The Truth about SPAM Traps

By: Email on Acid

Email on Acid

Table of Contents

Chapter 1: What are SPAM traps?

It's a lot easier than you'd think for an innocent, legitimate email to be mistaken as SPAM. **22% of opt-in email messages never make it to the inbox** according to Return Path's *Email Intelligence Report: Placement Benchmarks 2013*. The most chilling part of this stat? It is increasing year by year. Last year's count of "Missing/Blocked" emails was only 18%.

One major way to get tangled up in SPAM filters is sending to a "honeypot email", aka a SPAM trap. You might get lucky and not get hurt too badly if you hit a spam trap, but sometimes the consequences can be deadly. In an effort to help people better understand SPAM traps, their associated risks, and the practices that should be followed to avoid them altogether, BriteVerify Email Verification partnered with Travis Wetherbee, former postmaster at Hotmail and current anti-SPAM advocate and deliverability expert. We at Email on Acid are excited to host this whitepaper on SPAM traps.

The logic behind SPAM traps

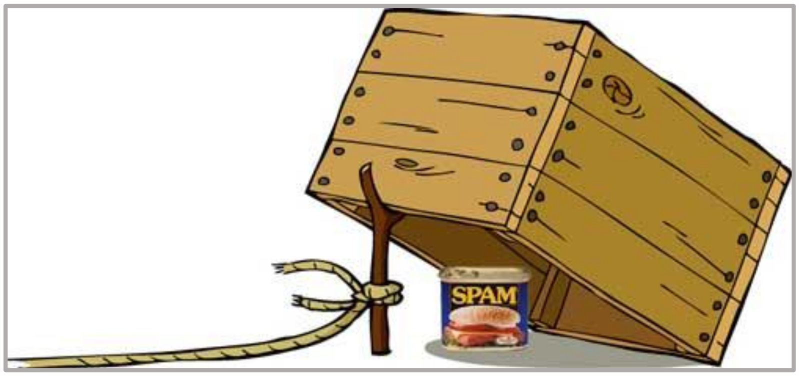
SPAM traps, or "honey pots" are one of the most widely used fraud management tools by large domestic and international Internet Service Providers (ISPs). ISPs use SPAM traps to lure SPAM from, you guessed it, spammers. Through the use of SPAM traps ISPs can keep track of spammers and block the IPs of those sending email to SPAM trap addresses. Since SPAM trap addresses can't opt-in to receive email there is no way to acquire SPAM traps in your database if you're following best practices.

Maintaining the use of SPAM traps 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 SPAM traps as a way to poison the lists of spammers who knowingly engage in email address harvesting, which is illegal under CAN-SPAM.

Definitions of the types of SPAM traps

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

Pure SPAM traps 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 SPAM traps because they are created for the sole purpose of being a SPAM trap. Therefore, 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 SPAM trap.



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 SPAM traps**. Recycled SPAM traps are email addresses that were once owned by customers of the ISP/Email provider (hence the name recycled) that 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 SPAM traps. Any email delivered to these accounts is recorded as a SPAM trap hit.

Recycled SPAM traps have a lower penalty or effect on your IP & Domain reputation. Nonetheless, this is still recorded as a SPAM trap 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 SPAM trap 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.

Chapter 2: How do SPAM traps end up in your database?

SPAM traps are by definition a secret, known only to the owner of the SPAM trap 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 SPAM traps end up in marketers' databases.

The surest way to become infected with SPAM traps 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 SPAM traps.

The second most common method is **sending email to old lists** that have been dormant for years. This is a real good way to ring up quite a few SPAM trap hits. For example, I had a client that ran contests as a way to acquire email addresses. After the contests these lists would sometimes be forgotten for years. In this case, during a revenue meeting someone remembered that an old contest list of 200,000 addresses hadn't been contacted and were therefore added to the production list. The result was quite literally catastrophic.

Other common ways SPAM traps make their way into legitimate opt-in lists is by way of common role account hits or typos that lead to dead domains. **Dead domains** are quite obviously domains that are no longer in service. For example, some ISPs go out of business, merge with another service, or are purchased outright. In this scenario the ISP can either gravestone all addresses or migrate them over to the new service. Considering that most Anti-SPAM services don't have the infrastructure to maintain webmail services, this presents them with an opportunity to purchase the gravestoned addresses and transfer them into SPAM traps.

