interweb

Generated on 21/10/2026 16:00

KNOWLEDGE BASE · PUBLIC DOCUMENT

How to tell whether an e-mail really came from us

Security

CODE	VERSION	COUNTRY · LANGUAGE
RLX-AO-KB-302	v2026.09.28	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/302

How to tell whether an e-mail really came from us

Security Created on **September 11, 2026** Updated on **September 28, 2026** 4 min read

A fake message pretending to be your hosting provider is the most common attack against accounts like yours - and the most profitable one to run, because a single password opens the site, the e-mail and the domain all at once. It is worth knowing how to tell them apart.

Which addresses we write from

We **always write from** `interweb.ao`, and only from these four addresses:

Address	What for
nao-responda@interweb.ao	Automatic messages: invoices, renewal notices, activations. It does not take replies.
suporte@interweb.ao	Replies to technical support requests.
vendas@interweb.ao	Sales and billing matters.
info@interweb.ao	General contact.

But on its own, this proves nothing.
The name shown as the sender **can be written to say anything**. Anyone can send a message that *claims* to come from `suporte@interweb.ao`. That is why this article does not end here: looking at the address is the first step, not the proof.

What actually confirms it: the headers

Every message carries a record of the checks the receiving server performed. There are three, and what matters is that they say **PASS**:

```
spf=pass      the sending server was authorised
dkim=pass     the signature matches and nobody altered the message
dmarc=pass    the sender's domain agrees with that signature
```

1. In **Gmail**, open the message, click the three dots and choose *Show original*. The three lines are right at the top.

2. In **Outlook**, open the message in its own window and go to *File → Properties*, in the headers box.

3. In **webmail**, look for the option to view the raw message or its source.

If any of them says **fail** or **softfail**, be suspicious - even if the address looks right. For what these three records are and how they work, see **SPF, DKIM and DMARC**.

The signs of a fake message

Sign	Why it is suspicious
Urgency with a threat	«Your account will be suspended in 24 hours.» The pressure is there to make you click before you think. Our notices give you **days**, and they are always visible in the portal.
The link does not go where it says	Hover over it without clicking and read the real address at the bottom. On a phone, press and hold. If it does not start with **https://www.meu.interweb.ao**, it is not ours.
It asks for your password	We never ask for it. Not by e-mail, not by chat, not on the phone.
It changes payment details	The most expensive sign of all. See the section below.
An attachment you were not expecting	Our invoices are PDFs and they are always in the portal. A .zip, an .exe, or a document asking you to enable macros is never ours.
Odd wording	Machine translation, your name wrong, or a form of address that is not the usual one.

What we never ask you for

1. **We never ask for your password.** We do not need it for anything: from our side we can see what we need without it. Whoever asks you for it is not us.

2. **We never ask you to confirm card details by e-mail**, nor through any form outside the portal.

3. **We never send you a verification code to read back to us.** If you receive a code you did not request, somebody is trying to get into your account - change the password and turn on **two-factor authentication**.

The changed-bank-account fraud - read this one carefully.
There is a specific scam aimed at anyone who pays by transfer: a message arrives looking like ours, saying we have **changed banks** and asking you to pay into a new account. **Do not pay.** Our bank details are on the invoice inside the portal, and those are the ones that count. If we ever do change account, it will appear in the portal - and even then, call us to confirm before transferring. A sent transfer cannot be undone.

The one rule that replaces all the others

Do not click the e-mail. Go to the portal. Type `www.meu.interweb.ao` into the browser with your own hands, and log in. If the message was genuine, whatever it says is in there: the invoice, the notice, the request. If it is not in there, it does not exist.

That single rule makes nearly every scam useless, and it asks you to understand nothing about headers.

I already clicked. Now what?

1. **Change the password now** - the portal one, and the cPanel one if they are similar. See **how to recover access to your account**.

2. **Turn on two-factor authentication.** From then on, the stolen password alone is no longer enough.

3. **Look at what changed:** e-mail accounts you did not create, new forwarders, the account's contact details, and your domains' nameservers.

4. **Tell us** through the **portal, by opening a ticket** - we can see recent logins and tell you whether anyone got in.

If you suspect the site itself was tampered with, that is a different path: **how to tell if your site has been compromised**.

Got a fake one? Send it to us

Forward it to `suporte@interweb.ao` with the headers included, if you know how. It lets us warn other customers and ask for the address used to be shut down. It is not a bother - it is useful.

NEED A HAND?

Received something odd in our name? Show us.

Open a ticket →

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-302 · v2026.09.28 · Generated on 21/10/2026 16:00