What You Need to Know about SPAM TRAPS

By: G-Lock Software

Table of Contents

Introduction

It's easier than you think for a legitimate email to be flagged as SPAM. According to Return Path's Email Intelligence Report for 2013, 22% of opt-in email messages never reach the Inbox and this number is increasing year by year.

One of the sure ways to get the message treated as SPAM is sending it to a "honeypot" or SPAM trap email address. You might be lucky and not spoil your sender reputation too much if you hit a SPAM trap address, but often times the consequences are serious.

The bad thing is that you may not even know that there are SPAM traps on your list. There is no email verifier software or service that could determine SPAM trap email addresses because **these addresses are always reported as "valid"**. And they are actually valid, but used to identify spammers.

The good news is that you can take measures to minimize the risk of getting SPAM traps on your list and to avoid sending email messages to such addresses to maintain your good reputation with ISPs (Internet service providers).

In an effort to help you better understand SPAM traps, associated risks, and the best practices that you should follow to avoid SPAM traps on your mailing list, we at G-Lock Software are excited to give you this PDF report.

What are SPAM Traps?

SPAM traps are email addresses that are used not for communication, but for identifying senders with poor quality email lists and punish spammers and unscrupulous marketers. With the use of SPAM traps ISPs can track spammers and block their IPs.

Since people cannot use SPAM trap addresses to subscribe to someone's emails, there is no way to get SPAM traps on your list if you are following best email marketing practices.

There are many SPAM traps out there, and new ones are set up each day. SPAM traps are managed by large ISPs, anti-spam organizations like Spamhaus, and security companies like TrendMicro. Even corporate email servers and particular domains may be set up for the purpose of fishing for SPAM traps.

ISPs and anti-spam services use SPAM trap addresses as a way to create the lists of senders known to engage in email address harvesting or buying, which is illegal under CAN-SPAM law.

SPAM trap email addresses are typically published in a location hidden from view so that an automated email harvester used by spammers can find the email address, but nobody would be encouraged to send messages to that email address for any legitimate purpose.

Types of SPAM Traps

Not all SPAM traps have the same origin, which means not all SPAM traps carry the same negative impact to your sender reputation. There are two main types of SPAM traps used by ISPs and anti-spam services:

True SPAM traps — these email addresses are created solely to capture spammers. These addresses never subscribe to receive emails. Therefore, any email received at such addresses is considered SPAM by the ISP or anti-spam services. There is no legitimate reason for a message to reach the inbox of a true SPAM trap email.

With that said, sending to a true SPAM trap has the worst impact on your reputation and your ability to deliver messages to the major ISPs. The negative consequences are the greatest because a true SPAM trap is created for the sole purpose of being a SPAM trap.

Recycled email addresses — these are email addresses that were used by customers of the ISP/email provider and then were abandoned. After a pre-defined but undisclosed period of inactivity, the ISP will disable the account and return a hard bounce error 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, the ISP will reactivate (recycle) the address, convert it to a SPAM trap and allow email to be received by the email address. Any email delivered to such an address is recorded as a SPAM trap hit.

Recycled SPAM traps frequently catch legitimate senders with poor list hygiene and bad list building practices. Sending to a recycled SPAM trap address has a lower penalty or effect on your IP.

What about role accounts?

A role address is not a spam trap. It is generally foolish for most to send to these email addresses because they are not associated with a particular person, but rather with a company, department, position or group. Role accounts begin with admin@, webmaster@, hostmaster@, sales@, support@, postmaster@, etc. and are not generally intended for personal use.

How SPAM Traps Get into Your List

SPAM traps are not disclosed by ISPs and anti-spam organizations so one day you can be very surprised and upset (considering the penalties) finding that your emails are blocked because of SPAM trap addresses in your database. Below are the most common ways email marketers can acquire SPAM traps on their mailing lists:

1. By purchasing and/or harvesting email lists. Purchasing an email list or using an email harvester tool to collect email addresses on the Internet is the quickest yet the most dangerous way to build the contact database.

Firstly, such lists are aggregated without permission and do not contain opt-in records. Secondly, when you buy or harvest email addresses, you cannot tell how old the email address is and if it's still valid or not. So, if you purchased or harvested email addresses, it can happen that you are currently sending to a large number of SPAM traps.

2. By using an old list that has not been emailed for years. If you do not contact your prospects during a year or more, you cannot be sure that all those emails are still active and are being used by people to receive emails. There is a good chance that some of those addresses were abandoned by users and turned into SPAM traps by the ISP or anti-spam organization. So, sending to an old list of addresses is a real way to raise a few SPAM trap hits.

