interweb

Generated on 13/11/2026 17:45

KNOWLEDGE BASE · PUBLIC DOCUMENT

Threats sent from your own address: why extortion e-mails show you as the sender

Security

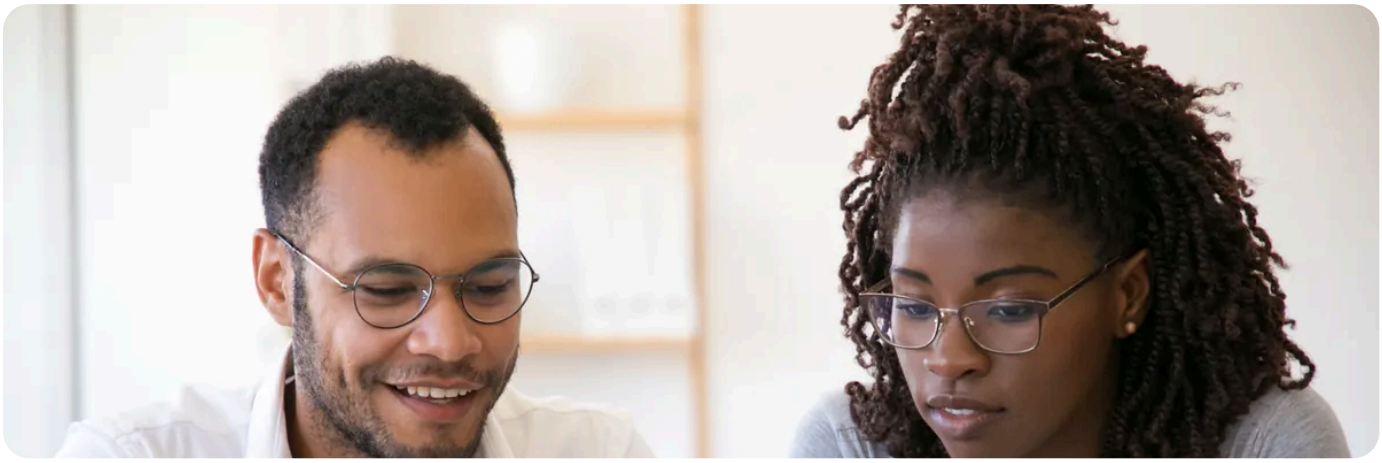
CODE	VERSION	COUNTRY · LANGUAGE
RLX-AO-KB-2404	v2026.11.13	Angola · English

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/2404

Threats sent from your own address: why extortion e-mails show you as the sender

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



The short answer: you received an e-mail that seems to come **from your own address**, saying your mailbox or computer was broken into and demanding cryptocurrency to keep quiet. It is almost always **fake**: the sender of an e-mail is just text anyone can type, like the return address on a letter. **Do not reply, do not pay and do not click anything.** Then check two simple things, below.

Why it looks like it came from you

The "From" field is not checked by whoever sends the message, and the scammer types your address there to scare you: "if I send from your address, I must be in your account". They are not. The message left some server far from ours. If you open the header, the Received lines show where it really came from: **how to read the header**.

Sometimes the message quotes a **real password** of yours. That is scarier, but it has another explanation: the password came from an old data breach at a site you signed up to, and it sits on lists that are sold online. It does not mean your mailbox was broken into, but it does mean that password is worthless now.

What to do

1. **Do not reply and do not pay.** Replying confirms a person reads the address, and paying only brings more messages.
2. **Mark it as spam** in webmail or your e-mail program, and delete it.
3. **If it quotes a password you still use,** change it now everywhere you use it, starting with the mailbox: **changing a mailbox password**.
4. **Check the mailbox is not sending by itself:** look at the Sent folder in webmail. If there are messages you did not write, then there is a real problem: follow **what to do when the account was hacked**.

How to see fewer of these

Your domain's **DMARC** record tells receiving servers what to do with messages that use your domain without permission. With a stricter policy, many of these fakes are rejected or sent to spam, in your customers' mailboxes and in yours. See **someone is sending e-mail in the name of your domain**.

Do not open attachments or links in these messages.
Some carry a "proof" that is really malicious software. If you already opened one, see **what to do if you clicked**.

Warn the team.
These messages often reach several people in the company at once. A short warning stops someone paying out of fear.

NEED A HAND?

Got one of these and want to be sure your mailbox is safe? Open a ticket and we will check with you.

Open a support ticket →

SEE ALSO

- **Someone is sending e-mail in the name of your domain: what SPF, DKIM and DMARC do about it** →
- **How to recognise a phishing e-mail or message, and what to do if you clicked** →
- **Your e-mail account has been hacked: what to do in the first hour** →
- **Reading an e-mail header: did SPF, DKIM and DMARC pass?** →
- **How to change an e-mail account password** →
- **A strong password and a password manager: how to stop reusing the same one** →

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

RLX-AO-KB-2404 · v2026.11.13 · Generated on 13/11/2026 17:45

Online version of this document