



SPAMTRAP 101: The Email Marketer's Guide to Understanding Spamtraps

TABLE OF CONTENTS:

Spamtrap Basics.....	3
What Happens if I Email a Spamtrap?.....	5
How Marketers Get Spamtrap Addresses on their List.....	6
The Keys to a Spamtrap Free Life.....	7

SPAMTRAP BASICS

WHAT IS A SPAMTRAP?

A spamtrap is a valid, deliverable email address that is exclusively used to receive unsolicited email. Spamtraps may be virginal (i.e. a new email address) or re-purposed (i.e. previously used by a person).

Messages sent to spamtrap addresses are monitored by both human or automated processes. Appearance-wise, a spamtrap address may be indistinguishable from any normal email address.

Two Types of Spamtraps

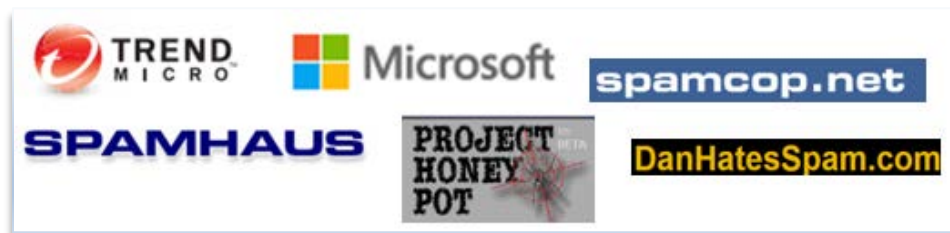
Created

- New email address, set up solely for a spamtrap.
- Often hidden in websites, waiting to be 'harvested' by scraping software and then sold to others

Recycled

- Former email address of a real person, now abandoned
- Held in quarantine for 1+ yrs, during that time it bounces. Then turned back on, as a spamtrap.

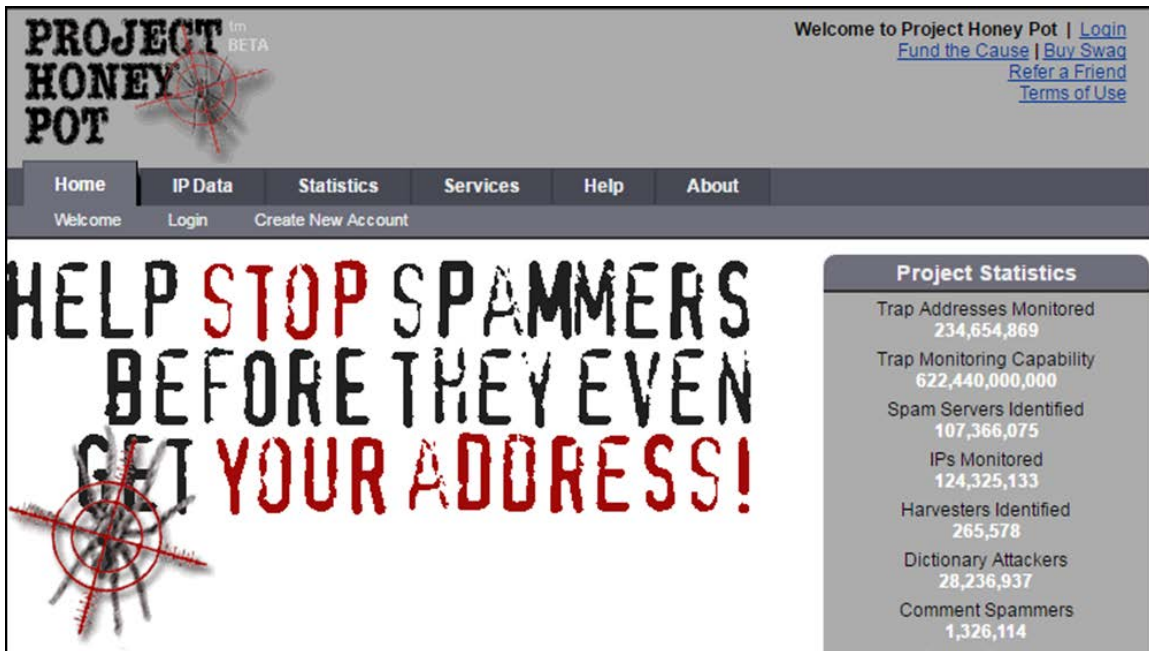
WHO CREATES SPAMTRAPS?



- ISPs & mailbox providers (e.g. Verizon, Comcast, AOL, Microsoft, etc.)
- Companies selling spam-filtering services (e.g. Barracuda, Trend Micro, etc.)
- Nonprofits and volunteer groups (e.g. Spamhaus, Project Honeypot, etc.)
- Individual anti-spam crusaders

HOW MANY SPAMTRAPS ARE THERE?

Hundreds of millions or more! New spamtraps are created 24/7/365. For example, one spamtrap operator, Project Honeypot, has a constantly updating counter on their site indicating how many traps they themselves monitor, and it's currently at 234 million.