3. By not using a confirmed opt-in method. SPAM traps can creep in to your contact database if you use a single opt-in process on your web site. This is when the

email address is added to the database immediately without the user having to confirm the subscription. The user can simply enter his email address with a typo and the mistyped email address can turn to be a SPAM trap.

Sometimes users do not want to subscribe with their real email and use a fake email address to subscribe on online forms and shopping carts that do not require subscription confirmation. Fake email addresses may be used as SPAM traps as well.

4. By making a typo in the email address. Often times marketers collect email addresses offline (at presentations, festivals, shows, etc.) by writing the user's email address on a sheet of paper or business card. In such situations, the human mistake can take place. The marketer can enter the email address with a typo into his online database.

For example, the customer's email address "john@domain.com" may be mistyped as "jonh@domain.com" by accident. Unfortunately, "jonh@domain.com" is a SPAM trap and reports the sender's email as spam since, technically, it did not subscribe.

5. By not eliminating role accounts. As we told above, role accounts are not associated with a person, but denote the entire organization, department, or group of people in the organization, so it's supposed that nobody will subscribe to get email newsletters using a role email address. Since the email is not subscribed, every message sent to that address may be treated as spam.

Deliverability Problems Caused by SPAM Traps

If you send an email to a SPAM trap address, this is the indication that, at worst, you are a spammer and, at best, you are a lazy or unscrupulous sender with a list of poor quality. SPAM trap owners will take the measures accordingly.

The penalties for hitting a SPAM trap account depend on: the type of the SPAM trap you hit, how many times you hit it, and how the SPAM trap manager handles things at their end. Of the three types, true SPAM traps represent the greatest danger for your reputation.

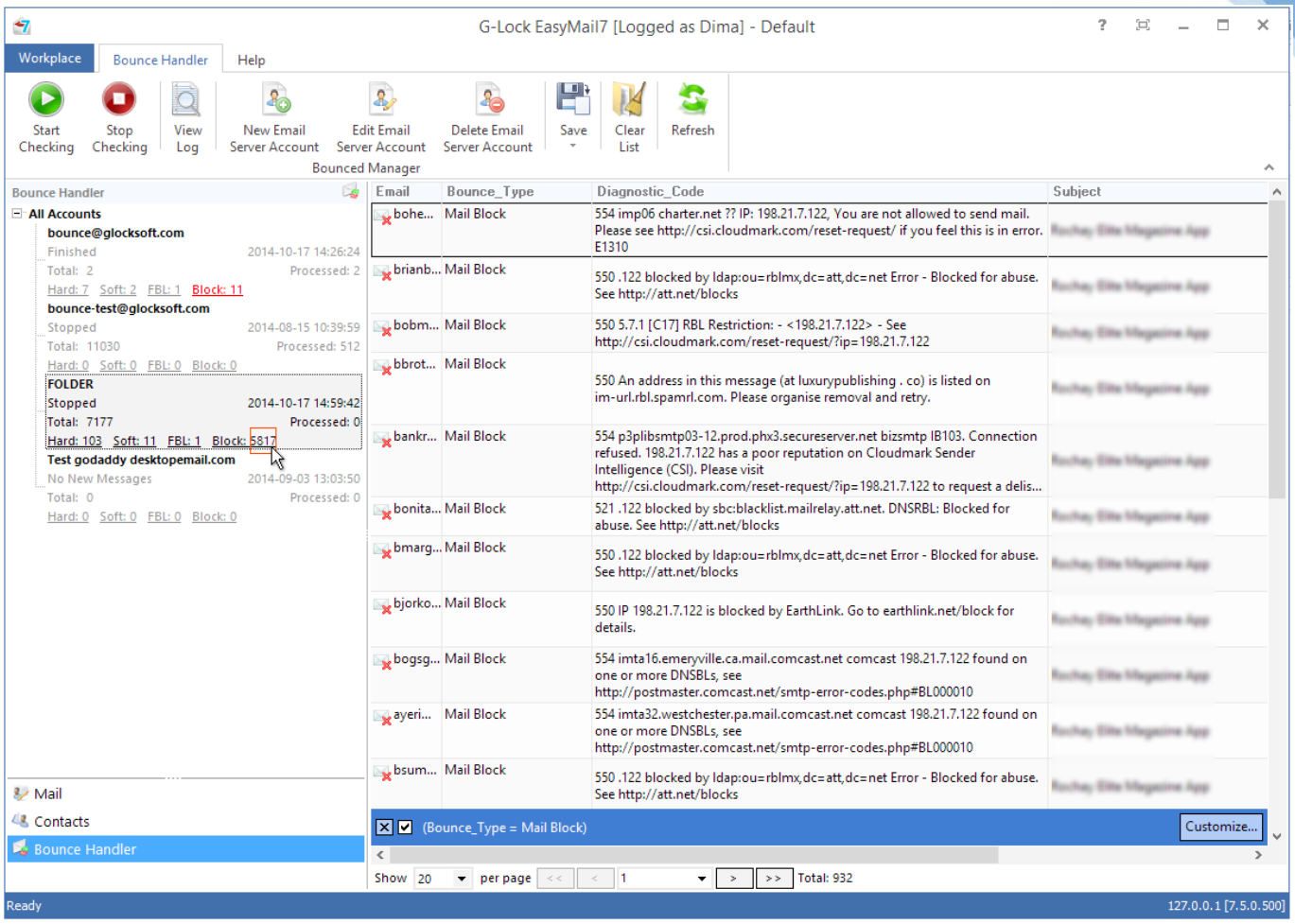
Hitting a true SPAM trap will almost always lead to an **immediate block on your IP address or the IP address of your SMTP server**. If a SPAM trap is operated by an ISP, such as Yahoo! or AOL, that ISP could permanently **blacklist your whole "From" domain**. Your bounce rate will increase and your sender

