How to Prevent Bots from Submitting Forms and Keep Your Email List Clean

by Amber Iven - Monday, June 08, 2020

https://www.searchbug.com/info/how-to-prevent-bots-from-submitting-forms/

If you have a business or a website, you use forms. Web forms are how you get contact information from your visitors and customers. The problem is, your customers are not the only ones filling out those forms.

Bots, short for “robots”, can be good or bad. They have the power to help or harm. When it comes to email marketing, the ones you really need to look out for are spambots.

At their worst, spambots fill out forms using legitimate information. However, without a human behind the submission, the lead is not only useless, but it could lead to a TCPA violation if it requires the user to provide a phone number.

Do you know how to prevent bots from submitting forms and entering your database? In this article, we cover the different types of bots, how to avoid the bad ones, and what to do if you can’t.

What Are Bots and How Do They Work?

bot *noun* a computer program designed to perform automatic repetitive tasks

bot *noun* a computer program designed to mimic the actions of a person

bot *noun* (slang) in video gaming, an insult used for a person who plays terribly as though incapable of sensible human decision-making skills

Good Bots

Considering the first two definitions above, bots don’t sound too bad, right? Right. Bots make the Internet go round. Good bots, that is.

Search engine bots, for example, generate frequently searched keywords and phrases in search engines such as Google. Companies like eBay and Amazon use **trader bots** to compete with product prices. These bots scour the web for available prices and deals to help a company offer a competitive rate.

Companies like Facebook use **feed fetcher bots** to identify trends and patterns among users to personalize what posts and ads are presented almost immediately. You might use feed fetcher bots if you have a subscription list. These bots can track subscribers’ click and view history to make recommendations based on users’ specific interests.

Chatbots communicate with your online users who have questions regarding processes, procedures, order

statuses, etc. These bots recognize keywords and respond using corresponding, pre-set templates. This saves you time and gives users immediate answers, therefore, strengthening your communication channel.

Backlink bots are responsible for checking your ability to compete with other articles online. These are great help for SEO specialists. With the ability to analyze where traffic comes from, appropriate adjustments can be made to websites and campaigns.

Monitoring bots check for issues with websites. They flag areas users have issues with so that the owner can make changes to improve the user experience.

Copyright bots track duplicated content. This is helpful if you want to make sure your content is original and to keep your own content safe from copiers.

These helpful bots save humans time by handling tedious tasks. It's easy to just have robots take care of them because they are repetitive and don’t require a lot of decision making. However, bots can be set up to do harmful tasks as well.

Bad Bots

The term “bot” has recently become a commonly heard insult among the gaming community. This is due largely in part to the 2017 release of the online game *Fortnite*.

Fortnite is a battle/survival game. New players are often assisted by bots, or robot players acting as other human players, in order to advance. To give new players a feel for the game, bots will join as easily defeatable opponents.

The point is that “bots”, in this case, cannot, should not, and do not perform better than actual human players. Bot players lack intuition, creativity, sensibility, etc. If someone calls you a bot, it most certainly is not a good thing….

Most bad bots are out to get personal customer information like names, phone numbers, email addresses, etc. **Spy bots** do this by tracking keystrokes to then access company and customer data. **Transfer bots** redirect traffic from a legitimate website to an unsecured page where users might unwittingly input personal information.

Impersonator bots mimic the actions of human users to get past website security and scour the site for info. **Spambots** gain access to user data by filling out lead forms, posting links in comments sections of websites, and spamming email inboxes once they locate the addresses.

Hackers use **file-sharing bots** and **zombie bots** to download malware onto a user’s computer and gain remote access without the user ever knowing.

Other bots are just plain annoying. **Scraper bots**, for example, steal content from other sites to use on fake sites that are set up for the sole purpose of selling ad space. **Click bots** visit sites and click on ads

which can skewer data and drain the advertising budget.

Despite the good that bots can do, the term overwhelmingly carries a negative connotation.

How Spambots Hurt Your Business

Spambots fill out forms with either unintelligible information or legitimate information. You might have a form on your website to allow users to subscribe to your email list or to access a lead magnet. The purpose is to generate leads.

If you don't verify the email addresses in your database before sending out a campaign, those invalid email address spambots use could hurt your sending reputation. To prevent your own emails from being marked as spam and to make sure you hit the inboxes of legitimate leads, you have to get rid of invalid addresses that find their way into your database (more on this below).

