Preventing Spam Responses

Download the PDF of this article.

In this Article

Related Articles

Stop Spam

Spam is unfortunately an inescapable part of the modern internet.

While there is no 100% surefire way to prevent all spam, there are a variety of steps you can take to reduce and minimize spam submissions.

In this document, we'll talk more about what spam is and the variety of solutions FormAssembly offers to help you stop spam.

What is Spam?

The term spam is used to refer to the many types of unwanted and unsolicited messages and communications people receive.

Though typically associated with email, spam circulation (or spamming) online predates the widespread use of e-mail and originated in online forums.

Spam can now be seen everywhere: on forums; in social media; in email; and most relevant here, in form submissions.

Form Spam

You might think that form spam shouldn't be an issue these days thanks to spam filters. But many spam prevention options are constantly playing catch-up.

In addition, spammers often look for vulnerabilities in forms so they can hijack them and use them to relay email spam messages to others.

In short, **spammers are constantly working to overcome any security or spam barriers** that have been put in place.

Types of Form Spam

Manual Spamming

Manual spamming happens when people manually fill out web forms with spam messages. This type of form spam is the most difficult to stop because human spammers can get through most (if not all) anti-spam measures that you can put in place.

Spambots

Spambot spamming happens when programs are built to seek out web forms on the internet and fill them out. This type of form spam is easier to combat because spambots are not humans and have a tough time getting past some of the more advanced anti-spam measures.

These bots can be programmed to leave junk text and links in form submissions and comments, and they can perform more malicious activities such as taking personal information, spreading malware, or hijacking control of a website.

Can you Prevent All Spam?

In essence, no. **Spam is an inescapable part of the internet.**

Because most spammers conceal their identity from recipients and internet service providers, it's difficult to hold them accountable for their actions. The low risks and costs also make spam an attractive option for less-scrupulous advertisers and marketers.

If you want to combat form spam, you're going to need to do everything in your power to **make it difficult for automated bots to fill out your forms**, but they're tricky and won't go down without a fight.

We'll go over some of the ways to make it difficult for bots to fill out forms. However, **it is not possible to prevent all spam all of the time**. But by using a combination of the methods below, we can prevent as much of it as possible.

Which Spam Prevention Methods are Available on Your Plan?

Method	Plan
ALTCHA	Team plan or higher
Google reCAPTCHA	Team plan or higher
Akismet	Essentials plan or higher, plus an Akismet subscription
Respondent Authentication	Team plan or higher
Honeypot Field	All plans
Human Test Field	All plans
Blocking Links with Validation	All plans
Keeping the form out of Google Search (noindex)	Essentials plan or higher

Google reCAPTCHA

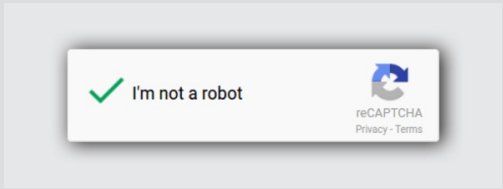
Google reCAPTCHA is a button that asks users to click to confirm they are not robots.

This is easier and less time-consuming for users than the original CAPTCHA (typing in those annoying wavy letters) and is still effective for blocking most spam submissions.

However, some spambots have cracked reCAPTCHA, so while this is a popular and effective method for preventing spam, it will not stop everything.

Google reCAPTCHA can be added to any form and has the added benefit of enforcing JavaScript in browsers. However, FormAssembly does not own reCAPTCHA (it is a Google Product), so no additional customization of reCAPTCHA is possible within FormAssembly.

More information on setting up reCAPTCHA is available here in our documentation.



ALTCHA

ALTCHA is a GDPR-compliant form abuse protection option that blocks automated form submissions without requiring respondents to solve a puzzle.

If ALTCHA validation fails, respondents will be unable to submit their form response.

For Team plans or higher, ALTCHA is enabled by default for forms created on or after October 20th, 2026. Forms created before that date do not have this default and have not been changed.

Note:

- You can use either reCAPTCHA or ALTCHA on a form, but not both at the same time.
- Akismet, which uses post-submission spam filtering, can be used in addition to ALTCHA

More information on setting up ALTCHA is available here in our documentation.

Honeypot Method

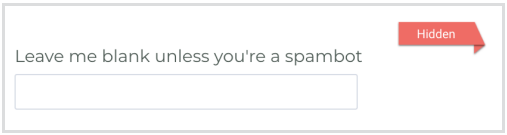
Honeypots catch spambots by presenting a hidden form field only they can see.

These hidden fields prevent submission of the form and/or flag the response if the field is filled out. Plus, they stay hidden from humans so they never see the fake form field.

