

KNOWLEDGE BASE · PUBLIC DOCUMENT

Phishing pages found on your site or server: remove them, find the way in and avoid a block

Security

CODE

RLX-MZ-KB-2262

VERSION

v2026.10.21

COUNTRY · LANGUAGE

Mozambique · English

Interweb Mozambique

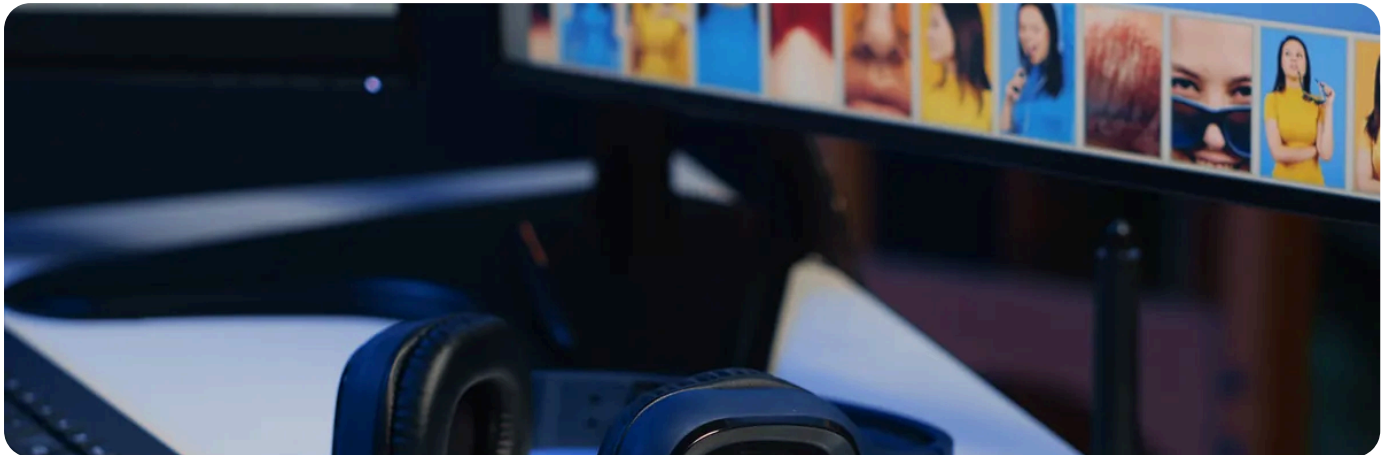
RLX Holdings, S.A. · Group RLX Holdings

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/2262>

Phishing pages found on your site or server: remove them, find the way in and avoid a block

📁 Security 📅 Created on **October 21, 2026** ⌚ 5 min read



The short answer: a phishing page pretends to be a bank, a delivery company or a well-known service to steal passwords and card details. When one turns up on your site, the owner almost never put it there: someone got in through an outdated plugin, a stolen password or a file upload form, and left a folder behind. The notice reaches us from our network provider, from a national incident response team (CERT) or from the company being imitated, with a **short deadline, often a single day**, and we forward it to you as a support ticket in My Interweb. The job has three parts: **take the page down, find the way in** and close it, and send us a **short report**. The whole process is in **an abuse notice about your server**.

🔍 What to look for, and where it usually is

What to look for	Where it usually is
The page in the notice	The address (URL) in the notice tells you the folder. An address ending in <code>/wp-content/uploads/xyz/login.php</code> lives in <code>public_html/wp-content/uploads/xyz/</code> .
The zip kit	.zip files named after banks or couriers, left next to the page. It is the package the attacker unpacked.
Hidden folders	Folders starting with a dot, or inside <code>.well-known</code> , where nobody usually looks.
Sending and collecting scripts	Small PHP files that send e-mail or store what victims type, sometimes into a .txt file alongside.
Back doors (web shells)	PHP files with random names in image or cache folders, often using <code>eval</code> or <code>base64_decode</code> .
Access you did not create	New WordPress administrators, FTP accounts, users or SSH keys on a VPS.

➔ Fixing it, in order

1 Take the page down without destroying the evidence. In cPanel's File Manager, compress the folder into a zip **outside** `public_html` (or download it), and only then delete the folder. On a VPS, with your site's real path: `mkdir -p /root/analysis`
`tar czf /root/analysis/phishing.tar.gz /var/www/PATH/TO/FOLDER`
`rm -rf /var/www/PATH/TO/FOLDER` Check the path twice before `rm -rf`: it deletes without asking.

2 Look for the other copies. Whoever gets in nearly always leaves more than one. On a hosting plan, run the Imunify scan: **scanning your site for malware in cPanel**. On a VPS, list the PHP files changed in the last few days and the ones using functions typical of hidden code: `find /var/www -type f -name "*.php" -mtime -14 -ls`
`grep -rLE "eval\(|base64_decode\(" /var/www --include=*.php` Go through the list one by one: some legitimate plugins use these functions too.

3 Find the way in. In the access log, look for the first request to the page's folder, then for what the same IP did before that. In cPanel the log is under **Metrics > Raw Access**. On a VPS: `grep "FOLDER_NAME" /var/log/nginx/access.log /var/log/apache2/access.log`
`grep "ATTACKER_IP" /var/log/nginx/access.log | head -50` An upload (POST) to a plugin or to `wp-login.php` shortly before the folder appeared is usually the door.

4 Close the door. Update the CMS, themes and plugins, remove the abandoned ones (**an abandoned plugin or an old PHP version**), change every password (cPanel, FTP, database, site administrators) and delete any access you do not recognise. On a VPS, also run the checks in **is my VPS compromised?**.

5 Check whether phishing e-mail went out from the server. On a hosting plan, use **Track Delivery**. On a VPS, look at the mail queue with `mailq`. If it did, the IP may end up on a blacklist: **your server IP is on a spam blacklist**.

6 Reply in the support ticket with the report: the cause and how they got in, what you found and removed, and what you did so it does not happen again. There is a template in **writing the reply to an abuse notice**.

7 If browsers or Google flag the site as "deceptive", once it is clean, request a review in Google Search Console, in the security issues report.

**Deleting the folder and replying “removed” is not enough.**

If the door they used is still open, the page comes back, and so does a new notice. If the deadline passes without a fix, the hosting service may be suspended (**a service suspended for another reason**) or the server switched off, and our network provider may block the IP: **why the server was switched off or locked**. On a heavily tampered server, the safest path is to reinstall and restore a clean copy: **which backup to restore after a hack**.

**Keep the folder’s zip until the case is closed,**

outside the public folder. It shows what was there and the file dates, and it helps you write the report. Do not open the fake page in a browser where you are logged in to anything.

 NEED A HAND?

Got a phishing notice and need help reading it? Reply in the same support ticket with what you have found so far.

[📄 Open a support ticket →](#) **SEE ALSO**[An abuse notice about your server: what it means, the deadline and what we need from you](#)[Writing the reply to an abuse notice: cause, what you removed and how it will not happen again](#)[Scanning your site for malware in cPanel: what Imunify finds and what to do with the result](#)[How to clean up a compromised site](#)[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](#)



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-2262 · v2026.10.21 · Generated on 21/10/2026 20:41