interweb

Generated on 21/10/2026 17:21

KNOWLEDGE BASE · PUBLIC DOCUMENT

Locked out: password, two-step authentication and the recovery e-mail

Security

CODE	VERSION	COUNTRY · LANGUAGE
RLX-MZ-KB-470	v2026.10.18	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/470

Locked out: password, two-step authentication and the recovery e-mail

Security Created on **September 26, 2026** Updated on **October 18, 2026** 5 min read



«I lost my password» is really three different questions, and the first thing to do is work out which one is yours. Mixing them up is why people spend a morning trying to reset the wrong password.

Three logins that get confused

Login	Opens	How it is reset
The client area	Invoices, your services, your domains, support tickets and your contact details.	From its own login page, via the forgotten password option. A reset link arrives by e-mail.
cPanel	Site files, databases, e-mail accounts, backups, DNS.	From the client area, by setting a new one. You do not need to know the old one.
Each e-mail account	Reading and sending mail in that mailbox, on the phone, in the mail program and in webmail.	In cPanel, by whoever manages the hosting. Each mailbox has its own, independent of the rest.

They are **independent**. Changing one does not touch the others, and using the same password for all three is the mistake that turns one problem into three. The steps for each are in «How to recover access to your account», «How to recover your cPanel password» and «How to recover an e-mail account password». If you need a new one that is not one of your usual ones, use the **password generator**.

There is a hierarchy here, and it is worth understanding.
Whoever holds the client area resets cPanel; whoever holds cPanel resets the mailboxes. The client area is the master key to everything you have with us. Which is why it deserves the strongest password, and why it deserves a second factor.

When two-step authentication is on a phone you no longer have

This is the case that cannot be solved by yourself, and it cannot be solved *by design*. The code is generated inside the phone and never leaves it. If there were an easy way around the second factor it would protect nothing, and whoever guessed your password would use that exact same way.

1. **Look for the recovery codes** you saved when you switched the second factor on. If you saved them, this is the two-minute route: one of them works instead of the code from the phone.

2. **If you only changed phones**, check whether your authenticator app keeps a copy in the cloud. Several do. Install it on the new device, sign into the same app account, and the keys come back.

3. **If the phone is genuinely gone**, it becomes a manual check on our side. Since you cannot get in to open a ticket, use one of the direct channels on **contact**.

4. **We will confirm you are the account holder** against the details the account already has, before switching the second factor off. Once you are back in, turn it on again, and this time keep the codes.

We do not switch the second factor off on an e-mailed request.
Not for someone who knows the company name, not for someone who knows the domain. If that were enough, the second factor would be worth nothing, and turning it on would have made the account weaker rather than stronger. The check takes time, and it is meant to.

Today, while you still have access:
Keep the recovery codes somewhere other than the phone (printed, in a drawer, is perfectly good) and set the authenticator app up on two devices if you have two. Five minutes now is the difference between two minutes and two days later.

The recovery e-mail is the piece nobody checks

Almost every automatic recovery goes through an e-mail. If that e-mail arrives nowhere, none of this works, and you only find out on the day you need it. There are two addresses, in two different places, and they are not the same one:

1. **The e-mail on your client account.** That is where the reset link goes, along with invoices and renewal notices. Check it in your profile details, and update it whenever you change address or somebody leaves the company.

2. **The contact e-mail stored inside cPanel.** It is a different one, and it is where cPanel sends the code when a reset is requested there. Plenty of people never filled it in, which is why that route fails at the first step.

3. **Neither of the two should be an address on your own domain.** This is the rule most often ignored and the one that costs the most.

The reason for that last one is easy to grasp and easy to forget: if the hosting has been suspended, if the domain expired, or if mail itself is what stopped working, the mailbox on that domain is **exactly the one that stops receiving**. You end up locked out with the key on the inside. Use an address on another domain, ideally a personal one that does not depend on us.

And if the e-mail is gone too?

Then the automatic reset has no way of reaching you and it becomes a manual check. Contact us through a direct channel, give us the domain or service in question and a new address we can reply to. We always confirm ownership against the details already on the account before handing access over. We never hand over an account just because somebody knows the domain name: that information is public.

We will never tell you an old password

, for any of the three. None of them is stored in readable form, not even for us. What we do is set a new one after confirming the account is yours. If anybody tells you they can «look up» your password, be suspicious from that moment on.

Five minutes that prevent the worst

1. Check the client area e-mail today, and check it is not an address on your own domain.
2. Fill in the contact e-mail inside cPanel, if you never did.
3. Keep the second factor recovery codes somewhere other than the phone.
4. Use different passwords for the three logins, in a password manager or, at the very least, written somewhere that is not the computer screen.
5. If other people work on the site, give them their own access instead of sharing yours. When they leave you revoke one login instead of changing three passwords.

RECOMMENDED

Locked out and unable to open a ticket? Reach us through one of the direct channels.

See how to contact us →

SEE ALSO

- **Direct contact channels** →
- **Password generator** →
- **Support Policy** →

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-470 · v2026.10.18 · Generated on 21/10/2026 17:21