Spam Trap Information

Article Number

000087845

Information

Spam traps or honeypots as they are often referred to are used to identify and monitor spam email. Anti-spam organizations, Internet Service Providers (ISPs), and corporations use spam traps to lure spammers and block them.

A spam trap looks like a real email address, but it does not belong to a real person nor is it used for any legitimate form of communication. Its only purpose is to identify spammers and senders not utilizing proper list hygiene.

Spam traps are commonly used by inbox and blacklist providers to catch malicious senders, but quite often, legitimate senders with poor list hygiene or acquisition practices end up on the radar as well. Because of this, spam traps can easily lead to your IP address or even your domain to be blacklisted. Being blacklisted will hurt your sender reputation and could lead to further email deliverability being halted.

Types of Spam Traps

There are three types of Spam Traps to be aware of:
• Pristine
• Recycled
• Typo

Pristine Spam Traps

Pristine Spam Traps are email addresses created by Internet Service Providers (ISPs) and other organizations that are publicly accessible in forum posts or blog posts, so web scrapers can find and collect them.

• When spammers scrape websites to grow their contact list, the spam traps end up in their list.

• Pristine Spam Traps can also be found on purchased or rented lists.

• All spam traps negatively affect your sender reputation, but the Pristine Spam Trap is the most severe, and as a result is more likely to blacklist your IP address or your domain.

Recycled Spam Traps

Recycled Spam Traps are often domain registrations or email addresses that were once valid but have been reassigned for trapping spam.

When an email address that was used by a real person in the past is not used anymore, inbox providers will usually deactivate it after a certain time. These email addresses can then be reassigned for trapping spam.

• A couple of common examples are role addresses (sales@, info@, support@), email addresses of employees who are no longer with a company, and abandoned email addresses.

• When someone sends an email to these types of email addresses, the inbox provider returns a hard bounce. This is a signal to the sender to remove this email address from the list.

• When a hard bounce is recorded in Encompass, the “email is valid” indicator for that record is deselected. (An admin can manually update the valid checkbox, or it can be updated from an import.)

• After some time, the abandoned address will not return a hard bounce anymore, and it will become an active spam trap. It will now mark everyone sending an email to it as a misbehaving sender.

• Keeping bounced email addresses is how you end up with a dead address trap on your list. Make sure you are actively reviewing email marketing reporting, especially the bounces so you do not accidentally continue to email a dead address.

Typo Spam Traps

Emails with common typos, such as “gnail” instead of “gmail” or “yaho” instead of “yahoo” can also be used as spam traps.

• Typo spam traps are real email addresses which despite their domain misspelling, do not bounce. Internet Service Providers create addresses that contain intentional mistakes. They are mistakes people are likely to make when typing their address on a form. Then, they analyze the emails those addresses receive to detect phishing and other malicious practices.

Tips and Tricks to Avoid Spam Traps

The only way of finding and deleting spam traps is to take a close look at your list quality.
Since spam traps do not belong to real people, they do not behave like engaged constituents and will not have clicks or opens. If you actively manage your inactive recipients, you will likely get rid of your spam traps too.

• Review open rates and manage inactive and unengaged recipients. Remove addresses that have not engaged in the last year. These are either at risk of being converted into recycled spam traps or are truly disengaged constituents that are negatively affecting your open rates and engagement percentages.
The Engagement Metrics Dashboard area will also assist with your list hygiene and marketing efforts.

• The Engagement Metrics Dashboard will show engagement percentages based upon the time frame and class year filters.

• You can set the Date and Population by Class Year. Population is a multi-select option that allows you to pick multiple class years in the dropdown. There are also options for "Has Class Year Value" and “Missing Class Year Value”.

• By adjusting the date filter, you can analyze whether a constituent has engaged with email in the past year. If they have not, this would be an email address to remove from your list.

KB Product

Encompass

Last Modified Date

Mon Aug 26 09:57:28 GMT 2024

Title

Spam Trap Information