interweb

Generated on 15/11/2026 00:10

KNOWLEDGE BASE · PUBLIC DOCUMENT

Removing the red Google warning from your site

Hacked Sites & Malware

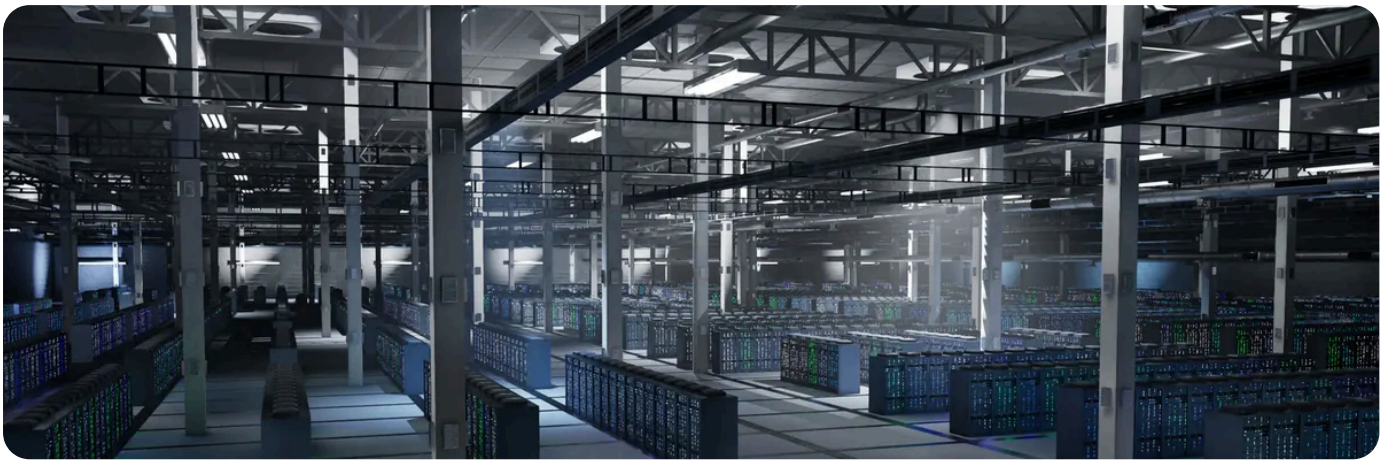
CODE	VERSION	COUNTRY · LANGUAGE
RLX-AO-KB-666	v2026.09.27	Angola · English

Interweb Angola
RLX Angola, Lda. · Group RLX Holdings
Tax ID (NIF) 500 260 5724 · Commercial registration no. 26464-25/250724

https://www.meu.interweb.ao/knowledgebase/666

Removing the red Google warning from your site

Hacked Sites & Malware Created on **September 27, 2026** 4 min read



It is the red screen covering the whole site, with a line like «the site ahead contains malware» or «deceptive site ahead». It is not the browser being dramatic: it is a public signal that something was found on your site. While it is there, practically nobody gets in.

> **The warning is the symptom, not the illness.**
> Clean first, request the review afterwards. Requesting a review while the site is still infected makes Google confirm the problem, and the second flag is harder to remove than the first.

First: see what Google found

1. Open **Search Console** and go to **Security and Manual Actions**, then **Security issues**.
2. Read the **type** of problem and the **list of example addresses**. That list is a map of what it saw, and it saves you hours of guessing.
3. **If the site is not in Search Console yet, add it now.** Without it you cannot see what was found and you have no way to request the review.

Type of warning	What is usually behind it
Malware	Files injected into the site, almost always through an out-of-date plugin or theme
Unwanted software	Aggressive advertising, redirects, or a third-party script that has been compromised
Social engineering	Phishing pages dropped into a folder of your site, imitating a bank or a well-known service
Harmful downloads	Downloadable files that Google considers dangerous

Cleaning the site

We run **Imunify360** on the server, and your cPanel has its icon in the **Security** section (depending on the version it appears as **Imunify360** or **Imunify Security**). That is where you start.

1. **Open Imunify in cPanel and run a scan.** It lists the flagged files and lets you clean them or move them to quarantine.
2. **Change every password**: cPanel, FTP, database, WordPress administrators and mailboxes. If you do not, whoever got in walks back in: **changing your cPanel password**.
3. **Update core, themes and plugins**, and delete the ones you do not use. A deactivated theme is still code on the server.
4. **Review the WordPress administrator accounts.** An administrator you did not create is the signature of whoever got in.
5. **Look for what was left behind**: odd lines in .htaccess, code at the start or end of PHP files, and scheduled tasks you do not recognise.
6. **If it will not come clean, restore a backup from before the infection** and update everything again before putting it back online: **restoring a backup yourself**.

The full procedure, in detail, is in **how to clean up a compromised site**. To confirm there really is an infection before touching anything, see **how to tell if your site has been compromised**.

> **!** **Restoring a backup without closing the hole is reinfecting.**
> The backup puts the files back as they were, including the out-of-date plugin they came in through. Update and change the passwords before opening to the public again.

Requesting the review from Google

1. **Confirm, address by address**, that the examples it listed are clean. Open them yourself.
2. In Search Console, under **Security issues**, click **Request a review**.
3. **Write down what you did.** Which files were infected, how they were cleaned, which passwords you changed and what you updated. A concrete account reads very differently from «it is fixed now».

4. **Wait, and do not repeat the request.** Insisting does not speed it up and can delay it. While you wait, leave the site alone.

We promise no timescale, for a simple reason: Google decides, and it publishes none that we could guarantee. Once it lifts the warning, the screen disappears by itself in every browser.

And if it is not an infection?

Cause	How to confirm it
Third-party advertising	A compromised ad network puts bad content on a clean page. Switch the adverts off and request the review
An external script	Old counters, chats and widgets load code from sites that have changed hands. Remove whatever you do not use
A forgotten subdomain	An old installation on a subdomain drags the main domain down with it. Look at everything on the plan
A form asking for passwords	A page of yours asking for another service's login details can read as phishing, even with no bad intent

Do not confuse it with the certificate warning.
The «your connection is not private» screen is a different thing and is fixed differently: **no padlock on your site: the causes, in order**.

Keeping it from coming back

1. **Updating is the main defence.** Nearly every break-in we see arrives through an out-of-date plugin or theme.
2. **Lock the WordPress login**: **three steps in order of effect**.
3. **Keep your own tested backups**, as well as ours: **making and testing your own backup**.
4. **Delete what you do not use.** Old installations in subfolders are the most used door of all.

NEED A HAND?

Site flagged and you cannot clean it on your own?

Open a support ticket →

SEE ALSO

- How to clean up a compromised site →
- How to tell if your site has been compromised →
- Being found on Google: Business Profile, Search Console and the basics →
- What we do about security, DDoS included, and what stays yours →
- Getting your site indexed in Google Search Console, step by step →

interweb

Interweb Angola

RLX Angola, Lda. · Group RLX Holdings

TAX ID (NIF)	500 260 5724
COMMERCIAL REGISTRATION NO.	26464-25/250724
REGISTERED OFFICE	Rua Direita do Patriota, Bairro Dangereux Belas, Luanda, Angola
CONTACT	info@interweb.ao · +244 942 011 191 · www.interweb.ao
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

Online version of this document

RLX-AO-KB-666 · v2026.09.27 · Generated on 15/11/2026 00:10