You can replicate this method in your forms with a hidden field inside your FormAssembly form. You can either add regex validation to prevent form submission if the field is filled or use skip-if formulas to skip Salesforce connector steps if the field is not blank. Or both!

However, this method does **not** work on manual spammers, and some spambots have figured it out as well.

So like any other method, it can help, but it will not be infallible.

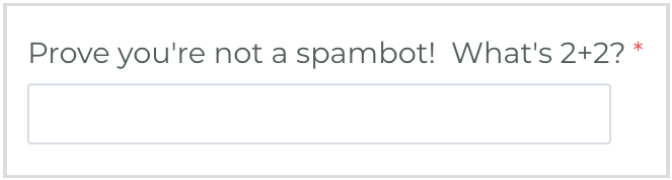


Human Test Fields

Spambots love filling out text input fields in your form. You can use this fact to your advantage when working to prevent spam!

Simply add a text field to your form that asks a very easy question. Something like, "What is 2+2?".

Then make the field required and add validation to prevent spam responses from being submitted. The validation could require numbers, numbers in a range, or could be as specific as using regex validation.

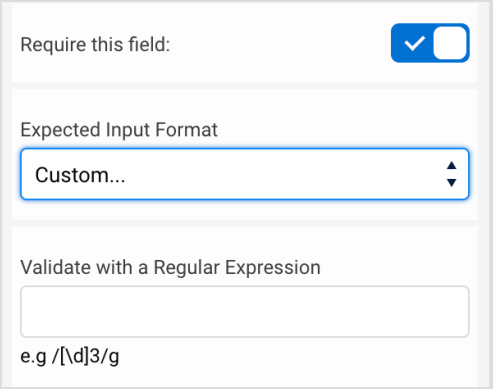


No Links in your Responses

If you are receiving spam submissions that contain links, try preventing those links with regex!

You can add custom validation that states that the text "http://" is not allowed to prevent a number of spam submissions.

You could do this for "https://" as well, but the majority of spam submissions tend to link to websites that are not secure.



Akismet

An Essentials plan or higher allows you to utilize Akismet for spam prevention.

When someone submits a response, Akismet will automatically check that response for spam. If the response gets flagged as spam, FormAssembly will delete the response or ask the respondent to correct it, depending on how you set it up.

Akismet is very powerful, **but will still never be perfect**.

In addition to an Essentials plan or higher, you also need an Akismet subscription.

More details on Akismet are available here in our documentation.

Respondent Authentication

A Team plan or higher allows you to require that respondents log in to fill out forms.

This method is **likely the only surefire way that there is to prevent spam** (provided your respondents don't misplace their credentials).

For example, if a customer has embedded their form inside a Salesforce Experience Cloud Site (formerly Salesforce Communities), then Salesforce Experience Cloud Authentication would require you to log in before filling out the form. **There's nothing quite as secure as authentication.**

More details on respondent authentication are available in our documentation:

- CAS Authentication
- LDAP Authentication
- SAML Authentication
- Salesforce Experience Cloud Authentication

Removing Forms from Google Indexing

Google indexes all web pages on the Internet that do not specify a "noindex" meta tag.

When Google visits your site or form, it detects changes to pages and links. When found, it updates the Google index, the backbone of Google Web Search and Custom Search.

Removing your site or form from Google's index can help prevent spambots from finding it in the first place. **You should do this before you publish, embed, and/or share your form.**

You can remove your site by adding this code in the <head>:

```
<meta name="robots" content="noindex" />
```

More details are here in our documentation.

Blocking IP Addresses

A common request our team receives is to block specific IP addresses from submitting form responses.

Unfortunately, this is **not** currently a FormAssembly feature; however, it is something our product team is looking into implementing in the future.

One major issue with blocking an IP address is that the spammer will usually use a VPN or a different IP to spam your form again. They often use an entire range of IP addresses and send a bulk amount of spam, then move to the next IP in the range and continue.

Blocking IP addresses can also cause problems in the future if a legitimate respondent tries to respond while using the IP address that was blocked.

Because of this, we recommend using the previously discussed methods in combination with each other to prevent spam instead.

In Conclusion

Spam is, unfortunately, going to happen.

We've been receiving spam emails, spam letters, spam texts, spam flyers, and more for decades, and webform spam is just the next evolution.

However, you can use one or more of the methods that we discussed today to help prevent spam!

In addition, **it's always important to keep an eye on your response data.**

If a spammer starts to slip through the cracks, you can look at the spam responses and alter the methods to scare off that particular spambot or spam human (and ask the Support team to help).

Spam is always evolving; we need to evolve right along with it!