interweb

Generated on 13/11/2026 18:07

KNOWLEDGE BASE · PUBLIC DOCUMENT

SMS fraud through your code form: how credits get burnt and how to stop it

Security

CODE
RLX-AO-KB-2648

VERSION
v2026.11.13

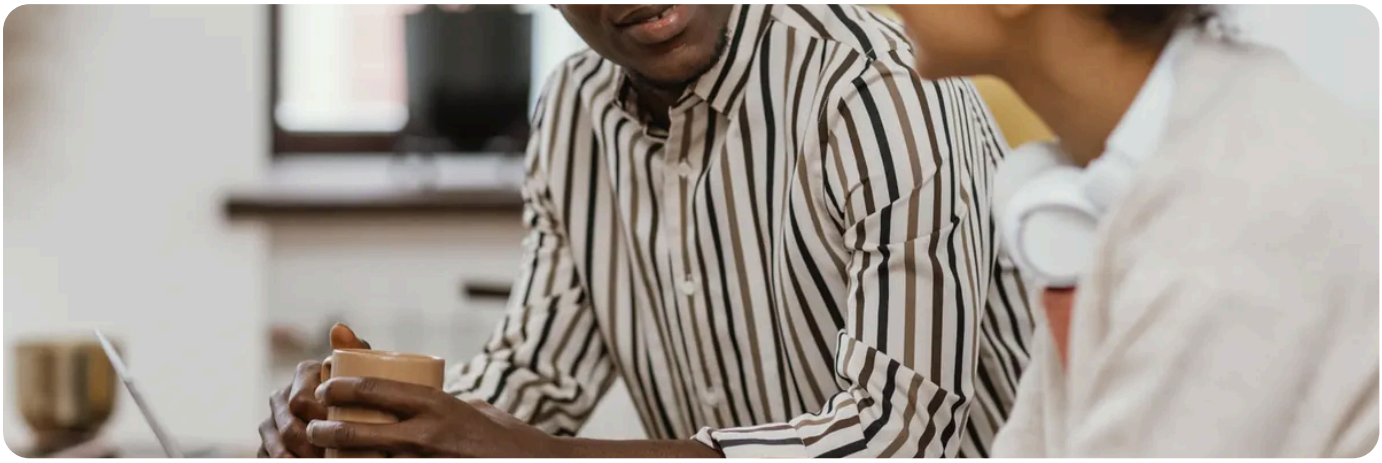
COUNTRY · LANGUAGE
Angola · English

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/2648

SMS fraud through your code form: how credits get burnt and how to stop it

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



The short answer: to an abuser, a form that sends SMS codes is a button that spends your credits. Bots type numbers in sequence and press “Send code” thousands of times; every request is an SMS you pay for. The defence comes in layers: brakes on your form (captcha, limits per IP and per session), the account rules in the verification API, and an eye on your balance.

How it happens

Sign	What it usually is
Lots of codes requested and almost none checked	A bot firing the form; nobody is reading the SMS
Numbers in sequence or with the same start	A generated list, not real customers
Many requests from the same IP or session	A program, not a person
Requests at odd hours, in volumes you have never had	An attack, not one of your campaigns
The SMS balance dropping fast with no new sales	Credits being burnt

The layers of defence

1. **A captcha before sending the code.** It is the cheapest brake on bots. Put it on the “Send code” button, not only at the end of the form.

2. **Limits in your system per IP and per session.** A person does not need codes for ten different numbers in a few minutes. Above your limit, do not call the API.

3. **The account rules in the API.** Turn on the wait between resends and the maximum codes per number per hour; by default they are off (see **limits against abuse**).

4. **Ask for the code only when needed.** After the right password, not before; at the end of checkout, not on the first page.

5. **Watch the balance.** `GET /v1/sms/balance` returns your credit balance. An alert in your system when the day's use goes beyond normal warns you before the balance runs out.

One help comes built in: the API only accepts numbers in Angola and Mozambique. Numbers from other countries, which are often behind this kind of fraud, never go out.

The key's spending limit does not cap SMS credits.
That limit is in currency and does not apply to the credits in your SMS balance. So the brakes have to be the ones above: your form, the account rules and a watched balance.

If it is already happening

1. **Turn on the account rules now**, in Meu Interweb (API keys page) or with `PUT /v1/sms/otp-settings`.

2. **Switch off the "Send code" button** on your site while you add the captcha and the limits.

3. **If you suspect the key was copied**, revoke it and create another: see **a leaked API key**.

4. **Talk to us: open a support ticket** with the times and volume of the attack.

Test the brakes in the Sandbox.
There you can fire your form as often as you like, watch the limits work and not spend a single credit.

NEED A HAND?

Seeing SMS use you do not recognise? Talk to us and tell us the times and the volume.

Open a support ticket →

SEE ALSO

- Limits against abuse: codes per number per hour and the wait between resends
- How much SMS verification costs: credits per code, free checks and a monthly estimate
- Code-sharing scams: protecting your customers from people who ask for their SMS code
- Resending, cancelling and replacing a verification code: what happens to the old one
- An API key or token has leaked: what to do, in the right order
- Sending one-time codes (OTP) by SMS safely: expiry, attempt limits and logs

interweb

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

Online version of this document

RLX-AO-KB-2648 · v2026.11.13 · Generated on 13/11/2026 18:07