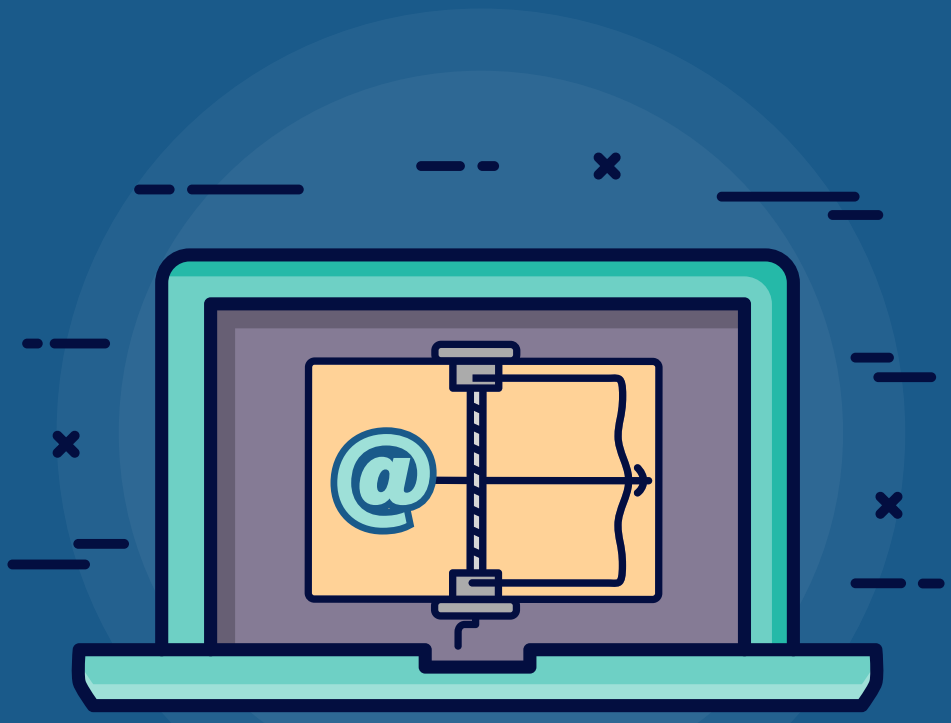
validity

ADVANCE YOUR
EMAIL MARKETING STRATEGY

The Truth about Spamtraps



BV BriteVerify

ABOUT

In an effort to help marketers better understand spamtraps, their associated risks, and the practices that should be followed to avoid them altogether, BriteVerify partnered with Travis Wetherbee, former postmaster at Hotmail and current anti-spam advocate and deliverability expert, to create this guide.

I: INTRODUCTION TO THE LOGIC BEHIND SPAMTRAPS

Spamtraps are one of the most widely used fraud management tools by large domestic and international Internet Service Providers (ISPs). ISPs use spamtraps to lure spam from, you guessed it, spammers.

Through the use of spamtraps ISPs can keep track of spammers and block the IPs of those sending email to spamtrap addresses. Since spamtrap addresses can't opt in to receive email, there is no way to acquire spamtraps in your database if you're following best practices.

"ISPs and Anti-Spam Services use spamtraps as a way to poison the lists of spammers who knowingly engage in email address harvesting."

Maintaining the use of spamtraps can be categorized many different ways in the anti-spam universe, but for the sake of this article it will be categorized as a form of list poisoning. ISPs and Anti-Spam Services use spamtraps as a way to poison the lists of spammers who knowingly engage in email address harvesting, which is illegal under CAN-SPAM.

II: DEFINITIONS OF THE TYPES OF SPAMTRAPS

Not all spamtraps are created equal, which means not all spamtraps carry the same negative impact to your sender reputation. There are two main types of spamtraps employed by ISPs and Anti-Spam services, and they are Pure Spamtraps and Recycled Spamtraps.

