interweb

Gerado a 15/11/2026 00:29

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Um formulário de site seguro e sem spam: honeypot, captcha e validação

Proteção do site e privacidade

CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-AO-KB-1508	v2026.10.10	Angola · Português

Interweb Angola
RLX Angola, Lda. · Grupo RLX Holdings
NIF 500 260 5724 · Matrícula 26464-25/250724

https://www.meu.interweb.ao/knowledgebase/1508

Um formulário de site seguro e sem spam: honeypot, captcha e validação

Proteção do site e privacidade Criado em **10 de outubro de 2026** 3 min de leitura



A resposta curta: um formulário é uma porta que qualquer pessoa, e qualquer robô, pode experimentar. Para o ter **sem spam**, ponha um campo-armadilha (*honeypot*) e, se for preciso, um captcha. Para o ter **seguro**, valide tudo no servidor, nunca confie no que chegou, e não deixe um campo de texto passar para o e-mail ou para a base de dados tal e qual. Os dois cuidados fazem-se juntos.

Contra o spam: da camada mais discreta à mais visível

Defesa	Como funciona	Incómodo para o visitante
Honeypot	Um campo escondido por CSS. Uma pessoa não o vê nem o preenche; um robô preenche tudo. Se vier preenchido, descarta-se.	Nenhum.
Tempo mínimo	Um formulário enviado um segundo depois de abrir foi enviado por um robô.	Nenhum.
Limite de envios	Poucas mensagens por minuto por endereço. Abranda quem insiste.	Quase nenhum.
Captcha	Pede ao visitante que prove que é pessoa. Há versões que nem pedem cliques (reCAPTCHA, hCaptcha, Cloudflare Turnstile).	Médio. Alguns visitantes desistem.
Moderação	Nada se publica sem aprovação. Aplica-se a comentários e avaliações.	Atraso na publicação.

Comece pelas duas primeiras: custam pouco e travam a maior parte dos robôs simples. Só junte o captcha se o spam continuar. No WordPress, a maioria dos *plugins* de formulários traz estas opções em caixas de seleção; para os comentários, veja **travar o spam de comentários**, e numa loja, **encomendas falsas e registos de spam**.

Para a segurança: o que o código tem de fazer

1. **Valide no servidor.** A validação no navegador (o campo que diz «e-mail inválido») é só cortesia: um robô nunca passa por ela. No servidor, confirme que o e-mail é um e-mail, que o tamanho é razoável e que os campos obrigatórios existem.

2. **Nunca ponha o texto do visitante, tal e qual, em contacto com a base de dados.** Use consultas preparadas (*prepared statements*), em que a instrução e os dados vão separados. É a defesa contra a «injeção de SQL», em que um campo preenchido com uma instrução se torna parte da sua consulta.

3. **Neutralize o texto antes de o mostrar** numa página, convertendo os caracteres especiais de HTML. É a defesa contra scripts inseridos por quem preencheu o formulário (XSS). Em PHP, a função `htmlspecialchars` serve para isso.

4. **Cuidado com o cabeçalho do e-mail.** Se o endereço do remetente e o assunto vêm do formulário, quem lá puser uma quebra de linha pode acrescentar destinatários e usar o seu servidor para enviar spam. Retire as quebras de linha desses campos, e prefira enviar com autenticação, como em **enviar e-mail com o PHPMailer**.

5. **Se aceita ficheiros,** aceite só os tipos de que precisa, limite o tamanho, mude o nome e nunca guarde em pastas onde se possa executar código. Um «currículo.pdf» que é, na verdade, um programa PHP é uma classe de ataque antiga.

Não ponha o e-mail de destino no formulário como campo escondido.
Quem o vê pode usar o seu formulário para enviar mensagens a qualquer pessoa. O destino fica no servidor.

Se as mensagens do formulário não chegam à caixa de entrada, a causa raramente é o spam: veja **um formulário de contacto que chega mesmo à sua caixa**. E se tem de guardar dados pessoais enviados pelos visitantes, leia **proteção de dados pessoais no seu site**.

PRECISA DE AJUDA?

Está a receber centenas de mensagens falsas ou o formulário foi usado para enviar spam? Diga-nos o domínio.

Abrir pedido de suporte →

VEJA TAMBÉM

- **Um formulário de contacto que chega mesmo à sua caixa**
- **Travar o spam de comentários no WordPress**
- **Enviar e-mail a partir do seu próprio código com o PHPMailer**
- **Proteção de dados pessoais: o que se aplica ao seu site**

interweb

Interweb Angola

RLX Angola, Lda. · Grupo RLX Holdings

NIF	500 260 5724
MATRÍCULA	26464-25/250724
SEDE	Rua Direita do Patriota, Bairro Dangereux Belas, Luanda, Angola
CONTACTOS	info@interweb.ao · +244 942 011 191 · www.interweb.ao
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado

RLX-AO-KB-1508 · v2026.10.10 · Gerado a 15/11/2026 00:29

Versão online deste documento