Gmail seu e abra **Show original**. Em dois minutos vê se o SPF, o DKIM e o DMARC passam, sem ferramentas de terceiros. O panorama geral está em **SPF, DKIM e DMARC**.

Quer que olhemos para o cabeçalho consigo? Envie-nos o cabeçalho completo, sem o corpo da mensagem.

[Abrir um pedido de suporte](#)

VEJA TAMBÉM

SPF, DKIM e DMARC: porque o seu e-mail cai no spam

Email Deliverability: o painel que audita o seu domínio

Criar o seu registo SPF, passo a passo

Criar o seu registo DMARC e ler o que ele devolve



Versão online deste documento

A MozOut é uma empresa líder em serviços de internet, com a missão de ajudar negócios a nascerem e prosperarem por meio da tecnologia.

2020

FUNDADA

37 mil+

CLIENTES

130+

INSCRIÇÕES POR DIA

MozOut Moçambique

RLX Holdings, S.A. • Grupo RLX Holdings

NUIT 401 191 607

NUEL 105 045 974

CAE 62022

SEDE Bairro 7 de Setembro
Vilankulo 1304 • CEP 0411-02, Inhambane, Moçambique

CONTACTOS info@mozout.com • +258 84 635 1111 • +258 86 635 1111 •
www.mozout.com

HORÁRIO 2ª. à 6ª. Feira - 08 à 16 Horas
Sábado & Domingo - Fechado