Pure spamtraps have the largest impact on your reputation and therefore your ability to deliver email to the major ISPs. The penalty is the greatest with pure spamtraps because they are created for the sole purpose of being a spamtrap. Thus, any email received at these addresses is considered spam by the ISP or anti-spam services. There is no legitimate reason for an email message to show up in the inbox of a pure spamtrap.

"There are two main types of spamtraps employed by ISPs and Anti-Spam services and they are Pure Spamtraps and Recycled Spamtraps."

The second type is known under several different names (dead addresses, dormant addresses, inactive addresses etc.), however, for the sake of this article we will refer to this type as Recycled Spamtraps.

Recycled spamtraps are email addresses that were once owned by customers of the ISP/Email provider (hence the name recycled) who have stopped using the accounts. After a pre-defined but undisclosed period of inactivity, the ISP will turn the account off and return hard bounce or SMTP errors to senders (for example, "550 – Unknown User").

This process is known as "gravestoning" accounts. After an email address has been gravestoned from 30 to 90 days, depending on the ISP, some addresses will be reactivated. Those addresses marked for reactivation then become recycled spamtraps. Any email delivered to these accounts is recorded as a spamtrap hit.

Recycled spamtraps have a lower penalty or effect on your IP & Domain reputation. Nonetheless, this is still recorded as a spamtrap hit. It is also good to note that not all ISPs have the same "gravestone" policies. It is always a good idea to check with the major ISPs that make up a larger share of your database.

Another type of spamtrap is known as Role Accounts or Function Email Accounts. These accounts include webmaster@, hostmaster@, sales@, support@, postmaster@, etc. The penalty for this type of trap hit can vary depending on the domain or ISP you are dealing with. More often than not these accounts hold a higher penalty with smaller B2B domains.

III: HOW DO SPAMTRAPS END UP IN YOUR DATABASE?

Spamtraps are by definition a secret, known only to the owner of the spamtrap address. Finding that you have one or more in your database can be very surprising and at the same time somewhat discouraging considering the penalties. Below are the most common ways spamtraps end up in marketers' databases.

The surest way to become infected with spamtraps is by purchasing email lists.

Purchased lists don't have "born on dates" accompanying each address, so there is no real way to tell how old purchased addresses are. Also, since 'email lists for sale' are aggregated without permission, they do not contain opt-in records. If you purchase lists, either frequently or infrequently, chances are you're currently sending to a large number of spamtraps.

"The surest way to become infected with spamtraps is by purchasing email lists."

The second most common method is sending email to old lists that have been dormant for years. This is a really good way to ring up quite a few spamtrap hits. Marketers often run lead generation campaigns to acquire new email addresses. When a database isn't properly managed, some of these addresses can be forgotten for long periods of time and then added into a new outreach campaign on a whim. The results can be catastrophic if no one has checked the age, source, and engagement history of the addresses being incorporated.

IV: THE RISK SPAMTRAPS DELIVER TO YOUR IP ADDRESSES

Spamtraps carry a very heavy penalty on your IP & Domain reputation. Of the two types, pure spamtraps have the most negative effect on your reputation. Hitting a pure spamtrap will almost always cause an immediate block on your IP address and, depending on the ISP, your 'from domain.' Not only is getting blocked both expensive and disruptive, but the process of re-establishing your reputation can be quite difficult.

"Your IP address or subnet of addresses can take upwards of 6 months to a year to fully recover from just one spamtrap hit."

In one specific example, there was a particular company that had built an excellent reputation. They followed the best practices by the book when building IP & Domain reputation. They hit a spamtrap at an Anti-Spam service and saw their inbox delivery to major ISPs go from 98% to 25% overnight. Every campaign was being monitored by an inbox monitoring service so the fallout from the spamtrap hit was immediately apparent.

Mitigating the after-effects of spamtrap hits can be a long and very frustrating process depending on the origin, type of spamtrap, and ISP/Anti-Spam service.

