

KNOWLEDGE BASE · PUBLIC DOCUMENT

A red warning from Google (Deceptive site ahead): what it means and how to ask for a review

Security

CODE

RLX-AO-KB-1994

VERSION

v2026.10.15

COUNTRY · LANGUAGE

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/1994>



The short answer: if someone opening your site sees a red browser page saying **“Deceptive site ahead”** or **“The site ahead contains malware”**, Google has flagged it as dangerous. Almost always it is because the site **was hacked** and someone put a fake page or malicious code on it. The warning only goes after you **clean the site and ask for a review**.

What the site needs

What	What to do
“Deceptive site”	A page imitates another (a bank, an e-mail login) to steal data. It is usually hidden in a folder on your site.
“Malware”	The site tries to install or download something harmful to its visitors.
“Dangerous site”	A more general warning. See the reason in Google’s tool.
Where to see the reason	In Search Console, under “Security issues”, if the site is registered: Search Console .
How long it lasts	Until Google reviews the site once clean. Asking before cleaning only delays it.

Getting started

1

Do not delete everything blindly. First see what is there: Search Console shows sample addresses.

2

Scan the site: [Malware scan in cPanel](#) and, if the warning persists, **[where an infection hides](#)**.

3

Restore a clean copy if you have one: **[After a hack, which backup to restore](#)**.

4

Change all passwords (cPanel, FTP, database, WordPress) and update whatever is out of date: **[Protecting the WordPress login](#)**.

5

Only once clean, ask for the review in Search Console, explaining what you did. The answer may take a while; the warning disappears when Google confirms.

If you ask for the review without cleaning, the request is refused and the wait gets longer. If the fake page comes back, the attacker's way in was not closed (a password, an old plugin): cleaning without closing the door does not solve it. **[Files that must never be public](#)**.

If you received a fake message and clicked: **[How to recognise a fake message](#)**. To stay protected afterwards: **[Ransomware](#)**.

Does your site have the red warning and you want help cleaning it? Open a ticket with the address, right away.

[Open a support ticket](#)

SEE ALSO

[Getting your site indexed in Google Search Console, step by step](#)

[Scanning your site for malware in cPanel: what Imunify finds and what to do with the result](#)

[The scan says clean but the site still redirects: where an infection hides](#)

[After a hack, which backup do you restore? Choosing a clean copy](#)

[How to recognise a phishing e-mail or message, and what to do if you clicked](#)



Online version of this document

Interweb is a leading internet services company, with a mission to help businesses to be born and prosper through technology.

2020

FOUNDED

37,000+

CLIENTS

130+

SIGN-UPS A DAY

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