Mozout

Generated on 14/11/2026 03:12

KNOWLEDGE BASE · PUBLIC DOCUMENT

Two-step login with an SMS code on your own site or app

Security

CODE	VERSION	COUNTRY · LANGUAGE
RLX-INT-KB-7980	v2026.11.13	International · English

MozOut International
RLX Holdings (Pty) Ltd. · Group RLX Holdings
Tax no. (SARS) 943 907 6234 · Registration no. (CIPC) 2025/667953/07

https://www.my.mozout.com/knowledgebase/7980

Two-step login with an SMS code on your own site or app

Security Created on **November 13, 2026** 3 min read



The short answer: once the password is right, your site sends a code to the customer's already confirmed phone and only opens the session when the code matches. Anyone who stole or guessed the password is stuck at the door, because they do not have the phone. With our verification API it takes two requests, and the customer does not need to install any app.

How it fits into your login

1. **Check the password as usual.** If it is wrong, stop there and send no SMS: every code uses credits, and a code sent to someone who got the password wrong invites abuse.

2. **Right password: do not open the session yet.** Create an in-between state, “second step pending”, tied to that user.

3. **Send the code** with `POST /v1/sms/otp` to the number the customer confirmed at sign-up, never to a number that arrives with the login form.

4. **Keep the `id` in that in-between state** and show the code screen with the masked number.

5. **Check it with `/verify`.** With `valid: true`, open the session; with `valid: false`, show the attempts left.

Rules that work well for logins

Choice	Why
5 minutes validity (the default)	The customer has the phone in hand; a code for now is no use tomorrow.

Choice	Why
3 to 5 attempts	Enough for typos; too few for guessing.
A wait between resends	Set it in your account rules. Without it there is no limit on resends (see **limits against abuse**).
Text with your service name and "Do not share it"	For example: `Your login code is {code}. Valid for {minutes} min.`

What your system decides

The API checks the code; the rules of your login are yours. Decide whether to ask for a code at every login or only on a new device, how long a device stays remembered, and what happens when the customer has lost the phone. That last case needs an answer before you switch the second step on: a recovery path that is not weaker than the code itself, such as contact with your team with an identity check.

SMS is a good second step, not the only one.
It can be read on a locked screen and, in an extreme case, diverted with a SIM swap. For high-value accounts, offer an authenticator app too. The differences are explained in **sending one-time codes safely**.

Tell the customer about each new login.
A normal SMS saying "You just signed in to your account" lets them react if it was not them. Ideas for notices are in **transactional SMS**.

RECOMMENDED

Want to protect your site login with a second step by SMS? See Verification SMS.

See Verification SMS →

SEE ALSO

- **SMS verification API: we generate, send and check the code, and your system keeps only the id**
- **Code-sharing scams: protecting your customers from people who ask for their SMS code**
- **Limits against abuse: codes per number per hour and the wait between resends**

- The code entry screen: the field, a countdown, attempts left and clear messages
- Sending one-time codes (OTP) by SMS safely: expiry, attempt limits and logs
- Transactional SMS: order notices, confirmations and alerts your customers expect

Mozout

MozOut International

RLX Holdings (Pty) Ltd. · Group RLX Holdings

TAX NO. (SARS)	943 907 6234
REGISTRATION NO. (CIPC)	2025/667953/07
REGISTERED OFFICE	1111 Olive Street Saint Louis 63101, Missouri, United States
CONTACT	info@mozout.com · +27 78 823 3325 · www.mozout.com
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

Online version of this document

RLX-INT-KB-7980 · v2026.11.13 · Generated on 14/11/2026 03:12