Your IP address or subnet of addresses can take upwards of 6 months to a year to fully recover from just one spam trap hit if you do exactly what's asked of you by the trap owner/ISP.

"They hit a spamtrap at an Anti-Spam service and saw their inbox delivery to major ISPs go from 98% to 25% overnight."

V: ARE YOUR DELIVERABILITY PROBLEMS RELATED TO SPAMTRAPS?

Based on experience with several top ESPs, it can honestly be said that a majority of delivery issues are not directly caused by spamtraps. The largest contributor to deliverability issues is the lack of adherence to basic email acquisition best practices (ex. don't buy lists).

However, if you suspect that your deliverability problems are caused by spamtraps, check the bounce logs for evidence of this. Also referred to as SMTP Failure logs or sending logs, these are the best first step to determining the source of your deliverability issues.

"The largest contributor to deliverability issues is the lack of adherence to most basic email acquisition best practices."

All ISPs who block or defer mail will send a rejection message or bounce message to the originating mail server (Non-Delivery Receipt/Report or Delivery Status Notification (DSN) for deferred messages). You can find detailed information as to the reason for non-delivery of the email messages in your campaigns.

If you've checked your bounce logs and come up with nothing, the next step is to check reputation monitoring services such as Senderscore.org. Also you can check the websites of popular anti-spam service providers, such as Cloudmark, Message Labs, Barracuda Network, and many others. Another option is to sign up for monitoring services.

VI: YOU HAVE SPAMTRAPS, NOW WHAT? (EXPENSIVE PARTIAL SOLUTIONS AHEAD!)

To restate the obvious, the easiest way to deal with spamtraps is to follow the best practices in email acquisition and avoid them altogether.

If, however, you discover that you have spamtraps, your IP address is blocked, and you are quickly looking for the next steps before your company's quarterly revenue is cut in half, the below information is for you.

Before you run out and spend a large portion of your marketing budget on services that claim they can make you spamtrap-free, remember this one important fact about spamtraps. They are only known to the owner of the spamtrap.

"Rooting out spamtraps is no walk in the park. It is costly, causes strained business relationships, and can have catastrophic implications for your brand's ability to deliver email to the inbox in the future."

First order of business is to identify the source of the breach and close it up before you do anything else. Spamtrap owners (ISPs and anti-spam services) won't talk to you unless you first tell them where you acquired the spamtrap, so be prepared. Word to the wise, don't ask the service provider for the address. It is your breach, and spamtrap owners have more important things to attend to, which includes preventing the spread of spam.

Providers simply will not tell you which spamtraps you hit, as setting up a new address takes valuable time and expensive resources they don't have. Any spamtrap removal service claiming their addresses are provided by ISPs are misrepresenting their services.

VI: YOU HAVE SPAMTRAPS, NOW WHAT?

(continued)

There are some very comprehensive sources that explain in great detail how to remove spamtraps from your database. You are free to read these but remember, the easiest and least costly way to have a spamtrap-free database is to never onboard traps in the first place. However, if you are infected, below are a few ways to help flush out a spamtrap.

1. Verify your list of emails before setting up further email marketing campaigns.

Email verification ensures that an email address actually exists without ever sending a message. It enables you to upload an email list and receive information about which of the addresses are valid and which are not, saving you the headache of sending out messages to emails of unknown status that could be spamtraps. BriteVerify, the leading real-time email verification solution, is capable of doing this in real time and uses three basic steps. Learn more about how it works here.

2. Reconfirm your entire database.

This is probably the most costly of the solutions because emails are worth money to your organization and reconfirming is sure to cut your subscriber base by 75% or more. Conversely, you can help mitigate this loss by only confirming certain segments of your database. This is a standard best practice, something that I recommend my clients do on a regular basis. Identifying certain segments can help reduce your fallout rate by 50% or more.