Of course, it's easy to recognize a spambot submission when the text is unintelligible or improperly formatted. However, there are instances where spambots use real information making it impossible to tell which contacts opted in and which were impersonated.

Not only do illegitimate leads waste your time, but they can also lead to TCPA violations if phone numbers are involved. Calling someone to market a service or product without his or her permission is unacceptable.

If a spambot uses a real name and phone number to fill out a form, and that information makes it into your database, and you call that number, you could be sued for breaking compliance with TCPA guidelines.

Fortunately, there are ways to block spambots from successfully submitting forms.

How to Prevent Bots from Submitting Forms

Again, bots do not have the decision-making capabilities of humans. Thank goodness! Because of this, there are *many* ways to block and weed out spambot submissions.

Identify Suspicious IP Addresses

You can set up a web application firewall (WAF), blacklist IP addresses that are suspicious, and limit the number of forms an IP address can submit in a given timeframe to find out which ones are spammy.

You can also use time analysis to determine which visitors are human users and which are bots. Typically, it takes a user a minute or two to fill out all of the fields on a form. Users also get distracted which keeps them on the page longer.

Bots complete forms immediately. Autofill can make this distinction a little more difficult, but when looking for bots, they're going to be the ones who spend 1-5 seconds on the page.

Honey Pot

A honey pot is another method of preventing spambot submissions. “Honey pot” is another name for “trap”. The “honey” is the irresistible lure.

In the data security world, honey pots are blank fields that bots cannot resist filling out to complete what they think is a form. What they are unable to recognize, though, is that only they can see these fields; they are invisible to human users. Therefore, filling in these fields clearly identifies them as bots.

CAPTCHA/reCAPTCHA

However, if you aren’t so tech-savvy, there are some simple ways to prevent bots from submitting forms and separate the bots from humans. You can add a CAPTCHA or reCAPTCHA to your forms. These require that users complete some action on the form before submitting to verify that they are human.

CAPTCHA has kind of gotten a bad rap for being too difficult for human users to complete. You’ve probably seen these before: the distorted alphanumeric characters that are almost impossible to distinguish even if you’ve got decent eyesight.

There is no doubt that CAPTCHAs have been responsible for deterring form submissions from genuinely interested users, especially those who might be disabled. The last thing you want to do is discourage your customers.

However, reCAPTCHA launched as a solution. The reCAPTCHA is that little checkbox that indicates “I am not a robot.”

Test Question

Another way to prevent bots from submitting forms is to add a question to your form. You might have seen these as well: 2 + 3 = ? Or a multiple choice question: I am a.) a unicorn b.) a robot c.) a potential customer.

Unfortunately, you could get those jokesters who will select “unicorn,” or humans who submit an incorrect answer due to an oversight. Nothing is perfect. You can use more than one strategy, though. A good combination would be a test question or reCAPTCHA and a double-opt-in form.

Double Opt-In

A double-opt in is exactly what it sounds like. The initial opt-in is the form submission. The second is through email. Have your forms set up to send a confirmation email to the address on the form. Users should then visit their inbox, open the confirmation email, and take some action to confirm their interest.

The hardest part of protecting your forms is making submission difficult for bots while keeping it simple enough for humans. Don’t use a complicated or confusing test question and don’t require too much action for a double opt-in. A button in the confirmation email can work just fine.

What Happens if Spambots Cannot be Prevented?

Bots evolve and even as new defense strategies arise, bots will likely figure out ways around them eventually. Even if you take the necessary steps to prevent spambot submissions, they can still make their way into your database.

But it's okay! As long as you properly maintain your email list, you can still identify bad email addresses before including them in your campaigns.

Searchbug's email verification API analyzes your email list and identifies invalid email addresses. Invalid email addresses can cause your emails to bounce which hurts your sending reputation and therefore your email marketing campaigns.

Invalid email addresses could be formatted incorrectly, they could be outdated and repurposed as spam traps, or they could just not exist. For these reasons, you always want to verify email addresses before adding them to your list.

Conclusion

Bots are smart. There's no doubt about that. But they're not as smart as people. There are plenty of things humans can do that robots cannot. This is great news when it comes to protecting your customer data from bots and distinguishing real users from impersonators. Now you know how to prevent bots from submitting forms and keep your email list clean.

There are tools available as well to help combat bad bots. Remember that there are good ones too that can help defend against them. If you use forms to collect customer data, be sure to check out Searchbug's email verification API to double-check the status of the addresses you collect. Your reputation is on the line.

Searchbug.com