Gerado a 20/10/2026 08:51

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Como saber se um e-mail é mesmo nosso

Segurança

CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-AO-KB-1044	v2026.10.18	Angola · Português

MozOut Angola
RLX Angola, Lda. · Grupo RLX Holdings
NIF 500 260 5724 · Matrícula 26464-25/250724

https://www.my.mozout.com/knowledgebase/1044

Uma mensagem falsa a fingir ser do seu fornecedor de hospedagem é o ataque mais comum contra contas como a sua - e o mais rentável para quem o faz, porque uma só senha dá acesso ao site, ao e-mail e ao domínio de uma vez. Vale a pena saber distinguir.

De que endereços é que nós escrevemos

Escrevemos **sempre a partir de** `mozout.com`, e só destes quatro endereços:

Endereço	Para quê
noreply@mozout.com	Mensagens automáticas: facturas, avisos de renovação, activações. Não recebe respostas.
support@mozout.com	Respostas a pedidos de apoio técnico.
sales@mozout.com	Vendas e assuntos financeiros.
info@mozout.com	Contacto geral.

> **Mas isto, sozinho, não prova nada.** O nome que aparece no remetente **escreve-se como se quiser**. Qualquer pessoa pode enviar uma mensagem que *diz* vir de `support@mozout.com`. É por isso que este artigo não acaba aqui: olhar para o endereço é o primeiro passo, e não é a prova.

O que confirma mesmo: o cabeçalho

Toda a mensagem leva consigo um registo de verificações que o servidor de destino fez. São três, e o que interessa é que digam **PASS**:

```
spf=pass      o servidor que enviou estava autorizado
dkim=pass     a assinatura bate certo e ninguém alterou a mensagem
dmarc=pass o domínio do remetente confere com essa assinatura
```

1 No **Gmail**, abra a mensagem, clique nos três pontos e escolha *Mostrar original*. As três linhas estão logo no topo.

2 No **Outlook**, abra a mensagem numa janela própria e vá a *Ficheiro* → *Propriedades*, no campo dos cabeçalhos.

3 No **webmail**, procure a opção de ver a mensagem em bruto ou a origem.

Se alguma delas disser **fail** ou **softfail**, desconfie - mesmo que o endereço pareça certo. Sobre o que estes três registos são e como funcionam, ver **SPF, DKIM e DMARC**.

Os sinais de uma mensagem falsa

Sinal	Porque é suspeito
Urgência com ameaça	«A sua conta será suspensa em 24 horas.» A pressão serve para o fazer clicar antes de pensar. Os nossos avisos dão-lhe **dias**, e estão sempre visíveis no portal.
O link não vai para onde diz	Passe o rato por cima sem clicar e leia o endereço real, em baixo. No telemóvel, mantenha o dedo premido. Se não começa por **https://www.my.mozout.com**, não é nosso.
Pede a senha	Nunca a pedimos. Nem por e-mail, nem por chat, nem ao telefone.
Muda dados de pagamento	O sinal mais caro de todos. Ver a secção abaixo.
Anexo que não esperava	Facturas nossas são PDF e estão sempre no portal. Um ficheiro .zip, .exe ou um documento que pede para activar macros nunca é nosso.
Português estranho	Tradução automática, o seu nome errado, ou um tratamento que não é o habitual.

O que nós nunca lhe pedimos

1. **Nunca lhe pedimos a senha.** Não precisamos dela para nada: do nosso lado vemos o que é preciso sem ela. Quem lha pedir não somos nós.

2. **Nunca lhe pedimos para confirmar dados de cartão por e-mail**, nem por formulário fora do portal.

3. **Nunca lhe mandamos um código de verificação para nos dizer.** Se receber um código que não pediu, alguém está a tentar entrar na sua conta - mude a senha e ligue a **verificação em duas etapas**.

A fraude da conta bancária trocada - leia esta com atenção. Há um golpe específico que ataca quem paga por transferência: chega uma mensagem que parece nossa a dizer que **mudámos de banco** e a pedir que pague para uma conta nova. **Não pague.** Os nossos dados bancários estão na factura dentro do portal, e são esses que valem. Se alguma vez mudarmos de conta, isso aparecerá no portal - e mesmo assim, ligue-nos a confirmar antes de transferir. Uma transferência enviada não se desfaz.

A regra que dispensa todas as outras

Não clique no e-mail. Vá ao portal. Escreva `www.my.mozout.com` no navegador, com as suas mãos, e entre. Se a mensagem for verdadeira, o que ela diz está lá: a factura, o aviso, o pedido. Se não estiver lá, não existe.

Esta única regra torna quase todos os golpes inúteis, e não exige que perceba nada de cabeçalhos.

Já cliquei. E agora?

1. **Mude a senha já** - a do portal e a do cPanel, se forem parecidas. Ver **como recuperar o acesso à sua conta**.

2	**Ligue a verificação em duas etapas.** A partir daí, só a senha deixa de chegar a quem a roubou.

3	**Veja o que mudou:** contas de e-mail que não criou, reencaminhamentos novos, os dados de contacto da conta, e os nameservers dos seus domínios.

4	**Avise-nos** pelo **portal, abrindo um pedido** - conseguimos ver os acessos recentes e dizer-lhe se alguém entrou.

Se desconfia que o próprio site foi mexido, o caminho é outro: **como saber se o seu site foi comprometido**.

Recebeu uma falsa? Diga-nos

Reencaminhe-a para `support@mozout.com` com os cabeçalhos incluídos, se souber como. Serve para avisarmos os outros clientes e para pedirmos o encerramento do endereço usado. Não é incomodar - é útil.

Recebeu alguma coisa estranha em nosso nome? Mostre-nos.

Abrir um pedido

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	37 mil+	130+
FUNDADA	CLIENTES	INSCRIÇÕES POR DIA

MozOut Angola

RLX Angola, Lda. · Grupo RLX Holdings

NIF	500 260 5724
MATRÍCULA	26464-25/250724
SEDE	Rua Direita do Patriota, Bairro Dangereux Belas, Luanda, Angola
CONTACTOS	info@mozout.com · +244 942 011 191 · www.mozout.com
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado

RLX-AO-KB-1044 · v2026.10.18 · Gerado a 20/10/2026 08:51