reputation will be spoiled, and as a result, the percentage of emails delivered to the Inbox will decrease.

If you hit a SPAM trap operated by an anti-spam service such as Abusix, Spamhaus, or SpamCop, delivery of your emails to all ISPs and companies who consult that service's database to filter incoming emails will suffer. Just one hit of a SPAM trap address at an anti-spam organization can reduce the Inbox delivery to major ISPs in 3-4 times.

If you have the deliverability problems and suppose they may be caused by SPAM traps, check the bounce logs (or SMTP failure logs or sending logs) for evidence of this. All ISPs who block or defer emails 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, they have detailed information as to the reason for non-delivery of the email message.

If you use **G-Lock EasyMail7** from http://easymail7.com, you can check your bounce log in the Bounce Handler. In particular, check the logs of bounce emails reported as "Mail Block".



If your bounce logs tell nothing, the next step is to check your reputation with a reputation monitoring service.

There is the handy [GlockApps reputation and spam testing tool]. You can use it to test your sender score, email authentication records, spam score, IP reputation and email placement at dozens of mailbox providers. GlockApps gives you an extra level of visibility into where your campaigns are going (Inbox or SPAM), why they are being directed to either, and actionable tips for better Inbox placement.

How to Limit Your Risk of Being Trapped

SPAM trap addresses are not obvious. Otherwise, they wouldn't do their job. So, it's important that you take measures to ensure SPAM traps never get on your list in the first place.

Here are the best practices you should follow to limit your risk of tripping a SPAM trap:

1. Never buy lists of email addresses. As any marketer, you are striving to increase your contact database. But bad ways to grow the list can have bad consequences. So, the first “no-no” in email marketing is buying email lists. You have no way to know how old the email address is and if it still exists or not.

And more importantly, by sending to a purchased list, you will violate the CAN-SPAM law that does not allow to send any emails to people without their expressed consent.

2. Never harvest email addresses. Using email harvester software to get email addresses is another bad practice, which can “ensure” the presence of SPAM trap addresses in your database. So, never add email addresses that you “found” online to your contact list.

