interweb

Generated on 21/10/2026 17:25

KNOWLEDGE BASE · PUBLIC DOCUMENT

Ransomware explained: how it reaches a website or a computer and how to be ready

Security

CODE	VERSION	COUNTRY · LANGUAGE
RLX-MZ-KB-1500	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/1500

Ransomware explained: how it reaches a website or a computer and how to be ready

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



The short answer: *ransomware* is malicious software that **encrypts your files** and demands a ransom to give them back. You cannot avoid it entirely, but you can prepare: **keep everything updated**, be careful with attachments and passwords, and above all keep **a backup the program cannot reach**. With that backup, a ransom demand turns from a disaster into an inconvenience.

How it arrives

Way in	How to close it
An attachment or link in an e-mail	Be suspicious, and do not open what you were not expecting. See **how to recognise phishing**.
A stolen or weak password	Long, unique passwords, and two-step verification. An FTP or SSH login with a reused password is an open door.
Out-of-date software	Update the system, the browser, WordPress, themes and plugins. See **abandoned plugins and old PHP**.
Pirated software	Do not install “cracked” programs, nor paid themes and plugins taken free from unofficial sites.

Can a hosted website be encrypted too?

The textbook case of ransomware is a person’s computer. On a shared hosting account, what can happen is a simpler version: someone gets in through a password or a vulnerable plugin, deletes or alters files and leaves a note asking for money. Accounts at Interweb run isolated from each other, which stops a compromised neighbour reaching your files, but does not stop **your** account being used if the password is stolen: see **what we do and what stays yours**.

What to do to be ready

1. **Keep a copy out of reach.** An external drive that stays plugged into the computer is encrypted along with everything else. After copying, unplug it, or keep the copy somewhere your everyday computer has no write access to.

2. **Back up the site, and test the backup.** The automatic daily server backup helps, but it only keeps the last 30 days and is no substitute for a copy of your own: see **making and keeping your own backup, and testing it**.

3. **Know how to restore before you need to.** Try a restore on a quiet day, following **how to restore your data with JetBackup**.

4. **Limit who can change what.** Everyone gets their own login, with only the permissions they need.

Keep a one-page plan on paper too: who warns whom, where the backup is, how to reach support. Ransomware preys on people who panic, and a simple list prevents hasty decisions, such as paying or deleting everything.

If you are hit, take the device off the network and Wi-Fi at once

, so the program does not spread to other computers and shared drives. Do not pay in a hurry: authorities and security specialists advise against it, because paying does not guarantee the files come back and marks you as someone who pays. First see what you have in backup.

If your site was altered and no longer opens, delete nothing. First work out the most recent clean copy in **after a hack, which backup to restore**, and only then follow **cleaning up a compromised site**.

NEED A HAND?

Did your site change, or stop opening, all of a sudden? Tell us what you saw and at what time.

Open a support ticket →

SEE ALSO

- How to recognise phishing →
- Making and keeping your own backup, and testing it →

After a hack, which backup to restore →

How to clean up a compromised site →

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-1500 · v2026.10.10 · Generated on 21/10/2026 17:25