interweb

Generated on 13/11/2026 17:46

KNOWLEDGE BASE · PUBLIC DOCUMENT

Lookalike addresses used to fool your customers: spotting them and what to do

Security

CODE	VERSION	COUNTRY · LANGUAGE
RLX-AO-KB-2424	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/2424

Lookalike addresses used to fool your customers: spotting them and what to do

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



The short answer: a scammer registers a domain almost identical to yours (one letter swapped, an extra hyphen, another extension) and writes to your customers as if they were your company, nearly always to **change the bank details** for a payment. SPF, DKIM and DMARC do not stop it, because the domain is theirs and correctly set up. The defence is different: **read the address carefully**, **confirm by phone** any change of payment details and **warn customers** before it happens.

What lookalike addresses look like

Trick	The real one	The fake
Letters that blur together	`yourcompany.ao`	`yourcornpany.ao` ("rn" looks like "m")
An extra hyphen or letter	`yourcompany.ao`	`your-company.ao` , `yourcompanys.ao`
Another extension	`yourcompany.ao`	`yourcompany.co.ao`
The right name, a free webmail domain	ana@ at the company	the company name on some free address

Signs of a fake message

1. **It asks you to pay into a new account**, "because we changed banks".
2. **It is in a hurry**: "today without fail", "or the service will be cut off".
3. **The address is almost the usual one**, or the Reply-To differs from the sender: **what Reply-To is**.

4 **It continues a real conversation.** Sometimes the scammer has read old messages and replies within the same subject. A familiar subject proves nothing.

What to do

1 **Confirm by phone**, on a number you already had (not the one in the message), any request to change bank details.

2 **Warn customers in writing, in advance:** a line on invoices and in your signature, such as "We never change our bank details by e-mail".

3 **Register the most obvious variations** of your domain, especially the other extension. A domain you hold cannot be used against you.

4 **Report the fake domain.** If the site or domain is with us, use **report abuse**. If not, **WHOIS** shows who manages it, so you can send them the complaint.

If a customer has already paid into the wrong account,
the first call is to their bank, as fast as possible. Then keep the messages with their full headers, which are the evidence for the bank and the police.

It may also be your mailbox.
If the scammer knew real conversations and amounts, someone may have read your mail. Change passwords and check forwarders: **what to do when the account was hacked**. For other channels, see **fake WhatsApp messages**.

RECOMMENDED

Want to protect your name? Register the variations of your domain before someone else does.

Search for a domain →

SEE ALSO

- **How to recognise a phishing e-mail or message, and what to do if you clicked** →
- **Someone is sending e-mail in the name of your domain: what SPF, DKIM and DMARC do about it** →

Replies going to the wrong address: setting Reply-To in webmail and Outlook

Fake WhatsApp messages in your company name: protecting customers from scams

Everyday e-mail habits for a business: To, Cc and Bcc, reply all, subjects and attachments

Your e-mail account has been hacked: what to do in the first hour

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-2424 · v2026.11.13 · Generated on 13/11/2026 17:46