The screenshot shows the Project Honeypot website. At the top left is the logo "PROJECT HONEY POT" with a spider icon. To the right, it says "Welcome to Project Honeypot" followed by links: "Login", "Fund the Cause", "Buy Swag", "Refer a Friend", and "Terms of Use". Below this is a navigation bar with "Home", "IP Data", "Statistics", "Services", "Help", and "About". Under "Home" are links for "Welcome", "Login", and "Create New Account". The main content area features a large, stylized text graphic that reads "HELP STOP SPAMMERS BEFORE THEY EVEN GET YOUR ADDRESS!" with a spider icon. To the right of this graphic is a "Project Statistics" box containing the following data:

Project Statistics	
Trap Addresses Monitored	234,654,869
Trap Monitoring Capability	622,440,000,000
Spam Servers Identified	107,366,075
IPs Monitored	124,325,133
Harvesters Identified	265,578
Dictionary Attackers	28,236,937
Comment Spammers	1,326,114

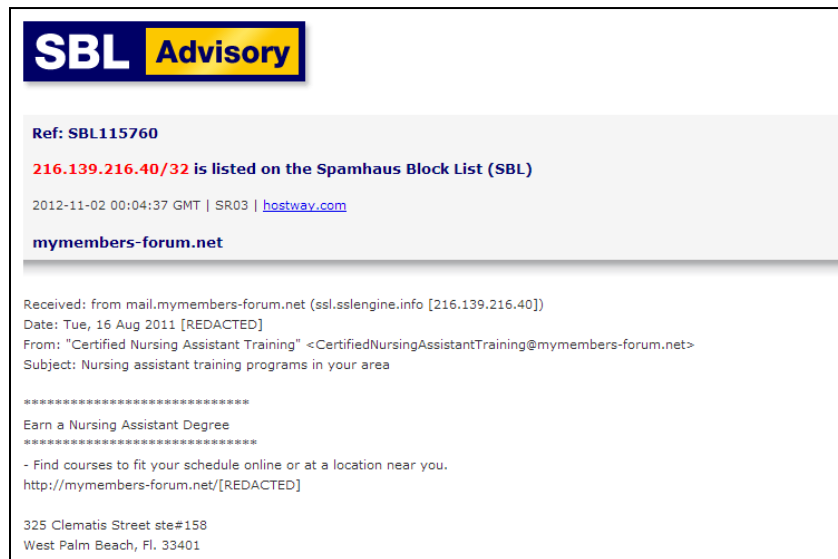
ARE SPAMTRAPS EVIL?

No! Spamtraps are a valuable component of our email ecosystem because they provide critical insight into the behaviors and electronic fingerprints of true spammers. The spam filtering technology we all depend upon for a cleaner inbox often utilizes the insight gleaned from spamtraps.

It's probably best to think of spamtraps like spiders... you recognize their importance but you certainly don't want them popping up in undesired locations.

WHAT HAPPENS IF I SEND EMAIL TO A SPAMTRAP?

As a marketer or ESP, it's bad news if you send an email to a spamtrap. Exactly what happens next has a lot to do with the spamtrap operator, the quantity of their traps you hit, the number of times you email the same spamtraps, and the content of what you mailed. **Possible outcomes include:**



- **Nothing.** The spamtrap operator may ignore the email entirely or perhaps just record what you sent in case it happens again.
- **Flag similar messages as spam.** The spamtrap operator may decide to deliver other emails that look like yours to their customers' spam folders.
- **Block similar messages.** Your mailserver's IP or domain may start seeing blocks/delivery rejections from the domain(s) managed by the spamtrap operator.
- **Delete similar messages.** In extreme cases, the spamtrap operator may make the decision to protect their user base and unceremoniously delete all mail incoming from your mailserver IP or domain.
- **List you** – Your mailserver's IP, your domain, or more may appear on a blacklist, and other mail operators who watch that list may also take any of these listed actions as well.

Usually your ESP will let you know if you message a spamtrap. Alternatively, you can utilize a service that monitors blacklists or you can simply watch your marketing outcomes - if you are seeing a decrease in your key performance metrics (sometimes only within a single domain/ISP), it is likely you are having a deliverability problem that may be caused by mailing a spamtrap.

HOW MARKETERS GET SPAMTRAPS ON THEIR LIST

Actual Spamtraps

- psbltrap@kernelnewbies.nl
- kevin822@aol.com
- foceisahniienoowo@oucs.ox.ac.uk



1. **Bad data.** The vast majority of lists for sale contain spamtraps, many of which were the result of scraping (aka 'harvesting') email addresses off the Internet. Thus, the adage 'don't buy a list' is sound advice. Sometimes unbeknownst to you, the source or vendor you utilized to help you build your list is filling your database with low quality bought or scraped addresses, including spamtraps.
2. **Bad list management.** Conscientious email marketers message their list routinely and carefully suppress bounces and unsubscribes from future sends. Failure to follow these best practices may result in you messaging re-purposed spamtraps.
3. **Bad luck.** It is possible that spamtraps are registered accidentally through your regular signup process. Some spamtrap networks operate off the typo domains of major ISPs and can end up in your list simply because of sloppy keystroking.
4. **Poisoning.** Spammers or competitors have been known to intentionally register known spamtrap email addresses in an effort to get the marketer in trouble or discredit the spamtrap provider.

SOLUTION: LIVING FREE OF SPAMTRAP FEARS

Marketers who want to live a spamtrap-free life should follow these three tenets:

- A. **Formalize best practices.** Don't buy lists. Don't scrape the internet for email addresses. Scrutinize your vendors and data sources carefully. And of course, always suppress bounces and unsubscribes.
- B. **Routinely message.** Be sure you are actively utilizing your email addresses. If you aren't touching every address on your list at least a few times a year, you may fail to notice when an address goes bad, which could be a precursor to it becoming repurposed as a spamtrap.
- C. **Run routine list hygiene.** Work with an industry expert to help you regularly scrutinize your email list for typos and spamtraps. You can implement an API at the point of acquisition, do quarterly reviews, or set up for automated monthly monitoring. Trace any problems upstream and fix (or remove) that acquisition source.

ABOUT FRESHADDRESS:

FreshAddress, Inc. helps companies including 25% of the Fortune 100 and many of America's leading nonprofits to build, clean, and update their email databases to maximize revenue and donations. FreshAddress offers services including its SafeToSend® Deliverability Solution, patented Email Change of Address (ECOA), and Postal and Email Appending. FreshAddress also provides customer lifecycle and optimization solutions.