interweb

Generated on 21/10/2026 17:25

KNOWLEDGE BASE · PUBLIC DOCUMENT

After a hack, which backup do you restore? Choosing a clean copy

Security

CODE	VERSION	COUNTRY · LANGUAGE
RLX-MZ-KB-1502	v2026.10.10	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/1502

After a hack, which backup do you restore? Choosing a clean copy

Security Created on **October 10, 2026** 3 min read



The short answer: restore the **last copy from before the infection**, not the most recent one. If you restore yesterday's copy and the site had been infected for a week, you bring the whole attack back. So the first job is to find out **when** it started, and only then pick the day.

1. Find out when it started

Look for the first sign, not the most visible one. These help to date it:

Where to look	What to look for
Files in File Manager	Files with a recent modification date that you did not change, especially in folders that rarely change (`wp-includes` , `wp-admin` , the site root).
Site users	A WordPress administrator you did not create, and the date it was registered.
"Imunify Security" in cPanel	The list of what was detected or quarantined, with dates. See **how to tell if your site has been compromised**.
Access logs	The first odd requests (for example to a file that should not exist) give you the time the door was used.
What visitors saw	When the first customer complained about the red warning or the redirect.

2. Choose and try the copy

1. **Open JetBackup in cPanel** and look at the dates available. Interweb takes one backup a day, before dawn, and keeps the last 30 days; you restore them from your own panel. The step by step is in **how long we keep backups, and how to restore one**.

2 **Pick a date with some margin before the first sign**, not the one right next to it. If in doubt, go further back: a lost day of work can be redone, a re-infection costs more.

3 **Use "Download" instead of "Restore"** on the candidates. You can open them and look for the infection before anything goes onto the site. If you have a test site, restore there first: see **a test site before touching what is live**.

4 **Restore only what you need.** Usually the site files and the database, from the same date, so they match. Restoring the files from one day and the database from another invites errors.

5 **Before it goes live, close the door:** change every password (cPanel, FTP, site administrator, database), update WordPress, themes and plugins, and delete the ones you do not use. Without this, the infection returns through the same entrance. The full list is in **how to clean up a compromised site**.

Restoring replaces, and there is no undo.
Before you restore, download the current state (infected as it is) to somewhere safe: you may need it to work out how they got in, or to recover a post or an order made after the date you chose.

And if there is no clean copy?

If the infection is older than every copy kept, or the attack was only found after the window had passed, every copy is infected. The way out then is to clean by hand (files and database) or to rebuild the site on a fresh install and bring across only the content. Our automatic backup is a safety net, not your backup: see **making and keeping your own backup**.

Write down the day and time the site was restored and what changed. If the warning comes back, that note tells you straight away whether it is the same infection or a new one.

NEED A HAND?

Not sure which date to choose? Give us the domain and the first sign you saw, and we will help you read the logs.

Open a support ticket →

SEE ALSO

How long we keep backups, and how to restore one →

- **How to clean up a compromised site**
- **A test site before touching what is live**
- **Restoring a backup yourself, without opening a ticket**

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-1502 · v2026.10.10 · Generated on 21/10/2026 17:25