Gerado a 21/10/2026 17:42

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

# Proteger a entrada do WordPress: três passos por ordem de efeito

WordPress e CMS

| CÓDIGO | VERSÃO | PAÍS · IDIOMA |
| --- | --- | --- |
| RLX-PT-KB-1084 | v2026.09.27 | 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/1084

# Proteger a entrada do WordPress: três passos por ordem de efeito

WordPress e CMS · Criado em **11 de setembro de 2026** · Atualizado em **27 de setembro de 2026** · 7 min de leitura



O endereço de entrada do WordPress é o mesmo em todos os sites do mundo: `/wp-admin` e `/wp-login.php`. Isso quer dizer que qualquer varredor automático sabe onde bater sem ter de procurar, e bate, de dia e de noite, em todos os sites que encontra.

Na maior parte das vezes não passa disso. Mas basta uma senha fraca para deixar de ser ruído e passar a problema. Há três coisas a fazer na entrada, por ordem de efeito, e depois há o resto do site, que é por onde eles entram de verdade.

## Antes dos três passos: o que já está ligado do nosso lado

Vale a pena saber o que já tem, para não instalar três *plugins* a fazer o que o servidor já faz:

| O que está ligado | O que faz por si |
|---|---|
| **Imunify360** | Está no cPanel, na secção **Segurança**. Inspecciona os pedidos que chegam ao site com um conjunto de regras mantido, inclui um firewall específico para WordPress **activo por omissão**, e analisa os ficheiros da conta em tempo real, à medida que são escritos. |
| **Certificado automático** | O certificado dos domínios da conta é emitido e renovado sozinho. Não precisa de pedir, nem de plugin: **o que é um certificado SSL**. |
| **Cópias diárias** | Se algo correr mal, há caminho de volta sem depender de um *plugin* de cópias: **quanto tempo guardamos as cópias**. |
| **Contas isoladas** | Um vizinho comprometido não chega aos seus ficheiros. A lista completa do que corre e do que não prometemos está em **o que fazemos pela segurança**. |

## 1. Antes de tudo: a senha e o segundo passo

Nenhum dos truques abaixo substitui isto. Se a senha de administrador for adivinhável, esconder a porta apenas atrasa quem está a tentar.

1. Apague o utilizador **admin**, se ainda existir. Metade das tentativas que um site recebe usam exactamente esse nome. Crie um administrador novo com outro nome e remova o antigo, reatribuindo o conteúdo dele.

2. Uma senha longa, usada só neste site. Uma frase de cinco palavras vale mais do que oito caracteres com símbolos, e não se repete no e-mail nem em mais lado nenhum. Se quiser uma feita ao acaso: **gerador de senhas**.

3. Ligue a autenticação em dois passos no WordPress, com um *plugin* de autenticação. A do My MozOut liga-se à parte: **como ligar a autenticação em dois passos**.

4. Uma conta por pessoa, com o papel certo. Quem só escreve artigos não precisa de ser administrador. E quando alguém sai, a conta sai.

## 2. Mudar o endereço de entrada

Isto não é segurança a sério: é arrumação. Mudar o `/wp-login.php` para um endereço que só você conhece faz com que os varredores automáticos deixem de lhe bater, e o site deixa de gastar recursos a responder-lhes. Em sites com muito ruído chega a ver-se na velocidade.

Faz-se com um *plugin* feito para isso, e a mudança é imediata. O passo a passo, e o que parte, está em **mudar o endereço de entrada no painel**. Para as tentativas que passam pelo formulário, **pôr um captcha na entrada**.

> **!** **Escreva o endereço novo antes de gravar.**
> No momento em que grava, o antigo deixa de funcionar. Feche a janela sem o ter apontado e fica trancado fora do seu próprio site: o caminho de volta é desactivar o *plugin* pelo Gestor de Ficheiros, mudando o nome da pasta dele. Escreva o endereço novo antes de carregar em gravar.

## 3. Uma senha antes da senha

Este é o mais eficaz dos três, e pertence ao cPanel e não ao WordPress: proteger a pasta `wp-admin` com uma senha ao nível do servidor. Quem chega tem de passar uma caixa do navegador antes de o WordPress sequer arrancar, o que significa que as tentativas nunca chegam a consumir PHP.

1. No cPanel, abra **Privacidade de Directório** (Directory Privacy).

2. Navegue até à pasta `public_html/wp-admin` e escolha protegê-la.

3. Crie um utilizador e uma senha, diferentes dos do WordPress, e grave.

**Duas coisas partem com isto, e ambas têm solução.**
O ficheiro `admin-ajax.php` vive dentro do `wp-admin` e é usado por *plugins* no lado público do site: formulários, carrinhos, filtros. Protegido, isso deixa de funcionar. A cura é acrescentar uma excepção para esse ficheiro no `.htaccess` que o cPanel criou. A segunda é o `wp-cron.php`, que fica inacessível por fora. Se o site começar a dar erros estranhos a seguir a isto, **erros comuns do WordPress** ajuda a confirmar que foi isto.

