

KNOWLEDGE BASE · PUBLIC DOCUMENT

Forgotten subdomains and DNS records that point nowhere: how they get hijacked

Security

CODE

RLX-MZ-KB-1984

VERSION

v2026.10.15

COUNTRY · LANGUAGE

Mozambique · English

Interweb Mozambique

RLX Holdings, S.A. · Group RLX Holdings

Tax ID (NUIT) 401 191 607 · Legal entity no. (NUEL) 105 045 974 · Economic activity code (CAE) 62022

<https://www.meu.interweb.co.mz/knowledgebase/1984>



The short answer: when you stop using a service but **forget the DNS record** that pointed to it (a CNAME to a shop, a blog or an application you cancelled), someone can open an account at that service, claim the name and **show whatever they like on your subdomain**, with your domain in the address. The defence is simple: clean the DNS.

What the site needs

What	What to do
How it happens	A subdomain (shop.your-domain.com) points by CNAME to a service. The service is cancelled, but the record stays. Another customer of the service claims the name.
What the attacker gains	A page with your domain in the address: useful for scams, for stealing passwords and for looking legitimate.
Address records (A)	An A pointing to an IP that is no longer yours may end up on someone else’s machine.
Warning signs	Subdomains that show the service’s error (“site not found”, “does not exist”) or pages you do not recognise.
Who is at risk	Anyone who has had several services, changed provider or application, and never cleaned the DNS zone.

Getting started

1

Take a copy of the zone: open the Zone Editor and keep a list (or a screenshot) of all the records.

2

Go through each CNAME and each A and ask: where does it point, and do I still use that? **DNS records**.

3

Open each subdomain in the browser: if it shows the destination service's error, it is a candidate.

4

Delete the ones you do not use. A record that serves nothing can only do harm. If you are not sure, change it temporarily so you can delete it a few days later.

5

When you cancel a service, delete its DNS record the same day. When you move DNS, check the list: **Moving the DNS zone**.

Do not delete blindly. Some records look odd but serve e-mail or a verification (MX, TXT, SPF). If in doubt about a record, ask first: deleting the wrong one can cut your e-mail. The e-mail records are in **SPF, DKIM and DMARC**.

To limit who can issue certificates for your domain, see **CAA records**. For a subdomain that points to another service: **A or CNAME**.

Found a subdomain you do not recognise? Open a ticket with the name and do not delete it before telling us.

[Open a support ticket](#)

SEE ALSO

DNS records explained: A, CNAME, MX, TXT and TTL

Moving your DNS zone to a new provider and checking it before you switch

CAA records: who may issue certificates for your domain

Pointing a subdomain to another server or service: A record or CNAME

SPF, DKIM and DMARC: why your e-mail lands in spam



Online version of this document

Interweb is a leading internet services company, with a mission to help businesses to be born and prosper through technology.

2020

FOUNDED

37,000+

CLIENTS

130+

SIGN-UPS A DAY

Interweb Mozambique

RLX Holdings, S.A. • Group RLX Holdings

TAX ID (NUIT)	401 191 607
LEGAL ENTITY NO. (NUEL)	105 045 974
ECONOMIC ACTIVITY CODE (CAE)	62022
REGISTERED OFFICE	Bairro 7 de Setembro Vilankulo 1304 • CEP 0411-02, Inhambane, Mozambique
CONTACT	info@interweb.co.mz • +258 84 635 1111 • +258 86 635 1111 • www.interweb.co.mz
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed