knowledgeowl

Spam protection

Last Modified on 03/14/2024 8:47 pm EDT

If any part of your knowledge base is publicly available, you're probably interested in preventing spam from reaching you!

There are three main areas you can get spam from:

- The Contact Form: either the full contact form in the live knowledge base, or the Contact tab of Contextual Help Widget (2.0).
- If Comments are enabled and you are not checking the box to "Only allow logged in readers and authors to leave comments". See Comment restrictions and permissions.
- Bogus subscription sign-ups: only generally possible if public subscriptions have been enabled

KnowledgeOwl provides two ways for you to prevent spam:

ReCAPTCHA

reCAPTCHA is a free service from Google that helps prevent spam activity in your knowledge base.

It's designed to verify that someone signing up for a subscription is a real person and not a bot. A "CAPTCHA" is a simple test--usually a task that is very easy for a human to perform, but hard for bots and other malicious software to figure out. There are two versions of reCAPTCHA:

- v2: Verify requests with a challenge. Example: checking a box next to "I am not a robot."
- v3: Verify requests with a score. Example: click on all the images that have cars in them.

KnowledgeOwl currently supports specific versions in specific places:

- v2: Supported in the full knowledge base; not supported in Contextual Help Widget (2.0). For these reCAPTCHAs, configurations with "I am not a robot" reCAPTCHAs, and you can see one in action if you try to subscribe to a category in this knowledge base.
- v3: Supported in Contextual Help Widget (2.0); not supported in the full knowledge base.

Only v2 reCAPTCHAs will work properly in your main knowledge base. We've tested our configurations with "I am not a robot" reCAPTCHAs, and you can see one in action if you try to subscribe to a category in this knowledge base!

See Add reCAPTCHA for more information on setting up reCAPTCHA.

Pros

- Free service provided by Google
- Once set up, you don't have to think about it
- Most readers are familiar with reCAPTCHA processes, since they're used so many places

- Generally very effective at blocking spambot traffic

Cons

- Requires you to set up one or more site keys and secrets with Google and get them configured
- People can get caught in a reCAPTCHA loop, depending on the type of reCAPTCHA you've selected--this is why we recommend using the checkbox version rather than the "select all pictures of xx" version
- reCAPTCHA is a Google-supported tool, and particularly if you have GDPR requirements or concerns, reCAPTCHA might not be a viable option

Honeypot

Honeypots are an alternative way to handle spam protection. Honeypots are used in a variety of ways, but the basic gist is that they create something that is enticing and somewhat irresistible to bad actors.

For things like contact forms, this means that instead of making all readers complete an action or test before they can submit a form, a honeypot might include some hidden form fields that no human will see. Spambots do see them and generally fill them out. Submissions with these fields completed are ignored.

Honeypots might also include time or repeat submission restrictions, where they'll flag repeated submissions from the same reader within xx seconds of each other, or flag submissions that took fewer than xx seconds to fill out.

Our built-in honeypot function works similarly to these options (though for security reasons, we can't tell you the full details!).

Pros

- Simple setup: check a box, Save, and you're done; no registration or site keys to configure
- Better end-user experience for your average human reader (no tests/tasks to complete)

Cons

- If someone seriously wants to attack and spam you, they can figure a honeypot out and bypass it, so they aren't as effective as reCAPTCHA when it comes to dedicated malicious attackers