interweb

Generated on 21/10/2026 17:25

KNOWLEDGE BASE · PUBLIC DOCUMENT

A website form that is safe and spam-free: honeypot, captcha and validation

Security

CODE	VERSION	COUNTRY · LANGUAGE
RLX-MZ-KB-1526	v2026.10.10	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/1526

A website form that is safe and spam-free: honeypot, captcha and validation

Security Created on **October 10, 2026** 3 min read



The short answer: a form is a door that anyone, and any robot, can try. To keep it **spam-free**, add a trap field (a *honeypot*) and, if needed, a captcha. To keep it **safe**, validate everything on the server, never trust what arrived, and do not let a text field go into the e-mail or the database as it is. The two kinds of care go together.

Against spam: from the quietest layer to the most visible

Defence	How it works	Annoyance to the visitor
Honeypot	A field hidden with CSS. A person does not see it or fill it in; a robot fills in everything. If it comes back filled, you discard it.	None.
Minimum time	A form sent one second after it opened was sent by a robot.	None.
Rate limit	Few messages a minute per address. It slows down whoever insists.	Hardly any.
Captcha	Asks the visitor to prove they are a person. Some versions do not even ask for clicks (reCAPTCHA, hCaptcha, Cloudflare Turnstile).	Medium. Some visitors give up.
Moderation	Nothing is published without approval. It applies to comments and reviews.	A delay in publishing.

Start with the first two: they cost little and stop most simple robots. Add the captcha only if the spam carries on. In WordPress, most form plugins have these options as tick boxes; for comments, see **stopping spam comments in WordPress**, and for a shop, **fake orders and spam sign-ups**.

For safety: what the code has to do

1. **Validate on the server.** Validation in the browser (the field that says “invalid e-mail”) is only a courtesy: a robot never goes through it. On the server, confirm the e-mail is an e-mail, the length is reasonable and the required fields exist.

2. **Never let the visitor’s text touch the database as it is.** Use prepared statements, where the instruction and the data travel separately. It is the defence against “SQL injection”, where a field filled in with an instruction becomes part of your query.

3. **Neutralise the text before showing it** on a page, by converting special HTML characters. It is the defence against scripts inserted by whoever filled in the form (XSS). In PHP, the `htmlspecialchars` function does this.

4. **Watch the e-mail header.** If the sender address and subject come from the form, anyone who puts a line break there can add recipients and use your server to send spam. Strip line breaks from those fields, and prefer sending with authentication, as in **sending e-mail with PHPMailer**.

5. **If you accept files,** accept only the types you need, limit the size, rename them and never store them in folders where code can run. A “resume.pdf” that is really a PHP program is an old class of attack.

Do not put the destination e-mail in the form as a hidden field.
Anyone who sees it can use your form to send messages to anyone. The destination stays on the server.

If the form’s messages do not reach the inbox, the cause is rarely spam: see **a contact form that actually reaches your inbox**. And if you have to store personal data sent by visitors, read **personal data protection: what applies to your website**.

NEED A HAND?

Receiving hundreds of fake messages, or was the form used to send spam? Tell us the domain.

Open a support ticket →

SEE ALSO

- **A contact form that actually reaches your inbox** →

- **Stopping spam comments in WordPress**
- **Sending e-mail from your own code with PHPMailer**
- **Personal data protection: what applies to your website**

interweb

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

Online version of this document

RLX-MZ-KB-1526 · v2026.10.10 · Generated on 21/10/2026 17:25