interweb

Generated on 15/11/2026 00:16

KNOWLEDGE BASE · PUBLIC DOCUMENT

Someone asked for your WhatsApp code or took over the number: what to do

Security & Consent

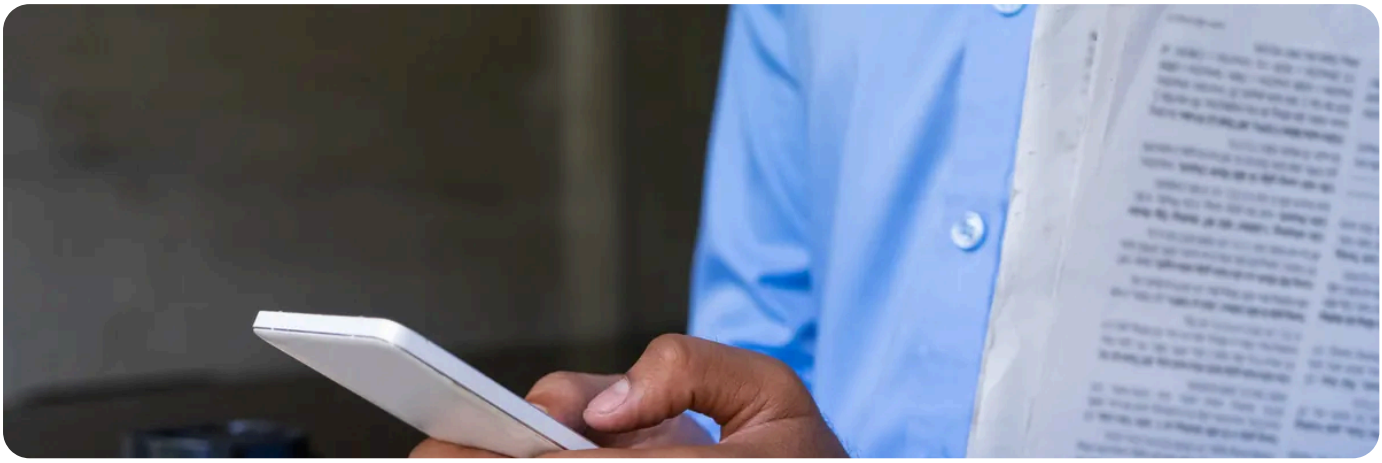
CODE	VERSION	COUNTRY · LANGUAGE
RLX-AO-KB-1512	v2026.10.10	Angola · English

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/1512

Someone asked for your WhatsApp code or took over the number: what to do

Security & Consent Created on **October 10, 2026** 3 min read



The short answer: the six-digit code WhatsApp sends by SMS or call is used to **register your number on a phone**. Whoever gets it takes your account. So **never tell it to anyone**, not even to a "friend" who asked by message. If you have already given it, or the code arrived without you asking, act now: the first step is to register again on your own phone, which throws the intruder out.

How it happens

Scam	How it presents itself
The "friend" in trouble	A message from a contact whose account was already taken: "I sent you a code by mistake, can you pass it on?". Whoever gives it hands over their account.
The fake prize or fake delivery	"To receive the prize, confirm the code you received." Same thing.
A code that arrives unasked	Someone is trying to register your number at that very moment. They are not in yet: they lack the code.
A SIM swap	The intruder talks the operator into moving your number to another SIM. In that case the codes go to them.

If the code arrived and you did not ask for it

1. **Do not share it or write it anywhere.** Ignore it. Without it, whoever tried gets nowhere.

2. **Switch on WhatsApp's two-step verification now** (in the account settings). A six-digit PIN, yours alone, is asked for whenever the number is registered again. Add a recovery e-mail for that PIN too.

3. **Warn whoever wrote to you.** If a contact asked for the code, their account has been taken; tell them through another channel.

If you already gave it, or lost the account

1. **Install or open WhatsApp on your phone and register the number.** Ask for a new code and use it: registering on your phone ends the intruder's session.

2. **If it asks for a PIN you did not set,** the intruder switched on two-step verification. WhatsApp's help says how long you must wait before the number can be reset without the PIN. It is a waiting period, but it passes.

3. **Once in, check "Linked devices"** and end the sessions you do not recognise. Switch the PIN on with a recovery e-mail.

4. **Warn your contacts and groups,** through another channel: "messages sent from my number between such and such a time were not mine".

5. **Ask WhatsApp for help** from within the app (Settings, Help) if you cannot recover the number.

If you lost control of a company number,
customers keep writing to it and the intruder answers them. Tell them on every channel (site, e-mail, social networks) that the number was compromised, and confirm payments by another route. See **the risks of WhatsApp for business**.

If the code does not arrive when you need it, the cause is a different one and has a different article: **the WhatsApp verification code does not arrive**. So that a company number is never tied to a single phone, see **choosing the number for a WhatsApp API**.

NEED A HAND?

Were you the victim of a scam that also involved your domain or e-mail? Write to us.

Open a support ticket →

SEE ALSO

- **WhatsApp for business: the risks, and the practices that avoid them**
- **The WhatsApp verification code does not arrive: what to try**
- **Fake WhatsApp messages in your company name**
- **Which two-step verification to use**

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-1512 · v2026.10.10 · Generated on 15/11/2026 00:16