interweb

Gerado a 15/11/2026 00:25

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Tirar o aviso vermelho do Google do seu site

Sites atacados e malware

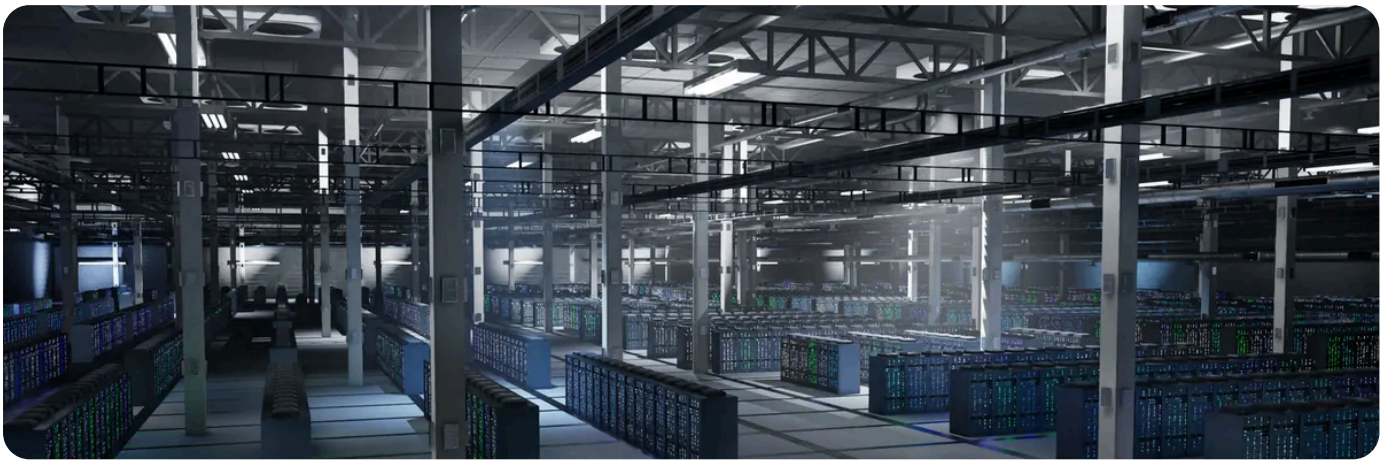
CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-AO-KB-666	v2026.10.28	Angola · Português

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

https://www.meu.interweb.ao/knowledgebase/666

Tirar o aviso vermelho do Google do seu site

Sites atacados e malware · Criado em **27 de setembro de 2026** · Atualizado em **28 de outubro de 2026**
4 min de leitura



É o ecrã vermelho a tapar o site inteiro, com uma frase do género «o site à frente contém software malicioso» ou «site enganador à frente». Não é o navegador a ser exagerado: é um sinal público de que alguma coisa foi encontrada no seu site. Enquanto lá estiver, praticamente ninguém entra.

> **O aviso é o sintoma, não a doença.**
> Limpe primeiro, peça a revisão depois. Pedir a revisão com o site ainda infectado faz o Google confirmar o problema, e a segunda marca é mais difícil de tirar do que a primeira.

Primeiro: ver o que o Google encontrou

1. Abra o **Search Console** e vá a **Segurança e acções manuais**, depois **Problemas de segurança**.
2. Leia o **tipo** de problema e a **lista de endereços de exemplo**. Essa lista é o mapa do que ele viu, e poupa-lhe horas às cegas.
3. **Se ainda não tem o site no Search Console, adicione-o agora.** Sem ele, fica sem saber o que foi encontrado e sem forma de pedir a revisão.

Tipo de aviso	O que costuma estar por trás
Software malicioso	Ficheiros injectados no site, quase sempre por um plugin ou tema desactualizado
Software indesejado	Publicidade agressiva, redireccionamentos, ou um script de terceiros que foi comprometido
Engenharia social	Páginas de phishing metidas numa pasta do seu site, a imitar um banco ou um serviço conhecido

Tipo de aviso	O que costuma estar por trás
Descargas perigosas	Ficheiros para descarregar que o Google considera nocivos

Limpar o site

Temos o **Imunify360** no servidor, e o cPanel da sua conta tem o ícone dele na secção de **Segurança** (conforme a versão, aparece como **Imunify360** ou **Imunify Security**). É por aí que se começa.