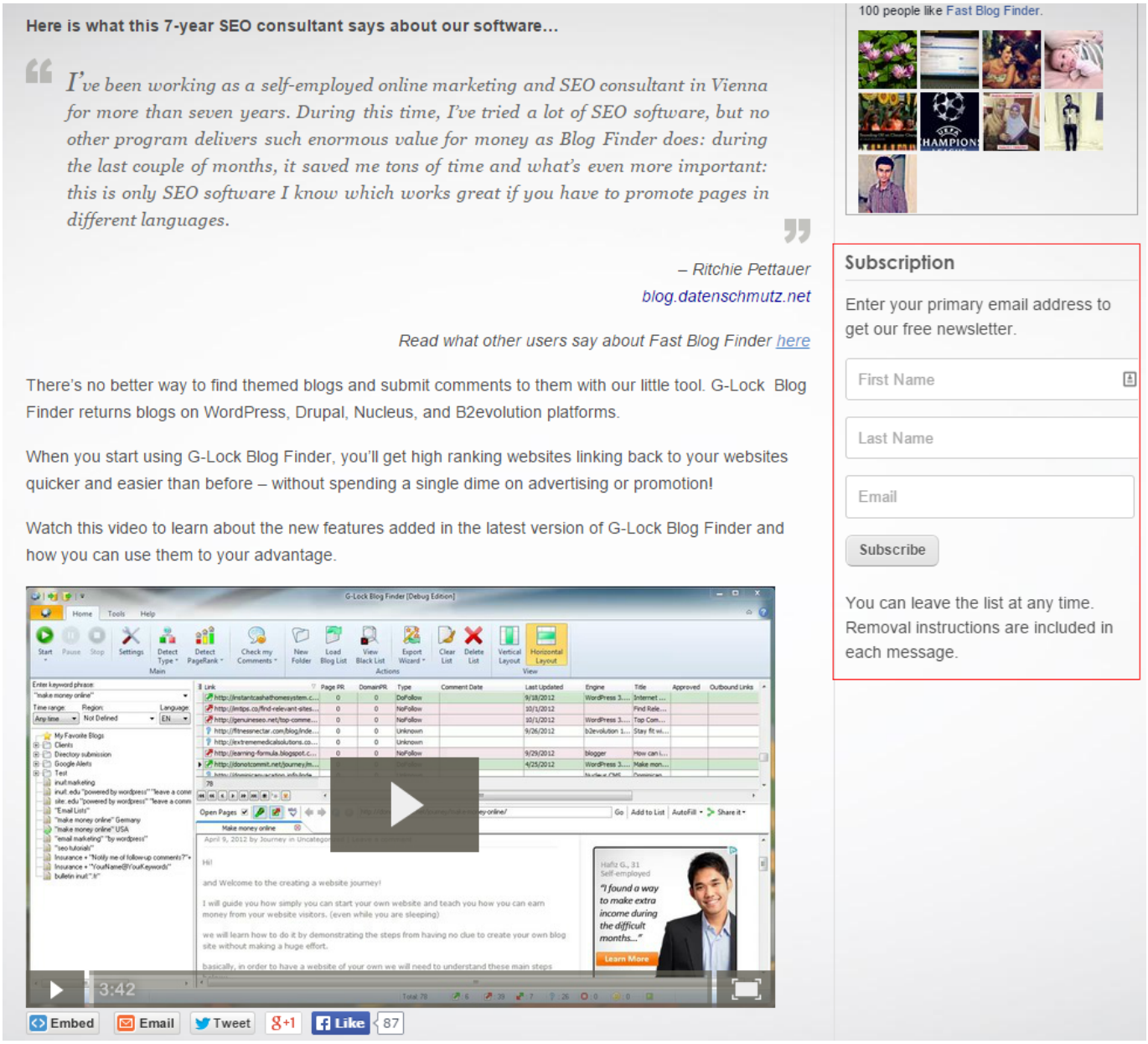
3. Delete invalid addresses before sending. Pruning invalid users is the effective way to maintain a healthy list over time and reduce your sending costs. Since ESPs have monthly plans based on the list size, cleaning the list helps keep your costs low, improving your ROI. To be on the safe side, use only email addresses reported as “good” by an email verifier tool.

If your list is very old and has not been emailed to for a long time, cleaning the list is not sufficient. In this case, it will be necessary to re-confirm the list, to ensure that the email address is still active and the subscriber is still engaged with your content.

4. Use smart opt-in forms. Using an opt-in form on your site to collect email subscribers is the good practice. However, there are pitfalls too. If you use a single opt-in procedure where the user does not have to confirm the subscription, you can end up with fake and mistyped addresses, which may turn to be SPAM traps.

With that in mind, make sure you are eliminating the risk associated with typos and fake addresses through confirmed opt-in forms. A confirmed opt-in process is the first defense in reducing the risk of getting SPAM traps.

Setting up a confirmed opt-in process on your site is easy with **WPNewsman**. WPNewsman always sends an email with a confirmation link to each new subscriber and only after the subscriber confirms the subscription, he is added to the database as confirmed. Unconfirmed users can be automatically deleted in 7 days.



5. Have a suppression list. Suppression files usually contain dead domains, role accounts, wireless domains, government entities etc. You can also add the subscribers who complained at your email at their respective ISPs to your suppression file.

Create and maintain a portable suppression list so that you can take it with you in case you change your ESP or decide to use an in-house email program. If you do not have the time or resources to maintain a suppression file, signup with feedback loops with major ISPs and use their service. However, it is still a good idea to keep those addresses on a suppression list.

