interweb

Generated on 13/11/2026 19:28

KNOWLEDGE BASE · PUBLIC DOCUMENT

Fake SMS in your company's name: helping customers recognise your real transactional messages

Security

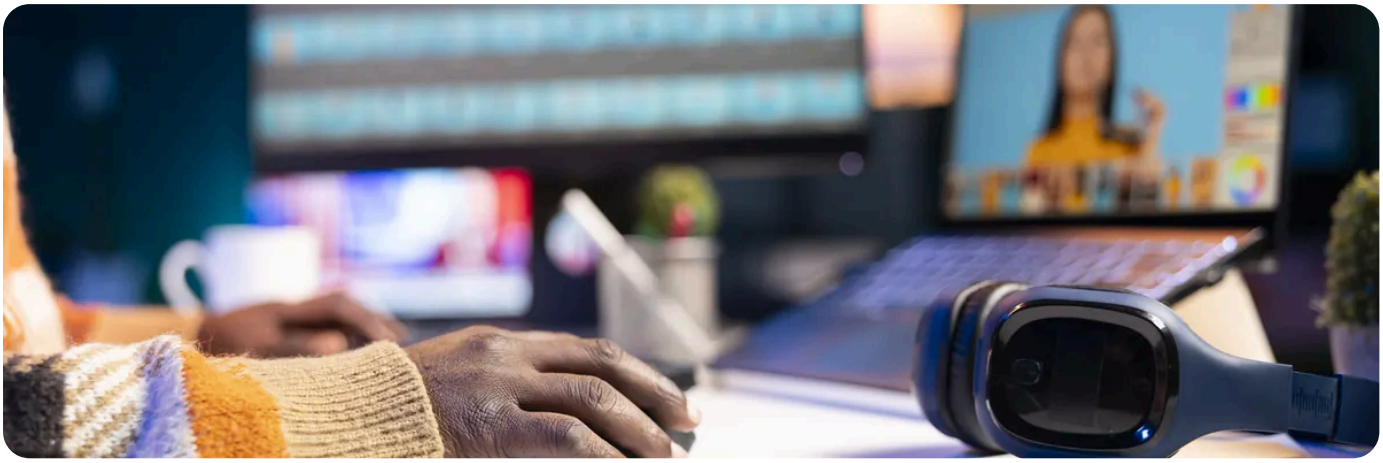
CODE	VERSION	COUNTRY · LANGUAGE
RLX-MZ-KB-2604	v2026.11.13	Mozambique · English

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/2604

Fake SMS in your company's name: helping customers recognise your real transactional messages

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



The short answer: some people send SMS pretending to be a bank, a courier or a well-known business, to steal data or money. Your customers' best defence is **knowing what your real messages look like**: always the same sender, always the same style, **never** a request for a password, PIN or code, and never a link to an address that is not yours.

What fake messages look like

Sign	Example of a fake message
Urgency and threats	«Your account will be blocked today. Confirm your details.»
Asking for a password, PIN or code	«Send us the code you received to validate your delivery.»
An odd link	An address that looks like yours, with swapped letters or an extra word.
An unexpected payment	«Pay a customs fee to receive your parcel.»
A different sender	A random number, or a name other than the one you normally use.

What makes your messages recognisable

1. **One sender.** Always use your Sender ID. Our team registers the name with the mobile operators, and customers get used to seeing it. See **what a Sender ID is**.

2. **A fixed style.** The same opening, the same references (order or invoice number), the same contact details.

3. **Nothing to ask for.** Your transactional texts inform; they do not ask for details, passwords, PINs or codes.

4. **Links only to your own domain**, always the same one, or no link at all. When in doubt, «see our website» is better than a shortened address.

Tell your customers

Put one simple sentence on your website, on receipts and in your welcome e-mail: **«We will never ask for your password, PIN or a code by SMS.»** And say which name your messages arrive under. A customer who has been told deletes the fake and calls you about it.

When fake SMS appear in your name

1. **Warn your customers** through your own channels: website, social media, e-mail, and an SMS from your usual sender.

2. **Keep examples** of the fake messages (a screenshot showing the sender and time) and report them to the authorities and the mobile operators.

3. **Make sure it is not your account.** Check the SMS Center history to see whether those messages went out from there. If you suspect your API key leaked, revoke it and create another: **what to do, in the right order**.

If the fake messages really did come from your account

, open a support ticket in Meu Interweb straight away, with the times and examples. Do not include your API key in the ticket: support does not need it.

RECOMMENDED

Want customers to always recognise your messages? See Transactional SMS.

See Transactional SMS →

SEE ALSO

- **What never to put in a transactional SMS: passwords, full card numbers and private details** →
- **What a Sender ID is: SMS that arrive with your company name instead of a number** →

An API key or token has leaked: what to do, in the right order

Transaction alert SMS for banks, microfinance and payment services: what to include

Sending one-time codes (OTP) by SMS safely: expiry, attempt limits and logs

SMS good practices and consent: who you may send to and how to let people opt out

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-2604 · v2026.11.13 · Generated on 13/11/2026 19:28