interweb

Generated on 22/10/2026 05:11

KNOWLEDGE BASE · PUBLIC DOCUMENT

Protecting the WordPress login: three steps in order of effect

WordPress & CMS

CODE	VERSION	COUNTRY · LANGUAGE
RLX-MZ-KB-340	v2026.10.21	Mozambique · English

Interweb Mozambique
RLX Holdings, S.A. · Group RLX Holdings
Tax ID (NUIT) 401 191 607 · Legal entity no. (NUEL) 105 045 974 · Economic activity code (CAE) 62022

https://www.meu.interweb.co.mz/knowledgebase/340

Protecting the WordPress login: three steps in order of effect

WordPress & CMS Created on **September 11, 2026** Updated on **October 21, 2026** 7 min read



WordPress's login address is the same on every site in the world: `/wp-admin` and `/wp-login.php`. That means any automated scanner knows where to knock without having to look, and it knocks, day and night, on every site it finds.

Most of the time it goes no further than that. But one weak password is all it takes for it to stop being noise and become a problem. There are three things to do at the door, in order of effect, and then there is the rest of the site, which is where they really get in.

Before the three steps: what is already on, on our side

Worth knowing what you already have, so you do not install three *plugins* to do what the server is doing anyway:

What is running	What it does for you
Imunify360	It is in cPanel, under **Security**. It inspects the requests reaching the site with a maintained rule set, includes a WordPress-specific firewall that is **on by default**, and scans the account files in real time, as they are written.
Automatic certificate	The certificate for the account's domains is issued and renewed by itself. You do not need to ask, and you do not need a plugin: **what an SSL certificate is**.
Daily backups	If something goes wrong there is a way back that does not depend on a backup *plugin*: **how long we keep backups**.
Isolated accounts	A compromised neighbour cannot reach your files. The full list of what runs and what we do not claim is in **what we do about security**.

1. First of all: the password and the second step

None of the tricks below replaces this. If the administrator password is guessable, hiding the door only slows down whoever is trying.

1. Delete the **admin** user if it still exists. Half the attempts a site receives use exactly that name. Create a new administrator under another name, and remove the old one, reassigning its content.
2. A long password, used only on this site. A five-word phrase beats eight characters with symbols, and it is not repeated on the e-mail or anywhere else. If you want one made at random: **password generator**.
3. Turn on two-factor authentication in WordPress, with an authentication *plugin*. The one on My Interweb is switched on separately: **how to enable two-factor authentication**.
4. One account per person, with the right role. Someone who only writes articles does not need to be an administrator. And when someone leaves, the account goes.

2. Changing the login address

This is not real security: it is housekeeping. Moving `/wp-login.php` to an address only you know means automated scanners stop hitting it, and the site stops spending resources answering them. On noisy sites you can even see it in the speed.

It is done with a *plugin* built for it, and the change is immediate. The step by step, and what it breaks, is in **changing the WordPress login address**. For the attempts that do come through the form, **putting a captcha on the login**.

> **!** **Write the new address down before saving.**
> The moment you save, the old one stops working. Close the window without having noted the new one and you are locked out of your own site: the way back is deactivating the *plugin* through File Manager, by renaming its folder. Write the new address down before clicking save.

3. A password before the password

This is the most effective of the three, and it belongs to cPanel rather than WordPress: protecting the `wp-admin` folder with a server-level password. Anyone arriving has to pass a browser box before WordPress even starts, meaning the attempts never get to consume PHP at all.

1. In cPanel, open **Directory Privacy**.
2. Navigate to the `public_html/wp-admin` folder and choose to protect it.

3. Create a username and password, different from the WordPress ones, and save.

Two things break with this, and both have a fix.
The file `admin-ajax.php` lives inside `wp-admin` and is used by *plugins* on the public side of the site: forms, carts, filters. Protected, those stop working. The fix is to add an exception for that file in the `.htaccess` cPanel created. The second is `wp-cron.php`, which becomes unreachable from outside. If the site starts throwing odd errors after this, **common WordPress errors** helps confirm that this was it.

