

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

# E-mails no lixo eletrônico do Hotmail e do Outlook.com: o que o remetente pode verificar

E-mail

CÓDIGO

RLX-BR-KB-6246

VERSÃO

v2026.10.18

PAÍS · IDIOMA

Brasil · Português (Brasil)

## MozOut Brasil

RLX Holdings (Pty) Ltd. · Grupo RLX Holdings

N.º fiscal (SARS) 943 907 6234 · N.º de registo (CIPC) 2025/667953/07

<https://www.my.mozout.com/knowledgebase/6246>

# E-mails no lixo eletrônico do Hotmail e do Outlook.com: o que o remetente pode verificar

 E-mail  Criado em 16 de outubro de 2026  Atualizado em 18 de outubro de 2026  3 min de leitura



**A resposta curta:** quando os seus e-mails chegam a quem usa Hotmail ou Outlook.com mas caem no **Lixo Eletrônico**, foram aceitos pela Microsoft e depois classificados como suspeitos. A Microsoft não publica a receita exata do filtro, mas o que pesa está do seu lado e pode ser verificado: a **autenticação** do domínio (SPF, DKIM e DMARC), a **reputação** do domínio e do servidor, o **conteúdo** e o **comportamento** de quem recebe.

## Sintomas e causas

| Sintoma                                                 | Causa mais provável                                                                                                                                 |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Todos os seus e-mails vão para o lixo, mesmo os simples | Falta ou está errado o <b>SPF</b> , o <b>DKIM</b> ou o <b>DMARC</b> do domínio. Veja <b>SPF, DKIM e DMARC</b> .                                     |
| Começou de repente, com o domínio já antigo             | Mudou alguma coisa: um registro DNS alterado, um serviço novo a enviar em seu nome sem estar no SPF, ou o domínio ou o IP numa <b>lista negra</b> . |
| O domínio é novo                                        | Ainda não tem histórico. A reputação constrói-se devagar: <b>um domínio novo a enviar e-mail</b> .                                                  |
| Só as newsletters ou os envios em massa                 | Volume, listas antigas, destinatários que nunca abrem ou que marcam como lixo. Veja <b>e-mail marketing bem feito</b> .                             |
| Só certas mensagens                                     | O conteúdo: só uma imagem, links encurtados, anexos de risco, assunto em maiúsculas. Veja <b>como escrever um e-mail que não cai no spam</b> .      |

## O que o remetente pode verificar

- 1 Faça um teste a si próprio:** crie ou use uma conta Hotmail ou Outlook.com sua, envie-lhe uma mensagem simples do seu endereço e veja em que pasta cai.

**2** **Leia o cabeçalho dessa mensagem:** no Outlook.com, abra a mensagem, clique nos três pontos e procure **Ver > Ver origem da mensagem**. Procure as linhas de autenticação e veja se o SPF, o DKIM e o DMARC dizem *pass*. Como se lê: **ler o cabeçalho de um e-mail**. Os nomes dos menus da Microsoft mudam com as atualizações e com a língua: se não encontrar o caminho exato, use a pesquisa das Configurações.

**3** **Abra o Email Deliverability no cPanel:** ele mostra se o SPF e o DKIM do domínio estão como devem e propõe a correção. Veja **o painel de entregabilidade**.

**4** **Confirme o DMARC:** se não tem, crie-o, começando por uma política que só observa. Veja **criar o registro DMARC**.

**5** **Confirme as listas negras do domínio e do IP de envio:** **como verificar e como sair**.

**6** **Peça a quem recebe** que marque a sua mensagem como **Não é lixo** e que acrescente o seu endereço aos **Remetentes seguros** (no Outlook.com, em Configurações > E-mail > Lixo eletrônico). Ajuda essa pessoa, mas não corrige a causa para os outros destinatários.



### **Não tente «enganar» o filtro**

com truques no assunto, texto escondido ou envio a partir de outro domínio. Isso piora a reputação e pode fazer a Microsoft passar de enviar para o lixo a recusar as mensagens. Corrija a autenticação e o comportamento.



### **Se envia de um site**

(formulários, WordPress, loja), essas mensagens também usam o seu domínio: devem sair pelo nosso servidor com SMTP autenticado, para passarem no SPF e no DKIM. Se usa um serviço externo de envio, ele tem que estar no SPF e assinar com DKIM do seu domínio.



### **PRECISA DE AJUDA?**

Já confirmou a autenticação e continua caindo no lixo? Envie-nos o cabeçalho completo de uma mensagem de teste.



**Abrir pedido de suporte →**

**VEJA TAMBÉM**[SPF, DKIM e DMARC: porque o seu e-mail cai no spam](#)[Ler o cabeçalho de um e-mail: o SPF, o DKIM e o DMARC passaram?](#)[Entregabilidade de e-mail: o painel que audita o seu domínio](#)[O seu domínio ou IP está numa lista negra: como verificar e como sair](#)[Um domínio novo a enviar e-mail: como criar reputação sem cair no spam](#)[O Hotmail ou o Outlook.com recusa ou atrasa os seus e-mails: ler a mensagem que volta](#)**mozout****MozOut Brasil**

RLX Holdings (Pty) Ltd. · Grupo RLX Holdings

|                       |                                                                      |
|-----------------------|----------------------------------------------------------------------|
| N.º FISCAL (SARS)     | 943 907 6234                                                         |
| N.º DE REGISTO (CIPC) | 2025/667953/07                                                       |
| SEDE                  | 72 York Road, Kensington<br>Joanesburgo 2094, Gauteng, África do Sul |
| CONTACTOS             | info@mozout.com · +27 78 823 3325 · www.mozout.com                   |
| HORÁRIO               | 2ª. à 6ª. Feira - 08 à 16 Horas<br>Sábado & Domingo - Fechado        |

RLX-BR-KB-6246 · v2026.10.18 · Gerado a 21/10/2026 13:31

Versão online deste  
documento