SPAM TRAPS AND HONEY POTS: DEFINITION, PREVENTION, AND ELIMINATION

GreenArrow
Fast, Reliable Email Delivery

EMAIL DELIVERABILITY SPAM TRAPS AND HONEY POTS: DEFINITION, PREVENTION, AND ELIMINATION

A spam trap is a special email address designed to receive spam and "trap" mailers that spam or otherwise use questionable mailing practices. Sending to a spam trap address can quickly damage your deliverability reputation and cause you to be blocked or, worse, get you blacklisted with Spamhaus or other blacklists. Fortunately, they can be avoided if you understand how they work, and adhere to best mailing practices.

This article discusses different kinds of spam traps, how to prevent sending to spam traps, and what to do if you discover spam traps on your list.

Different Kinds of Spam Traps

There are many different kinds of spam traps. Understanding the different kinds will help you understand how to avoid sending to them.

1. Reactivated Address Spam Traps

This is an email address that previously was a valid working address which became an invalid address, but was then reactivated and turned into a spam trap by the ISP.

For example, if one of your subscribers stops logging in to check their email, eventually the ISP (for example, Yahoo or Hotmail) will disable the email address. When the address is disabled, any email sent to this address will 'hardbounce.' ISPs re-enable a small percentage of these disabled email addresses and turn them into spam traps.

Reputable spam trap operators ensure that the email address was dead and returning hard bounces for a reasonable amount of time before turning the address into a spam trap (9 months to a

year or more, it will vary and nobody knows for sure). Mailers following the best practices below will have already noticed these hard bounces and removed this email address from their list.

2. Reactivated Domain Spam Traps

This is the close cousin to Reactivated Address Spam traps.

These are created when a domain name with many email addresses lapses (perhaps it belonged to a company that went out of business) and is then purchased by a company that wants spam traps. All addresses at this domain suddenly become spam traps.

Reputable spam trap operators ensure that the domain name was dead and returning hard bounces for a reasonable amount of time before turning the addresses into spam traps.

3. Classic Spam Traps (also called Honey Pots)

These are addresses that are designed from the beginning to be spam traps and whose sole purpose is to identify mailers that do not build their own email lists organically. Classic spam traps are created and placed on websites or forums or other publicly available locations to be "harvested" or "scraped." They have never been used to sign up for email, or used as a contact or ever been associated with an email account.

If sent to, the receiving ISP or mail system immediately knows that the address was part of a purchased or shared list that was harvested or scraped from a website—in other words, definitely obtained somehow other than organically via an opt-in sign up.

Sending to one of these addresses is far worse than the reactivated address or domain spam traps listed above. In fact it is entirely possible –and even likely –that sending to just one of these addresses could get you blacklisted or blocked.

4. Typo Domain Spam Traps & Typo Address Spam Traps

All of the typos of common email domain names have been purchased by spam trap companies. For example, "yahoo.com" could be a spam trap domain (but is not).

Typo address spam traps are addresses with a typo in the non-domain portion of the email address.

These kinds of spam traps get on lists when a person legitimately attempts to subscribe but accidentally typos their email address. Sending to a typo domain or address spam trap does not prove that your mail is spam, but it does show spam trap companies that you don't use a Confirmed Opt-In process and allows them to see your email. If your email looks spammy, this can be enough to get you blocked.

5. Investigative Traps

Sometimes when an employee of a spam trap operator or blacklist is investigating a potential spammer they will create a special one-time investigative email address and use it only to sign up at this potential spammer's site. If this company shares the email address with other companies and they mail to it, this address effectively becomes a spam trap – any mail received at this address from these other companies is spam, and evidence of email address sharing or purchasing.

How to Avoid Sending to Spam Traps

Basic email sending best practices will help you avoid sending to spam traps.

First, the basics of only sending permission-based email:

- NEVER purchase lists. Purchased lists are often full of Reactivated Address Spam Traps because the list maintainer is never sending to the addresses and doing bounce processing. They may also contain Classic Spam Traps and Investigative Traps depending on how the list was created.
- NEVER scrape the web or forums for email addresses. (Note: this is a CAN-SPAM violation in the United States.) This will pick up many Classic Spam Traps.
- NEVER "trade" email addresses with another company. This is basically a purchased list.

