DDoS and Bot Protection

Last Modified on 06/10/2026 11:02 pm EDT

Digioh runs in your site visitor's browser as externally sourced JavaScript (not from your server). This means that any DDoS or bot activity targeted at Digioh cannot directly impact your site performance.

However, since Digioh connects and sends data to your database (ESP, CRM, etc), we have taken steps to ensure that you are protected from malicious or fraudulent activity such as:

- Attempting to fill your database with junk data
- Brute force discovery of valid email addresses in your system
- Attempts to overwhelm your ESP or CRM (DDoS)
- In cases where Digioh is powering a login form, attempt to guess a password by brute force

The first thing to note is that Digioh forms are powered by JavaScript, which makes them practically immune to "off the shelf" hacking tools and bots. An attacker would have to specifically reverse engineer the Digioh forms on your site and customize their attack. Typically, hackers just move on to an easier target.

That said, Digioh has the following protections against determined attacks:

- Cloudflare CDN-level IP Rate Limiting and Firewall. Cloudflare is the leading provider in DDoS mitigation.
- Built in bot protections designed to deflect and mitigate bot submissions on forms and campaigns
- Digioh application-level IP Rate Limiting. This prevents any **one** computer from attacking your forms.
- Digioh application-level Campaign Rate Limiting. This prevents any single Campaign from submitting too frequently across all IPs. It will start blocking (for 30 minutes) if there are more than 100 submissions within any 10 second rolling window for a particular Campaign. Each new submission renews the 10 second rolling window.

If you have specific security requirements or would like to review additional details about our protections, please contact support@digioh.com.