6. Remove hard bounce emails. Hard bounce emails have "5XX Unknown user" SMTP error message that indicates that the address is invalid, expired or abandoned by the user. Unknown users play a role in the SPAM trap process. After approximately 6-12 months, the ISP may recycle the invalid or abandoned email address into a SPAM trap and stop sending unknown user error codes.

With that said, it is important that you check your bounce handling process to make sure you are excluding or removing hard bounce addresses from your active subscribers' list. Use professional email marketing software, for example G-Lock EasyMail7, or service with bounce management features that can remove dead addresses from your lists on autopilot.

7. Create a soft bounce threshold. Soft bounce emails can occur if the recipient's mailbox is full. This is an early indicator that the user's address may become gravestoned by the ISP in the near time and then turned into a SPAM trap. You can avoid a SPAM trap if you set a threshold for soft bounces to be treated as hard bounces and removed.

On average if you send 5 emails to a subscriber in a 30-day period, then your soft bounce threshold should be 5 soft bounces in 30 days. The 5th soft bounce email should be handled as a hard bounce one. This practice will save your reputation by avoiding hitting a recycled SPAM trap in the future.

Blocked for SPAM Traps. What's Next?

If after certain email campaign, you discover many bounce emails with the "Mail Block" error code, this may be an indication that your account with an ESP or your sender's domain with ISPs was blocked due to a SPAM trap hit, and you should take some steps to save your email marketing business.

Before you spend a large portion of your budget on services that claim they can clean your list from SPAM traps, remember this: **SPAM trap is only known to the owner of the SPAM trap.**

So, there is no email verifier tool or service that could determine SPAM traps. You will just waste your money with unfair SPAM trap removal services.

Providers and anti-spam organizations owning SPAM traps keep SPAM trap addresses in secret and simply will not tell you, which SPAM traps you hit because setting up a new address would require valuable time and expensive resources.

Getting blocked for SPAM traps is costly and disruptive, it can have catastrophic implications for your ability to deliver emails to the Inbox in the future, and the process of recovering can be quite difficult.

With that said, you must try **to never get traps in the first place**. However, if you hooked them, there is a lot of work to do. If you follow best email marketing practices, you've already done half of the work. If not, it's time to start.

Below are a few steps to help you wash SPAM traps off:

1) **Throw your purchased or harvested list out** no matter how you cherish it. As we've already told, purchased and harvested email lists are the primary source of SPAM traps. So, get rid of it and start from a scratch using a confirmed opt-in process on your website.

2) **Pay attention to a large increase in subscribers in a short period**. Any abnormal behavior should put you on guard. If your subscriber's database was growing slowly and suddenly, you got a boost in signups, scrutinize your subscription process. Probably it was changed to a single opt-in process and you got unconfirmed subscriptions from bots, or someone of your colleagues or employees added contacts taken from an untruthful source to your main database.

3) **Reconfirm your list.** If you are making money from your list, each email counts. Reconfirming will surely cut your email list by half or more. With that in mind, you can proceed with reconfirming only certain segments of your database. As an

example, you can segment your database by activity and reconfirm only those users who did not open your email during the last 3 months. Or, if you had a recent boost in signups, you can reconfirm only new subscribers. This is a standard best practice, something that all marketers should do on a regular basis.

4) **Suppress inactive and role accounts** before they are set as SPAM traps. You'll want to exclude subscribers who did not reconfirm their subscription from your main list. Never add unconfirmed users to your subscriber base. And never keep role accounts as there is no specific person behind it.

A good idea is to work with a deliverability and list monitoring service like Return Path to have an in-depth analysis of your list acquisition, list quality, list hygiene and monitor your progress. It will help you track if the measures you took have a positive effect on deliverability or not.

Recovering from negative consequences of SPAM trap hits can be a long and costly process depending on the origin, type of SPAM trap, and ISP/anti-spam organization, which owns the SPAM trap. Your blocked IP address or subnet of IP addresses can take from 6 months to a year to completely recuperate from just one SPAM trap hit if you do exactly what's requested by the trap owner.

When the block is removed, segment your list by opens and clicks and start by sending only to your most engaged subscribers, which will help you restore your sender reputation back to normal and productive level.

Obviously, being blocked for SPAM traps is distressing but it's not the end of the world. Going through the control and recovering process is actually a great opportunity for you to improve your list management and sending practices to avoid getting SPAM traps ever again.