Restricting by address: only with a fixed IP

You can allow only a few addresses and refuse everyone else. It is the strongest protection there is, and the one that locks the most people out of their own site, because hardly anyone has a fixed address: home connections change, mobile data always changes, and from then on not even you get in.

It is only worth it if you always work from the same office on a contracted fixed address. If you do lock yourself out, the rule is removed through File Manager, and for how the mechanism works, see **why your IP gets blocked**.

Updates: the defence that counts more than all the others

Worth saying without hedging: the overwhelming majority of hacked sites we see were not broken into through the front door. They were broken into through an out-of-date *plugin*. A published hole is exploited by automated scanners within days.

1. Turn on automatic updates for the WordPress core. For *plugins*, turn them on one by one, starting with the ones you know.

2. **Delete what you do not use.** A deactivated *plugin* does not run, but it is still an unpatched door, and a file that is still there. Same for themes: keep the one you use and one spare.

3. Never install paid themes or *plugins* obtained free from unofficial sites. They frequently come with code added, and that is exactly the price.

4. Look at the installation list in **WordPress Management**, in cPanel, under **Domains**. It shows on one page what is out of date across every site on the account, which is far quicker than signing into each one.

Update with a way back.
Before a big update, take a backup. And if the site matters, rehearse somewhere else first: **a test site before touching what is live**.

Files and permissions

This part is almost never seen and it closes more doors than most. You do it once.

What to do	Why
Folders 755, files 644	It is what WordPress needs and nothing more. In File Manager, select the folder and use **Permissions**, applying recursively to files and folders separately.
Never 777	If somebody tells you to set a folder to 777 to «fix» something, they are fixing the symptom and opening the door. It is never necessary.
`wp-config.php` at 600	It is the file holding the database password. Only the account needs to read it.
Switch off the file editor	With `define( 'DISALLOW_FILE_EDIT', true );` in `wp-config.php`, anyone who gets into the dashboard can no longer edit the theme and the *plugins* from there. It is the first thing an intruder reaches for.
No PHP in uploads	An `.htaccess` inside `wp-content/uploads` refusing `.php` files stops an image sent through a form from turning into running code.
Clear out the leftovers	The ZIP of the old site, folders called `old-site`, `backup`, `test`. Each one is an out-of-date installation serving as a door, and nobody updates them because nobody remembers they exist.

`xmlrpc.php`, which nobody uses and everybody has

It is an old WordPress door, older than the current API, and it is the favourite of anyone trying passwords in bulk: it lets them try many at once, in a single request, without going near the login form. A captcha on the login does nothing to it.

If you do not use the WordPress mobile app, or Jetpack, or remote publishing, you can close it. It is done with a security *plugin*, or with a rule in the `.htaccess` at the site root. If you do use one of those, leave it open and limit the attempts instead of closing it.

And if it has already happened

Do not start by deleting files. Start with **finding out whether the site really was compromised** and then move on to **how to clean up a compromised site**. And tell us: we can read the server log and say how they got in, which stops it happening again through the same door.

If right now you cannot even reach the dashboard, the cause is usually something else: **cannot get into the WordPress dashboard**.

NEED A HAND?

Want us to look at the login attempts on your site with you?

Talk to us →

SEE ALSO

- **Password generator**
- **Support Policy**
- **WordPress hosting**

interweb

Interweb Mozambique

RLX Holdings, S.A. · Group RLX Holdings

TAX ID (NUIT)	401 191 607
LEGAL ENTITY NO. (NUEL)	105 045 974
ECONOMIC ACTIVITY CODE (CAE)	62022
REGISTERED OFFICE	Bairro 7 de Setembro Vilankulo 1304 · CEP 0411-02, Inhambane, Mozambique
CONTACT	info@interweb.co.mz · +258 84 635 1111 · +258 86 635 1111 · www.interweb.co.mz
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

Online version of this document

RLX-MZ-KB-340 · v2026.10.21 · Generated on 22/10/2026 05:11