Gerado a 15/11/2026 01:41

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Como resolver um site infectado por malware

Sites atacados e malware

CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-PT-KB-236	v2026.10.18	Portugal · Português

MozOut Portugal
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/236

Como resolver um site infectado por malware

Sites atacados e malware · Criado em **14 de agosto de 2026** · Atualizado em **18 de outubro de 2026** · 3 min de leitura



Limpar é só metade do trabalho - se a porta que deixou entrar a infecção continuar aberta, ela volta. Siga esta ordem.

1. Ver o que foi detectado

1. No cPanel, abra **Imunify Security** e reveja o que está listado em itens detectados ou em quarentena - isto diz-lhe quais os ficheiros afectados antes de mudar seja o que for.

2. Mude todas as senhas, imediatamente

1. A maioria das infecções começa com uma senha roubada ou adivinhada, não com uma falha misteriosa. Mude a senha do cPanel, a senha de administrador do CMS (WordPress, Joomla...), e a senha da respectiva base de dados.

2. Se várias pessoas têm acesso (veja **gerir sub-contas**, se aplicável), peça a todos que mudem a sua também - não só ao titular da conta.

3. Actualize tudo

1. Actualize o núcleo do CMS, todos os plugins e todos os temas para as versões mais recentes. Um plugin desactualizado é a forma mais comum de um site ser comprometido.

2. Remova por completo qualquer plugin ou tema que já não use, em vez de o deixar apenas desactivado - código não usado continua a ser um alvo.

4. Restaure de uma cópia limpa, se tiver

1. Se tiver uma cópia de segurança anterior à infecção, restaurá-la pode ser mais rápido do que a limpeza manual - mas garanta que também completa os passos 2 e 3 a seguir, ou a mesma brecha deixa a infecção voltar de imediato.

Não apague apenas o aviso ou o ficheiro assinalado.
Se um plugin foi explorado para o colocar ali, remover só esse ficheiro deixa a vulnerabilidade aberta e a infecção normalmente volta em poucos dias.

Continua a mostrar avisos depois disto, ou não sabe por onde começar? **Abra um pedido de suporte** e descreva o que o Imunify Security assinalou - podemos aconselhar os próximos passos.

PRECISA DE AJUDA?

Quer uma segunda opinião antes de mexer em algo? Pergunte-nos primeiro.

Abrir um pedido de suporte →

Nos nossos planos

- Todos os planos de alojamento têm cópia de segurança automática diária, e o restauro não tem custos.
- Para ver que pontos de restauro a sua conta tem, abra JetBackup (ou Cópias de Segurança) no cPanel. Escolha um com data anterior ao ficheiro mais antigo assinalado pelo Imunify Security.
- Se não houver nenhum anterior à infeção, ou se preferir que sejamos nós a fazê-lo, abra um pedido com o seu domínio, a data que quer restaurar e o relatório do Imunify Security (caminhos dos ficheiros, nomes das ameaças e datas, ou uma captura de ecrã).
- Restaurar não fecha a porta: mude as palavras-passe e atualize tudo logo a seguir, como descrito acima.

VEJA TAMBÉM

Ainda não tem a certeza de que foi invadido?
Como saber se o meu site está infectado por malware →

ALOJAMENTO WEB

Precisa de um alojamento que não lhe dê trabalho?

cPanel, certificado SSL grátis, cópias de segurança todas as madrugadas guardadas durante um ano, e suporte que responde na sua língua.

Ver planos de alojamento →

Migração do site actual sem custo · sem fidelidade

Mozout

MozOut Portugal

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-PT-KB-236 · v2026.10.18 · Gerado a 15/11/2026 01:41