However, senders who only send to people who specifically signed up can sometimes still have trouble with spam traps. Here is some advice for avoiding Recycled Address and Domain Spam Traps:

- Ensure that your software or ESP is using proper bounce-processing practices and hard-bounces are removed from your list. If you don't have proper bounce-processing you will eventually hit Reactivated Address or Domain Spam Traps.

- Make sure you email every address in your database at least every 6 months. For example, send a Christmas card email to subscribers who you have not mailed otherwise. If you don't email an address for an extended period of time, you run the risk that it will turn into a Reactivated Address or Domain Spam Trap without your ever knowing. Consider it risky to send to an email address that you haven't mailed in over 18 months. It's better if you never send mail to an address over a year old.

- Review your internal processes to make sure there is no way that email addresses can "sit" in some database for a long period of time and then be mailed to, or be sent to by one system even though a different system received a hard-bounce. This is more important for larger organizations or enterprises that may have multiple email sending systems.

- NEVER send to or reactivate bounced subscribers. A major ESP reports that this is the most common reason their customers get on blacklists. Your list of bounced subscriber is likely FULL of Recycled Address and Domain Spam Traps. Just don't do it!

- Avoid address book importing. This is where your user gives you API access to their address book then you send an invite email to everyone in the address book. Think of all of the old data that exists in your own address book. This is a great way to hit Recycled Address and Domain Spam Traps.

Additionally be careful of the following:

- Be very careful of "incentivizing" subscription. For example, if you are a retailer and you offer a coupon at checkout for subscribing to your email newsletter, you will get plenty of email addresses that people will just make up to get the free coupon. Some of these addresses that people make up will be Spam Traps. Monitor the invalid user rates of your different email collection programs. If one program generates a high percentage of invalid email addresses, this is evidence of a problem in the address collection, and you may also be collecting spam traps.

- Remove non-responding addresses. It is a general best practice that email addresses who don't click or open for a long period of time should be removed. Spam traps should not

click on links in mail or trigger an email open, so following this advice will also remove spam traps.

- Ensure that your email does not look like non-relational unsolicited email. Even if people requested mail from you, don't send just a "flyer" without your logo or an email that is all one image. If your email messages look like spam and you send to a Typo Address or Domain Spam Trap, you are much more likely to get blacklisted.

Spam Traps Are Not the Problem, But a Symptom

If you have a spam trap on your list, it's critical to figure out how it got there. Something about your list practices allowed you to send to the spam trap—that's the real problem. Removing the spam trap would just be treating the symptom. Evaluating your list practices will get to the root of the problem and ensure you don't get any more spam traps on your list.

What To Do If You Have a Spam Trap on Your List

This below advice assumes you're sending permission-based email that was requested by your subscribers. If not, immediately stop sending to any purchased lists, traded email addresses, or scraped email addresses. You've been caught.

For those sending permission-based email: First of all, relax. It's a horrible feeling to have your email blocked, and especially more horrible to be told that you have a "Spam Trap" on your list if you are trying to follow best practices.

Recycled Address and Domain Spam Traps can get on a list due to an un-intentional failure to follow one of the best practices above. These best practices have evolved over time with the introduction of Recycled Address spam traps, so not everyone is aware of them.

Make sure you correspond respectfully with the spam trap operator:

- Be calm, clear, and respectful in your communication. If you need to vent, vent to someone else.

- Do not ask for the spam trap address so you can "remove" it. The spam trap operator will not (and often cannot) give you the spam trap address. Remember that sending to the spam trap is not the problem, but the symptom.

- Work with the spam trap operator to understand what went wrong and fix the root problem.

If you received an email from a spam trap operator, reply and let them know that you are permission based, briefly let them know where/how you collect addresses, and let them know you're checking out your practices to see if anything went wrong on your end, and ask if they have any info they can help with.

Then, evaluate your email program against the above best practices. This will often reveal the problem. If you find a problem, fix it, and then let the spam trap operator know what you changed. If you can't find anything wrong, share the details of what you've checked and see if they can offer you any guidance.

If nothing in the above appears to be the problem, there are more advanced techniques for identifying the problem that are beyond the scope of this article. One catch-all technique is to prune addresses that have not clicked or opened recently from your list, since spam traps should not open or click mail. This is a good best practice anyway, and can improve email delivery across the board.

You may want to enlist the help of an experienced email deliverability company, such as ours. We have years of experience doing this kind of work, so we know what to look for and would be glad to help.