interweb

Generated on 22/10/2026 05:12

KNOWLEDGE BASE · PUBLIC DOCUMENT

Authenticator app, SMS or security key: which two-step verification to use

Security

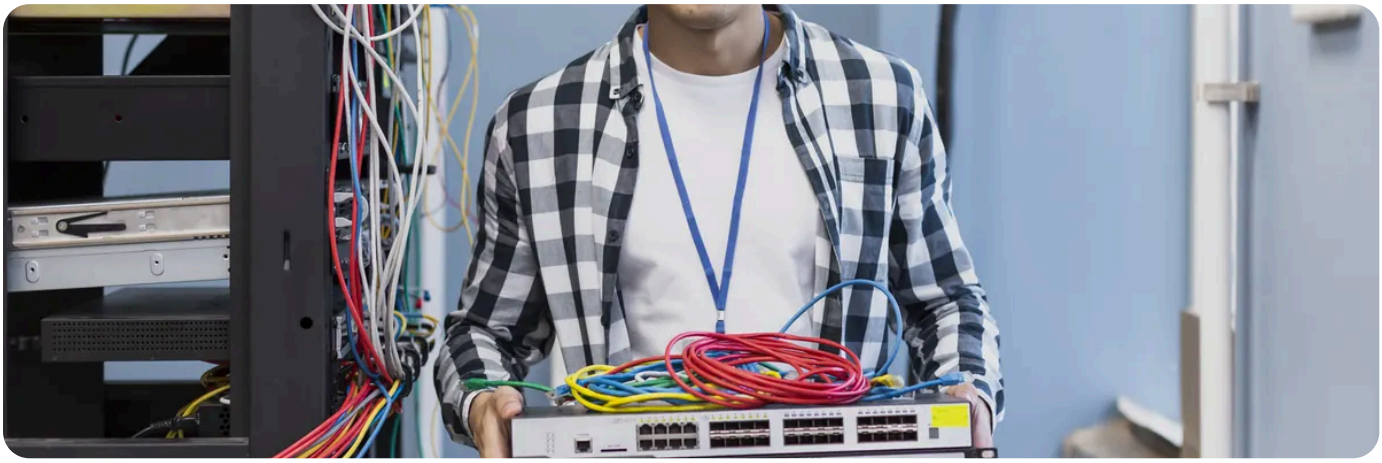
CODE	VERSION	COUNTRY · LANGUAGE
RLX-MZ-KB-1494	v2026.10.21	Mozambique · English

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/1494

Authenticator app, SMS or security key: which two-step verification to use

Security Created on **October 10, 2026** Updated on **October 21, 2026** 3 min read



The short answer: make an **authenticator app** on your phone your default. It is far safer than SMS, does not depend on the mobile network, and works with almost every service. For anything you cannot afford to lose (your main e-mail, your hosting account, your domain), a **physical security key** is better still. SMS is only better than nothing.

Two-step verification (2FA) adds a second proof after the password. Whoever learns your password, through your own slip or a data leak, is still stuck at the door. But “two steps” does not mean “equally safe”: the second step comes in three very different kinds.

The three kinds, side by side

Kind	How it works	Weak point
Authenticator app	The app on your phone generates a new code every few seconds. You type it after your password.	If you lose the phone without having saved the recovery codes, you are stuck.
SMS	You receive the code as a text message on your registered number.	It can be diverted: someone who talks the operator into moving your number to another SIM card receives your codes. It also needs signal.
Security key	A physical device (USB or NFC), or the passkey stored on your phone, proves it is really you, and only on the genuine address.	Not every service supports it. You should keep a second key as a spare.

How to choose, step by step

1. **Start with the accounts that open the others.** The e-mail you use to recover passwords, My Interweb, your password manager. Whoever gets into your e-mail can reset almost everything else.

2 **Pick the authenticator app** wherever the service offers one. In My Interweb, two-step verification works with an app of this kind: the path is in **how to enable or disable two-step verification**.

3 **Use the security key** on the accounts your business depends on, if the service accepts one and you are willing to keep a spare.

4 **Settle for SMS** only when it is the sole option. It is still much better than relying on the password alone.

5 **Save the recovery codes** somewhere other than your phone, printed or in a safe place. It is the difference between two minutes and two days when the phone goes missing.

! **Never read a code out to anyone**

, not even to someone claiming to be Interweb, your bank or WhatsApp. The code is for you. Anyone asking for it on the phone or in a message is trying to get into your account at that very moment. The same goes for codes that arrive when you did not ask for them: someone has just typed in your password.

What about WordPress and the site e-mail?

The My Interweb verification protects My Interweb only. The WordPress dashboard has its own entrance, which you protect with an authentication plugin, as **protecting the WordPress login** explains. Mailboxes created in cPanel have a password but no two-step verification, so those passwords need to be long and unique, as in **a strong password and a password manager**.

Set the authenticator app up on **two devices**, if you have two, at the moment you switch the service on. Some apps keep an encrypted copy in the cloud: check whether yours does before you change phone. If you still lose access, read **what to do when you are locked out**.

NEED A HAND?

Locked out of your two-step verification, or unsure what to switch on? Talk to us.

Open a support ticket →

SEE ALSO

Switching two-step verification on or off →

- **Locked out: password, two-step authentication and the recovery e-mail**
- **A strong password and a password manager**
- **Password generator**

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-1494 · v2026.10.21 · Generated on 22/10/2026 05:12