Help! I hit a spamtrap!

What is a spamtrap and what is it good for?

A spamtrap is an email address which is not used by an actual person. Its purpose is to find email senders who send unsolicited emails. Spamtraps are usually used to improve spam filters by blocking sending IP addresses which send emails to a spamtrap. There are two different types of spamtraps:

- pristine spamtrap:

  The email address of a pristine spamtrap was never before used by anyone. It was solely created for the purpose of "catching" spam. Any email which is sent to a pristine spamtrap cannot have been solicited. The only exception could be that someone misspelled their own email address while signing up to a newsletter and accidentally typed the exact address of a spamtrap. To prevent this, most spamtrap operators don't use "typo" domains for their traps. (e.g. outlok.com)

- recycled spamtrap:

  Contrary to pristine spamtraps, the address of a recycled spamtrap was owned by an actual person before. This could be the complete domain of a company who went out of business or individual email addresses of freemail users who deleted their account and released the address. Depending on the mailbox provider, an email address released by a former customer responds with a hard bounce for at least 6 to 12 months before it is turned into a spamtrap.

Who operates spamtraps?

Basically anybody can operate a spamtrap. Due to the purpose of a spamtrap, however, they are normally operated by postmasters from bigger companies or freemail providers to improve their spam filters and, of course, by blacklist providers. Many blacklists rely on spamtraps. If multiple emails (in rare cases, even only one email) from the same IP hit a spamtrap, the IP will be added to the blacklist.

How to avoid spamtraps?

Spamtraps in your email lists are a bad thing. How do they even get in there in the first place? The main reasons are:

- email address harvester: Some spamtrap operators publish the spamtrap addresses on simple websites, forums, etc. to expose them to harvester software. While the usage itself of these programs might be legal, using the collected addresses is, at least in the European Union, illegal and will most likely contain spamtrap addresses. Never use this kind of software!
- bought lists: While some list vendors work legally and clean, others don't. If you want to be safe, never buy lists.
- insufficient list management: This is especially a problem with recycled spamtraps. Do not send to old addresses you haven't used in years. Clean up inactive addresses immediately and take list management seriously.
- list poisoning: This can be either by accident (e.g. a typo in the registration process) or on purpose by someone who wants to harm you by entering known spamtrap addresses into your list. The easy fix for this problem is to use double opt-in when collecting addresses.

I hit a spamtrap anyway. What can I do now?

First of all, try to figure out what went wrong. If you never had any issues and, from one day to the next, you hit a spamtrap or even multiple spamtraps, have a look at the history of the list. Did someone recently import addresses? Did you send emails to a list which was inactive for a while? If nothing seems suspicious, cluster the list in smaller groups and try to find the part containing a spamtrap address. If in doubt, it is better to remove an address or even the whole cluster from the list. Hitting the same spamtrap again is worse than losing a few subscribers.

Conclusion

The best and easiest way to handle spamtrap hits is to never ever hit a spamtrap in the first place. This seems ironic, but prevention is the best method to not run into issues and protect your good reputation.

A few quite simple steps will help you to massively reduce the risk of hitting a spamtrap:

- Do not use harvested or bought email addresses
- Diligently maintain your lists. Remove bounces and inactive subscribers
- Use double opt-in
- Check email addresses in the opt-in process and when importing for irregularities like
  - non-existent domains
  - invalid/missing MX record
  - role account addresses like info@, spam@, root@, webmaster@,…
  - etc.

Authors: The technical team of the Certified Senders Alliance