

Deterring Spam Bots 🛡️

This article applies to:

What is a spam bot?

A Spam Bot is a computer program designed to assist in the sending of spam. It is often a submission to a database that is created autonomously from a third party. The more sophisticated the spam bot, the more difficult it is to identify. Typically, spam bots occur in two varieties:

1. The name of the contact is a string of numbers and letters, such as *58faf52f9e0f1*
2. The name of the contact doesn't match the email address, such as *Bob Smith* with an email address of *Alice@gmail.com*

Spam bots ultimately serve to increase spam complaints, damage sender reputation, and trigger Email Compliance flags which can shut down the ability to send email.

How do you identify and remove spam bots from the database?

A quick way to get rid of the *58faf52f9e0f1* spam bot is to navigate to **CRM > Contact search** and search for all contacts who have a first name beginning with *5*. You may need to spot check the results for any valid contacts who could be included in this list.

To remove **spam bots with valid names and email addresses**, do the following:

- To rule out contacts as spam bots, view contact records to see if they contain any identifying information that spam bots would not have, such as tags, opportunities, orders, or specific field data.
- If you have set up **double opt-in**, the spam bots will be among the group of unconfirmed email addresses.
- Use the **Email Status Search** to identify contacts who have never engaged. This often includes the spam bots and contacts who are not interested (both are good to remove for list hygiene).
- If the spam bots came from a web form that is no longer in use, use the **web form tracking report** to identify contacts who recently came through that form.
- **Send a broadcast email** to your contacts with a call-to-action to click a link or fill out a form. Return to the list at a later date and remove all contacts who have not completed the call-to-action.
- Follow the **List Hygiene** documentation to clean out unengaged, uninterested, and spam contacts.

If these methods aren't sufficient, you can manually sort through your contacts and remove invalid contacts, or wait until one of the above methods become feasible.

How do you prevent spam bots?

Spam bots scrape code from web forms, save it externally, and submit data to it via HTTP Post. We can anticipate how bots work and deter them using a few simple methods.

If the web form is already being targeted by Spam Bots:

- Make a copy of the form in Max Classic, delete the original, and replace it with the copy. This prevents the spam bot from resubmitting to the same form until it collects the new code from wherever the customer has posted it. This is a temporary fix. See Detering Spam Bots below.

Deterring Spam Bots:

- In Max Classic, use the [double opt-in](#) or [email confirmation](#) process for all new contacts. Remove all contacts who do not double opt-in after filling out a form.
- On active web forms, from the **Settings** tab, ensure the box to opt-out of **Google reCaptcha** is **unchecked**.
- On active web forms, include a question that only a human could answer such as “What is the third word of this sentence”. This would allow them to identify everyone who answers with “the” as a valid contact.
- On active web forms, set up a Spam Bot **Honeypot** (see below)

The Honeypot Method

The Honeypot Method leverages hidden fields in forms to catch spam bots. People can't see or enter data into hidden fields and spam bots often fill out every field on a form. Therefore hidden fields with data must come from spam bots. Caught ya!

To set up a Honeypot you need:

- An unused field (often a custom field)
- A web form
- A tag to identify spam submissions
- An action set

Steps:

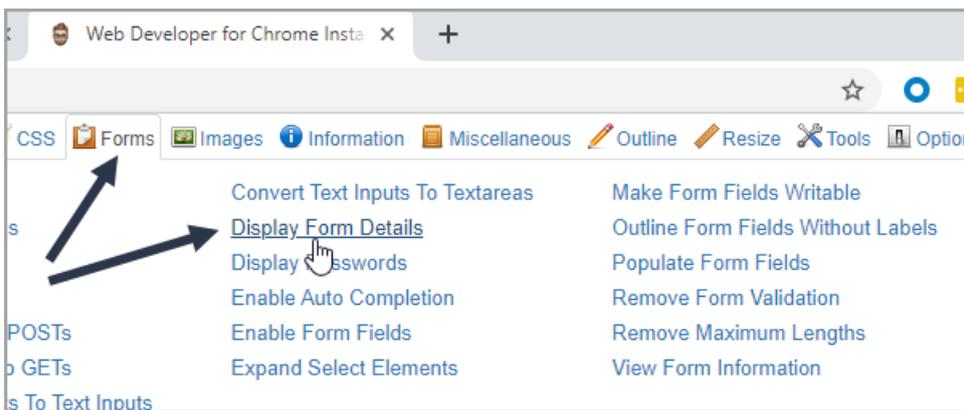
1. Create a new and unused text field that you will dedicate to identifying spam submissions. For this example, let's use "FillThisIn".
2. Navigate to **CRM > Settings > Action Sets** and set up a new action set.
 1. The action set should **apply a tag** that identifies the contact as spam (i.e. Customer -> Spam Contact).
 2. On the action to **apply the tag**, click the option to “Only run this action set when certain rules are met”.
3. Set up a rule with the following criteria:
 1. Rule is true when none of the following criteria are met.
 2. Based on data from the contact record, select the location of and the specific field you are using to identify spam contacts.
 3. When the contact's field **FillThisIn** is empty.
 4. Save the action set.
4. Navigate to the campaign builder.
 1. On the web form, add a **new hidden field** for the FillThisIn field.
 2. Immediately after the web form, add a sequence that begins with an action set and select the action set created above.
5. Spam Contacts will now be tagged as soon as they fill out the form. We can use that tag to end campaign processes, omit contacts from lists, and generate lists to be deleted.

Important: If the form that you modified is already published and hosted externally, the code will need to be updated for this to work.

Test a web form that uses honeypot / hidden fields

Next, test your web form with the hidden fields to verify that the honeypot method works.

1. First, install a dev tools browser extension. You will use this to view hidden fields.
 - Here is one option for a chrome extension/plugin that you can install: [LINK](#).
 - and an option for a Firefox extension/plugin: [LINK](#).
2. Access your web form from the Max Classic campaign and view it in a browser window.
3. Open the **Web Developer** extension from the upper right corner of the browser window and click the **Forms** tab.
4. Select **Display Form Details** to view all fields, including hidden fields.



5. Enter test data into the form fields including the hidden text field and click **Submit**.



6. Next, return to **Campaign Builder Reporting** to verify that the correct tags were applied. In this example, by entering data into the hidden field, this should result in identification as a spam bot.



7. Click on the contact name to view the contact record.

Campaign Contacts (Back to Campaign)

This report includes all existing Contacts who have entered the selected Sequence(s). It does not include contacts who have not entered the Sequence, which may cause a variance between the total number of records displayed in this report and the total number of records in the Campaign's Sequence.

Actions ▾ New Search Edit Criteria/Columns... Save... Print...

1-1 of 1 50 per page

Name	Campaign Name	Sequence Name	Status	Sequence Start Date
Amanda	Welcome	Spam Contact Sequence	Active	10/17/2019 12:13 PM

8. In the contact record, scroll down and click the Campaigns tab. View the Recent Campaign History to verify the results.

Recent Campaign History

	Removed from Sequence
Wait	
17 Oct 2019 12:13 PM	There is a timer at the end of the Sequence. Timers placed at the end of a Sequence will force the Contact to wait until the scheduled date.
	Welcome ► Spam Contact Sequence
	Spam Contact Tag Applied
17 Oct 2019 12:13 PM	Welcome