## Restringir por endereço: só com IP fixo

Dá para permitir apenas alguns endereços e recusar todos os outros. É a protecção mais forte que existe, e a que mais gente tranca fora do próprio site, porque quase ninguém tem endereço fixo: as ligações de casa mudam, os dados móveis mudam sempre, e a partir daí nem você entra.

Só vale a pena se trabalha sempre do mesmo escritório, com endereço fixo contratado. Se se trancar fora, a regra tira-se pelo Gestor de Ficheiros, e para perceber o mecanismo veja **porque é que o seu IP é bloqueado**.

## Actualizações: a defesa que conta mais do que todas as outras

Vale a pena dizer sem rodeios: a esmagadora maioria dos sites invadidos que vemos não foi invadida pela porta da entrada. Foi por um *plugin* desactualizado. Uma falha publicada é explorada por varredores automáticos em poucos dias.

1. Ligue as actualizações automáticas do núcleo do WordPress. Para os *plugins*, ligue-as um a um, começando pelos que conhece.

2. **Apague o que não usa.** Um *plugin* desactivado não corre, mas continua a ser uma porta por remendar, e um ficheiro que continua lá. O mesmo para os temas: fique com o que usa e um de reserva.

3. Nunca instale temas ou *plugins* pagos obtidos de graça em sites não oficiais. Vêm com frequência com código acrescentado, e é exactamente esse o preço.

4. Veja a lista de instalações em **WordPress Management**, no cPanel, secção **Domínios**. Ela mostra numa página o que está desactualizado em todos os sites da conta, o que é muito mais rápido do que entrar em cada um.

**Actualize com caminho de volta.**
Antes de uma actualização grande, uma cópia. E, se o site é importante, ensaie primeiro num sítio à parte: **um site de ensaio antes de mexer no que está no ar**.

## Ficheiros e permissões

Esta parte quase nunca se vê e é das que mais fecha portas. Faz-se uma vez.

| O que fazer | Porquê |
|---|---|
| **Pastas a 755, ficheiros a 644** | É o que o WordPress precisa e nada mais. No Gestor de Ficheiros, seleccione a pasta e use **Permissões**, aplicando recursivamente a ficheiros e pastas em separado. |
| **Nunca 777** | Se alguém lhe disser para pôr uma pasta a 777 para «resolver», está a resolver o sintoma e a abrir a porta. Nunca é preciso. |
| **O `wp-config.php` a 600** | É o ficheiro com a senha da base de dados. Só a conta precisa de o ler. |
| **Desligar o editor de ficheiros** | Com `define( 'DISALLOW_FILE_EDIT', true );` no `wp-config.php`, quem entrar no painel deixa de poder editar o tema e os *plugins* a partir dali. É a primeira coisa que um invasor usa. |
| **Nada de PHP nos envios** | Um `.htaccess` dentro de `wp-content/uploads` que recuse ficheiros `.php` impede que uma imagem enviada por um formulário se transforme em código a correr. |
| **Limpe o que sobrou** | ZIP do site antigo, pastas `site-antigo`, `backup`, `teste`. Cada uma é uma instalação desactualizada a servir de porta, e ninguém as actualiza porque ninguém se lembra delas. |

## O `xmlrpc.php`, que ninguém usa e toda a gente tem

É uma porta antiga do WordPress, anterior à API actual, e é a preferida de quem tenta senhas em massa: permite experimentar muitas de uma só vez, num pedido, sem passar pelo formulário de entrada. Um captcha na entrada não lhe faz nada.

Se não usa a aplicação móvel do WordPress, nem Jetpack, nem publicação remota, pode fechá-la. Faz-se com um *plugin* de segurança, ou com uma regra no `.htaccess` da raiz do site. Se usa alguma dessas coisas, deixe-a aberta e limite as tentativas em vez de a fechar.

## E se já aconteceu

Não comece por apagar ficheiros. Comece por **perceber se o site foi mesmo comprometido** e siga depois para **como limpar um site comprometido**. E diga-nos: conseguimos ler o registo do servidor e dizer por onde entraram, o que evita que voltem pela mesma porta.

Se neste momento nem consegue entrar no painel, a causa costuma ser outra: **não consigo entrar no painel do WordPress**.

PRECISA DE AJUDA?

Quer que vejamos consigo as tentativas de entrada no seu site?

Falar connosco →

VEJA TAMBÉM

- Gerador de senhas →
- Política de Suporte →
- Hospedagem WordPress →

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<br>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<br>Sábado & Domingo - Fechado |

RLX-PT-KB-1084 · v2026.09.27 · Gerado a 21/10/2026 17:42

Versão online deste documento