Managing spam on web forms

Support Team - 2025-01-24 - Comments (0) - Forms & Lead Capture

Spam submissions through website forms can be frustrating, but it’s a common challenge faced by businesses of all sizes. While no solution can completely eliminate spam, we employ a range of measures to significantly reduce its impact and help maintain the integrity of your website.

Why Does Spam Happen?

Spam form submissions occur for various reasons, including:

- **Promoting malicious links** – Spam submissions often contain links leading to unsafe websites.
- **Automated bot activity** – Bots scour the web to exploit forms for phishing or malware distribution.
- **Blacklisting risks** – If your website sends automated emails to spam-trap addresses, your email server may be blacklisted.

What Can Be Done to Reduce Spam?

We implement several techniques to help minimise spam while ensuring a smooth experience for legitimate users:

1. Google reCAPTCHA

A widely used tool that helps distinguish between real users and bots. We typically recommend reCAPTCHA v3, which works in the background without disrupting the user experience. However, more visible options like reCAPTCHA v2 (where users check a box or complete a challenge) are available if stricter security is needed.

What you need to know:

- reCAPTCHA can reduce spam, but persistent, sophisticated bots may still find ways through.
- More aggressive settings can sometimes block real users, so a balance is necessary.

2. Honeypot Fields

This technique adds hidden fields to forms that normal users don’t see, but spam bots often fill them out, allowing us to detect and discard spam submissions automatically.

What you need to know:

- Honeypots work well against simple bots but may be ineffective against more advanced spam techniques.

3. IP and Email Blacklisting

We can block known spam sources by preventing form submissions from certain IP addresses or email domains.

What you need to know:

- While effective for recurring spam sources, determined spammers can bypass this by using new addresses.

4. Third-Party Spam Protection Plugins

We can integrate specialised anti-spam plugins that offer additional filtering and reporting capabilities. These tools analyse submission patterns and content to detect spam more effectively.

What you need to know:

- Some plugins may require an additional subscription or ongoing management.
- They provide more control and reporting options but may add slight performance overhead.

5. Manual Form Review

In some cases, manually reviewing form submissions and adjusting settings based on recurring patterns can help fine-tune spam protection.

What you need to know:

• This approach requires ongoing monitoring and adjustments to stay effective.

What We Can’t Do

While we take extensive measures to reduce spam, it’s important to understand that:

- **No solution is 100% effective.** Even the best measures cannot guarantee zero spam.
- **Stronger protection can impact user experience.** Adding multiple layers of protection may deter genuine users or introduce usability challenges.
- **Ongoing adjustments may be necessary.** Spam tactics evolve, and periodic updates to settings and filters may be required.

Managing Expectations

We are committed to helping you minimise spam without compromising user experience. However, a level of spam is inevitable. Our goal is to strike the right balance between usability and protection, ensuring your website remains functional and accessible to genuine users.

If you are experiencing excessive spam or need further assistance, please get in touch with your Account Manager to explore tailored solutions.