Mozout

Gerado a 13/11/2026 14:55

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Ameaças enviadas do seu próprio endereço: porque os e-mails de extorsão parecem vir de si

Segurança

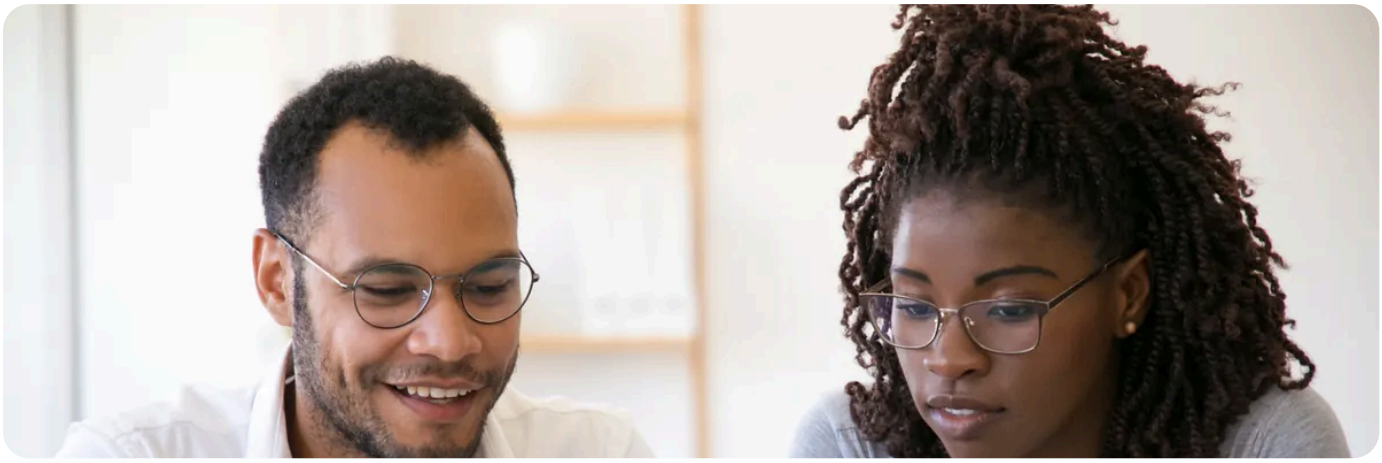
CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-BR-KB-7296	v2026.11.13	Brasil · Português (Brasil)

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/7296

Ameaças enviadas do seu próprio endereço: porque os e-mails de extorsão parecem vir de si

Segurança Criado em **13 de novembro de 2026** 3 min de leitura



A resposta curta: recebeu um e-mail que parece enviado **do seu próprio endereço**, a dizer que a sua caixa ou o seu computador foram invadidos e a pedir dinheiro em criptomoeda para não divulgar nada. Quase sempre é **falso**: o remetente de um e-mail é só um texto que qualquer um pode escrever, como o remetente de uma carta. **Não responda, não pague e não clique em nada.** Depois, confirme duas coisas simples, que estão abaixo.

Porque parece vir de si

O campo «De» de um e-mail não é verificado por quem envia, e o burlão escreve lá o seu endereço para o assustar: «se envio do seu endereço, é porque entrei na sua conta». Não entrou. A mensagem saiu de um servidor qualquer, longe do nosso. Se abrir o cabeçalho, as linhas Received mostram por onde ela passou: **como ler o cabeçalho**.

Às vezes, a mensagem cita uma **senha verdadeira** sua. Isso assusta mais, mas tem outra explicação: a senha veio de uma fuga de dados antiga de um site onde se registrou, e anda em listas que se vendem na internet. Não quer dizer que a sua caixa foi invadida, mas quer dizer que essa senha já não serve para nada.

O que fazer

1. **Não responda nem pague.** Responder confirma que o endereço é lido por uma pessoa, e pagar só traz mais mensagens.
2. **Marque como spam** no webmail ou no programa de e-mail e apague.
3. **Se a mensagem cita uma senha que ainda usa,** mude-a já em todos os lugares onde a usa, a começar pela caixa de e-mail: **mudar a senha da caixa**.
4. **Confirme que a caixa não envia nada sozinha:** veja a pasta Enviados no webmail. Se lá estiverem mensagens que não escreveu, aí sim, há um problema: siga **o que fazer quando a conta foi pirateada**.

Como reduzir estas mensagens

O registro **DMARC** do seu domínio diz aos servidores de destino o que fazer com mensagens que usam o seu domínio sem autorização. Com uma política mais rigorosa, muitas destas mensagens falsas são recusadas ou vão para o spam, nas caixas dos seus clientes e na sua. Veja **alguém envia e-mails em nome do seu domínio**.

Não abra anexos nem links destas mensagens.
Algumas trazem um «comprovante» que é, na verdade, um programa malicioso. Se já abriu, veja **o que fazer se clicou**.

Avise a equipe.
Estas mensagens chegam muitas vezes a várias pessoas da empresa ao mesmo tempo. Um aviso curto evita que alguém pague por medo.

PRECISA DE AJUDA?

Recebeu uma mensagem destas e quer confirmar se a sua caixa está segura? Abra um pedido e verificamos consigo.

Abrir pedido de suporte →

VEJA TAMBÉM

- Alguém envia e-mails em nome do seu domínio: o que fazem o SPF, o DKIM e o DMARC →
- Como reconhecer um e-mail ou mensagem de phishing, e o que fazer se clicou →
- A sua conta de e-mail foi pirateada: o que fazer na primeira hora →
- Ler o cabeçalho de um e-mail: o SPF, o DKIM e o DMARC passaram? →
- Como alterar a senha de uma conta de e-mail →
- Senha forte e gerenciador de senhas: como deixar de repetir a mesma senha →

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 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 Sábado & Domingo - Fechado

Versão online deste documento

RLX-BR-KB-7296 · v2026.11.13 · Gerado a 13/11/2026 14:55