interweb

Generated on 13/11/2026 18:08

KNOWLEDGE BASE · PUBLIC DOCUMENT

Code-sharing scams: protecting your customers from people who ask for their SMS code

Security

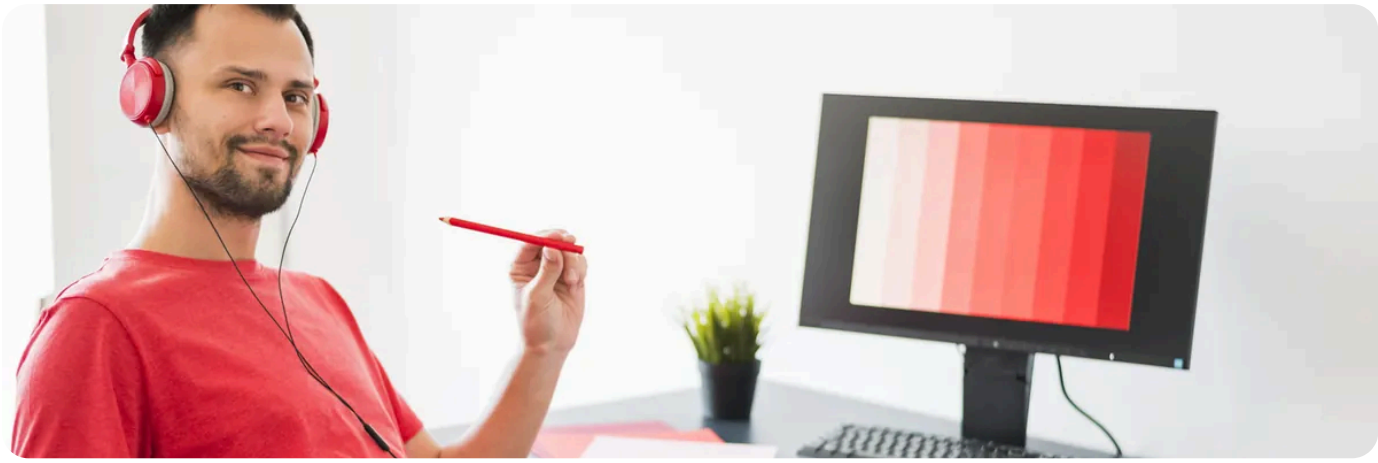
CODE	VERSION	COUNTRY · LANGUAGE
RLX-AO-KB-2650	v2026.11.13	Angola · English

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/2650

Code-sharing scams: protecting your customers from people who ask for their SMS code

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



The short answer: an SMS code only protects while it stays on the customer's phone. The most common scam does not attack your API, it attacks the person: someone calls or writes pretending to be from your company, the bank or the mobile operator, and talks the customer into reading out the code. On your side, the defence lies in the SMS text, in the rule that nobody on your team ever asks for codes, and in what you do when a customer says they fell for it.

How it usually goes

The story they tell	What the code is really approving
"We sent you a code by mistake, could you read it to me?"	Signing in to the customer's account, or changing the number
"To cancel this purchase, tell me the code you received"	The purchase itself, or a transfer
"You have won a prize; confirm the code to collect it"	A payment or a new payee
"I am from the technical team, I need the code to fix the problem"	Access to the account

What your SMS should say

1. **What the code is for.** "Code 739204 to confirm your payment" is much harder to use in a scam than "Your code is 739204".

2. **"Do not share it."** Three words the Verification SMS page recommends for every code.

3. **“Our staff will never ask for it.”** If it fits, this is the line that unravels the fake call.

4. **Who is sending.** Your company name at the start of the text and, if possible, a **Sender ID**: customers get used to seeing your codes always under the same name.

5. **No links.** A code SMS needs no address at all. A code with a link looks far too much like the fake messages.

An example that fits in one SMS: `[COMPANY]: code {code} to confirm your payment. Do not share it. Our staff never ask for it.`.

The house rule, and when a customer falls for it

Write it down and teach it to the whole team: **nobody ever asks a customer for a code**, not by phone, not by message, not at the counter. The customer types the code on your website or app, and only there. Named senders cannot receive replies, so asking the customer to “reply with the code” makes no sense either.

1. **Cancel anything pending** with `POST /v1/sms/otp/{id}/cancel` and stop the transaction in your system if it has not gone through yet.

2. **Close the account's open sessions** and ask the customer to change the password.

3. **Check the recovery details**: if the scam was used to change the number or e-mail, restore them with an identity check.

4. **Log the case**, with the code times (`created_at` and `verified_at`), to spot the pattern and warn other customers.

Do not use the code as proof of identity on the phone.
Asking a customer to read a code “to confirm it is them” teaches exactly the behaviour scammers exploit.

A notice after every sensitive action
helps the customer react in time: “A payment was confirmed on your account. If this was not you, call [PHONE].” It goes out as a normal SMS; ideas in **transactional SMS**.

RECOMMENDED

Want your codes to say clearly what they are for and who sent them? See Verification SMS.

See Verification SMS →

SEE ALSO

- Writing the verification SMS: the code placeholder, your Sender ID and staying in one part →
- Confirming payments, withdrawals and transfers with an SMS code: one code per operation →
- Changing a customer's phone number safely: confirm the new number before saving it →
- Two-step login with an SMS code on your own site or app →
- What a Sender ID is: SMS that arrive with your company name instead of a number →
- 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-2650 · v2026.11.13 · Generated on 13/11/2026 18:08