1. **Abra o Imunify no cPanel e corra uma análise.** Ele lista os ficheiros marcados e deixa limpar ou pôr em quarentena.

2. **Mude todas as senhas**: cPanel, FTP, base de dados, administradores do WordPress e contas de e-mail. Se não mudar, quem entrou volta a entrar: **mudar a senha do cPanel**.

3. **Actualize o núcleo, os temas e os plugins**, e apague os que não usa. Um tema desactivado continua a ser código no servidor.

4. **Reveja os utilizadores administradores** do WordPress. Um administrador que você não criou é a assinatura de quem entrou.

5. **Procure o que ficou para trás**: linhas estranhas no .htaccess, código no princípio ou no fim de ficheiros PHP, e tarefas agendadas que não reconhece.

6. **Se não ficar limpo, reponha uma cópia anterior à infecção** e volte a actualizar tudo antes de a pôr no ar: **restaurar uma cópia sem abrir pedido**.

O procedimento completo, com o detalhe todo, está em **como resolver um site infectado por malware**. Para confirmar se há mesmo infecção antes de mexer, veja **como saber se o meu site está infectado**.

> **Repor uma cópia sem tapar o buraco é reinfectar.**
> A cópia devolve os ficheiros ao estado anterior, incluindo o plugin desactualizado por onde entraram. Actualize e mude as senhas antes de voltar a abrir ao público.

Pedir a revisão ao Google

1. **Confirme, endereço a endereço**, que os exemplos que ele listou já estão limpos. Abra-os você mesmo.

2. No Search Console, em **Problemas de segurança**, clique em **Pedir uma revisão**.

3. **Escreva o que fez.** Que ficheiros estavam infectados, como foram limpos, que senhas mudou e o que actualizou. Um texto concreto é lido de outra maneira do que «já está resolvido».

4. **Espere e não repita o pedido.** Insistir não acelera e pode atrasar. Enquanto espera, não mexa mais no site.

Não prometemos prazos por uma razão simples: quem decide é o Google, e não publica um prazo que possamos garantir. Quando ele levantar o aviso, ele desaparece sozinho em todos os navegadores.

E se não for infecção?

Causa	Como se confirma
Publicidade de terceiros	Uma rede de anúncios comprometida põe conteúdo mau numa página limpa. Desligue os anúncios e peça a revisão
Um script externo	Contadores, chats e widgets antigos carregam código de sítios que já mudaram de dono. Tire o que não usa
Um subdomínio esquecido	Uma instalação antiga num subdomínio arrasta o domínio principal. Procure tudo o que tem no plano
Um formulário que pede senhas	Uma página sua que pede dados de acesso de outro serviço pode ser lida como phishing, mesmo sem má intenção

Não confunda com o aviso do certificado.
O ecrã de «ligação não privada» é outra coisa, e resolve-se de outra maneira: **o cadeado não aparece: as causas, por ordem**.

Para não voltar

1. **Actualizar é a defesa principal.** Quase todas as invasões que vemos entram por plugin ou tema desactualizado.

2. **Tranque a entrada do WordPress**: **três passos por ordem de efeito**.

3. **Tenha cópias suas e testadas**, além das nossas: **fazer e testar a sua própria cópia**.

4 **Apague o que não usa.** Instalações antigas em subpastas são a porta mais usada de todas.

PRECISA DE AJUDA?

O site está marcado e não consegue limpá-lo sozinho?

Abrir um pedido de suporte →

VEJA TAMBÉM

- **Como resolver um site infectado por malware** →
- **Como saber se o meu site está infectado por malware** →
- **Aparecer no Google: Perfil de Empresa, Search Console e o básico** →
- **O que fazemos pela segurança, DDoS incluído, e o que fica do seu lado** →
- **Indexar o site no Google Search Console, passo a passo** →

interweb

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

Versão online deste documento

RLX-AO-KB-666 · v2026.10.28 · Gerado a 15/11/2026 00:25