The risk SPAM traps deliver to your IP addresses

SPAM traps carry a very heavy penalty on your IP & Domain reputation. Of the two types, **pure SPAM traps have the most negative effect on your reputation.** Hitting a pure SPAM trap 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 reestablishing your reputation can be quite difficult. I recently worked with a client who built an excellent reputation. They followed the best practices by the book when building IP & Domain reputation. They hit a SPAM trap 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 SPAM trap hit was immediately apparent.

Mitigating the after-effects of SPAM trap hits can be a long and very frustrating process depending on the origin, type of SPAM trap, 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.

Are your deliverability problems related to SPAM traps?

In my experience with several top ESP's and with Windows Live Hotmail I can honestly say that a majority of delivery issues are not directly caused by SPAM traps. **The largest contributor to deliverability issues is the lack of adherence to the most basic email acquisition best practices** (ex. don't buy lists).

However, if you suspect that your deliverability problems are caused by SPAM traps 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. All ISPs who block or defer mail will send a rejection message or bounce message to the originating mail server. Also known as a Non Delivery Receipt/Report or Delivery Status Notification (DSN) for deferred messages, these have detailed information as to the reason for non-delivery of the email message.

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, BrightMail, Message Labs, Barracuda Network, and many others. Another option is to sign up for monitoring services provided by Return Path or DNSstuff.com which provides a SPAM Database Lookup tool.

Chapter 3: How can you limit trap risk?

Limiting your risk of contracting SPAM traps is fairly simple; follow the best practices for acquiring and sending email marketing messages. That said, I fully understand that 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 I give you the best bet options to limit your brand's risk of tripping a SPAM trap.

1) Use Smarter Webforms: For any email marketer, increasing the number of sign-ups is job number one. Improperly increasing list size however, can come at a cost. 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 SPAM traps. 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.com. I am a huge fan of this service and my clients can attest to the fact that this is one of my recommendations when working on improving email hygiene.

2) 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, again 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 which I will cover in another article; however it is a good idea to keep those addresses in a suppression file.

3) 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 recipients' 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 SPAM trap 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 SPAM trap in the future.

Chapter 4: You have SPAM traps, now what?

To restate the obvious, the easiest way to deal with SPAM traps is to follow best practices in email acquisition and avoid them altogether. If, however, you discover that you have SPAM traps, 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 SPAM trap-free **remember this one important fact about SPAM traps: they are only known to the owner of the SPAM trap**.

First order of business is to **identify the source of the breach** and close it up before you do anything else. SPAM trap owners (ISPs and Anti-SPAM services) won't talk to you unless you first tell them where you acquired the SPAM trap, so be prepared. Word to the wise, don't ask the service provider for the address. It is your breach and SPAM trap owners have more important things to attend to which includes preventing the spread of SPAM. Providers simply will not tell you which SPAM traps you hit as setting up a new address takes valuable time and expensive resources they don't have. Any SPAM trap removal service claiming their addresses are provided by ISPs are misrepresenting their services.

There are some very comprehensive sources that explain in great detail how to remove SPAM traps from your database. You are free to read these but remember, the easiest and least costly way to have a SPAM trap-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 SPAM trap.

1) 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.

2) Did you recently purchase a list? If so, throw it out not matter what the cost was. Purchased lists are again, the single largest cause of SPAM trap hits by legitimate email marketers. Throw it out and move on.

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.

As I have stated here and experienced along with my clients, rooting out SPAM traps 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.

Hitting a SPAM trap 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 you've already done most of the work. If not, start by working with an experienced Email Deliverability Consultant. Next, contact an email verification service like BriteVerify.com to identify hard bounces and role accounts before they are repurposed as SPAM traps. You may also consider working with an inbox monitoring service like Return Path in order to easily monitor your progress. Doing so will help you track how the changes you implement affect deliverability. Going at it alone is definitely possible, but it will ultimately end up causing delays in having your IP removed from the blacklist.

Ultimately your goal is to return your company’s deliverability rate back to normal and productive levels because, as we all know, deliverability affects the bottom line. Good luck and best practices!

This information was shared with Email on Acid, courtesy of Travis Weartherbee and BriteVerify Email Verification Services

Travis Wetherbee is an anti-SPAM advocate and email deliverability consultant. Travis has 10 years of email experience, starting as a member of the Postmaster group at Hotmail and including years of deliverability services at Strongmail Systems and WhatCounts. Travis' consultancy focuses on Email Deliverability, Marketing, Messaging Security, and Anti-SPAM Services.

BriteVerify.com is a global leader in email verification services. Their mission is to deliver tools that help data owners follow best practices in email acquisition and protect themselves from the email evil-doers. Visit BriteVerify.com today to learn more.