interweb

Generated on 15/11/2026 00:16

KNOWLEDGE BASE · PUBLIC DOCUMENT

Fake orders and spam sign-ups in WooCommerce: how to stop them

Customers, E-mails & Policies

CODE	VERSION	COUNTRY · LANGUAGE
RLX-AO-KB-1636	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/1636

Fake orders and spam sign-ups in WooCommerce: how to stop them

Customers, E-mails & Policies Created on **October 10, 2026** 3 min read



One day the shop wakes up with dozens of pending orders from odd names, small amounts and made-up e-mails. Or with hundreds of new accounts nobody created. It is not bad luck: it is **automatic programs** testing forms, or trying stolen cards on small shops with low amounts. You stop it in layers, from the simplest to the strongest, and you clean up with care.

How to recognise it

Sign	What it usually is
Many pending or failed orders in a short time, of low value	Card testing: someone is trying stolen numbers on your shop.
New accounts with random e-mails	Automatic sign-up by a program.
Meaningless names and addresses, all alike	A form filled in by a program.
A spike of checkout requests with no rise in visits	The program goes straight to checkout, without looking at the shop.

Stopping it, in layers

1. **See what the payment method offers.** Many operators have anti-fraud tools (limits, verification). If someone is testing cards, tell the operator: they care.

2. **Add a captcha** to registration and checkout, with a captcha plugin. See **a captcha on the WordPress login** for the idea; shops use the same principle at checkout.

3. **Switch off what you do not use.** If the shop allows guest checkout, turn off open registration on “My account”. Fewer doors, fewer programs at the door.

4. **Block what repeats.** Addresses, countries or ranges that bring only spam can be blocked: **blocking an IP address**. If you use Cloudflare, it has rules to limit requests (depending on your plan) to checkout (**Cloudflare options**).

5. **Require e-mail confirmation** on new accounts, with a plugin. Accounts with fake e-mails never confirm.

6. **Moderate reviews** and comments: **stopping spam comments**.

7. **Ship nothing that is not paid.** A pending order is not a sale: see **order statuses**.

Cleaning up

1. **Take a backup first.** A bulk clean-up cannot be undone.

2. **Delete only the orders and accounts you recognise as fake.** Sort by date and e-mail to catch them together. Do not delete paid orders by mistake.

3. **Check the state of the server.** A wave like this uses processor and database; if the shop became slow, see **what eats CPU on a website**.

Card testing can cost you.
Operators may charge for declined payments or suspend the account if there are many. If you see a wave, speak to the operator at once, and speed up the layers above.

Look at the access logs at the time of the spike.
If all the fake requests come from a few addresses, blocking solves it; if they come from thousands, the defence is the captcha and the operator. And keep the shop and plugins updated: **updating without breaking anything**.

NEED A HAND?

Under attack right now and the shop cannot cope? Tell us the address and the time of the spike, and we will go through the access logs with you.

Open a support ticket →

SEE ALSO

- A captcha on the WordPress login →
- Blocking an IP address →
- How to tell if your site has been compromised →

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-1636 · v2026.10.10 · Generated on 15/11/2026 00:16