3. Did you have an unexpectedly large increase in subscribers recently?

This one is tricky because of the word "recently." However, when compared to the first option of reconfirming your entire database the ramification of misinterpreting the word "recently" probably seems like a walk in the park. Scrutinize any subscribers or large number of subscribers and look for anything out of the norm.

Rooting out spamtraps is no walk in the park. It is costly, causes strained business relationships and can have catastrophic implications for your brand's ability to deliver email to the inbox in the future.

VII: ALTERNATIVE WAYS TO LIMIT TRAP RISK

Limiting your risk of contracting spamtraps is fairly simple; follow the best practices for acquiring and sending email marketing messages. That said, business objectives don't bend around email marketing objectives. It is usually a one-way street, and best practices are typically the first casualty of any revenue-based meeting. With that in mind, here are the best options to limit your brand's risk of tripping a spamtrap.

1. Use Smarter Webforms.

For any email marketer, increasing the number of sign-ups is job number one. Improperly increasing list size can come at a cost, though. Make sure you're limiting the risk associated with data entry mistakes through your web forms. Web forms are the first defense in reducing the risk of spamtraps. While you can hire a webpage designer/coder to code in all of the ISPs and B2B domains syntax rules and rules for dead domains, this can be costly when compared to using a service like BriteVerify. Email marketers around the world can attest to the benefits of this option when working on improving email hygiene.

2. Use Suppression Lists.

Create and maintain a suppression list that is portable and MD5 compliant. That way if you choose to move ESPs or take your email program in-house, you can bring your suppression file with you.

If you don't have the time or resources to maintain one, use a service. Suppression files usually consist of dead domains, role accounts, wireless domains, government entities etc. You can also include any subscribers that complain or hit the junk button at their respective ISPs. This would involve setting up feedback loops; however, it is a good idea to keep those addresses in a suppression file.

3. Employ Soft Bounce Management.

Create a soft bounce threshold that works in line with your marketing schedule, and stick with it. Soft bounces can occur if the recipient's mailbox is full. Mailbox full is an early indicator that the recipients address may be close to becoming gravestoned by that ISP. You can avoid hitting a recycled spamtrap if you set a threshold for soft bounces to be removed. On average if you send 5 emails to a subscriber in any given 30-day period, then your soft bounce threshold should be 5 soft bounces in 30 days. Once you set this threshold, the MTA will treat the 5th soft bounce in a 30-day period as if it were a hard bounce. This will save your reputation by avoiding hard bounces and possibly avoiding a recycled spamtrap in the future.

VIII: CLOSING

Hitting a spamtrap isn't the end of the world. However, if you hit one, there is a lot of work that needs to be done. If you follow best practices then you have done most of the work already. If not, start by working with an experienced Email Deliverability Consultant.

Next, contact BriteVerify to identify invalid emails, hard bounces, and role accounts to cleanse the quality of your email lists before you end up marketing to spamtraps. You may also consider working with an inbox monitoring service in order to easily monitor your progress. Doing so will help you track how the changes you implement affect deliverability.

Going it alone is definitely possible, but it will ultimately end up causing delays in having your IP removed from the blacklist.

Your overall goal is to return your company's deliverability rate and productivity levels back to normal as quickly as possible because, as we all know, deliverability affects the bottom line.

Good luck and best practices!

About Validity

Validity is a leading global provider of data integrity and compliance offerings that thousands of organizations worldwide rely on to trust their data. With highly-valued products including Trust Assessments, DemandTools, DupeBlocker, PeopleImport, and BriteVerify, Validity is empowering organizations worldwide to make better decisions that drive more leads, close more deals, and confidently plan for continued growth.

We want to help your efforts. **Get in touch** with our team of data quality consultants to learn how some of the most effective marketing teams in the world trust us to lend validity to their data.

Contact us today!

US: 1-800-961-8205 | UK: +44 (0) 118 403 2020
sales@validity.com

validity.com
briteverify.com

TA TrustAssessments
PI PeopleImport
DT DemandTools
DB DupeBlocker
BV BriteVerify

validity