

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Um aviso vermelho do Google («Site enganador à frente»): o que significa e como pedir uma revisão

Segurança

CÓDIGO

RLX-AO-KB-1994

VERSÃO

v2026.10.15

PAÍS · IDIOMA

Angola · Português

Interweb Angola

RLX Angola, Lda. · Grupo RLX Holdings

NIF 500 260 5724 · Matrícula 26464-25/250724

<https://www.meu.interweb.ao/knowledgebase/1994>



A resposta curta: se quem abre o seu site vê uma página vermelha do navegador a dizer «**Site enganador à frente**» ou «**O site à frente contém software malicioso**», o Google marcou-o como perigoso. Quase sempre é porque o site **foi invadido** e alguém pôs lá uma página falsa ou um código malicioso. O aviso só sai depois de **limpar o site e pedir uma revisão**.

O que o site precisa

O quê	O que fazer
« Site enganador » (engano)	Há uma página que imita outra (um banco, um e-mail) para roubar dados. Costuma estar escondida numa pasta do seu site.
« Software malicioso »	O site tenta instalar ou descarregar algo nocivo para quem o visita.
« Site perigoso »	Aviso mais geral. Veja o motivo na ferramenta do Google.
Onde ver o motivo	No Search Console, em «Problemas de segurança», se o site está registado: Search Console .
Quanto dura	Enquanto o Google não revê o site depois de limpo. Pedir antes de limpar só atrasa.

Como começar

1

Não apague tudo às cegas. Primeiro veja o que está lá: o Search Console mostra exemplos de endereços.

2

Faça uma análise ao site: **Análise de malware no cPanel** e, se o aviso persiste, **onde se esconde uma infeção**.

3

Reponha uma cópia limpa se tiver uma: **Depois de um ataque, que cópia repor**.

4

Mude todas as senhas (cPanel, FTP, base de dados, WordPress) e atualize o que estiver desatualizado: **Proteger o login do WordPress**.

5

Só depois de limpo, peça a revisão no Search Console, explicando o que fez. A resposta pode demorar; o aviso desaparece quando o Google confirmar.

Se pedir a revisão sem limpar, o pedido é recusado e a espera fica maior. Se a página falsa voltar, é porque a entrada do atacante não foi fechada (uma senha, um plugin velho): limpar sem fechar a porta não resolve. **Ficheiros que nunca devem ficar públicos**.

Se foi você que recebeu uma mensagem falsa e clicou: **Como reconhecer uma mensagem falsa**. Para ficar protegido a seguir: **Ransomware**.

O seu site tem o aviso vermelho e quer ajuda a limpá-lo? Abra um pedido com o endereço, já.

Abrir pedido de suporte

VEJA TAMBÉM

Indexar o site no Google Search Console, passo a passo

Analisar o site à procura de malware no cPanel: o que o Imunify encontra e o que fazer com o resultado

A análise diz que está limpo mas o site continua a redirecionar: onde se esconde a infeção

Depois de um ataque, que cópia restaurar? Como escolher uma cópia limpa

Como reconhecer um e-mail ou mensagem de phishing, e o que fazer se clicou



Versão online deste documento

A Interweb 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

Interweb 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@interweb.ao • +244 942 011 191 • www.interweb.ao
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado