

How spam traps work and how to avoid them

Internet Service Providers and organisations that help keep the internet safe create email addresses that act as fishing nets, left sitting wide open and hovering in cyberspace, waiting to receive spam email, so they can trace and block senders.

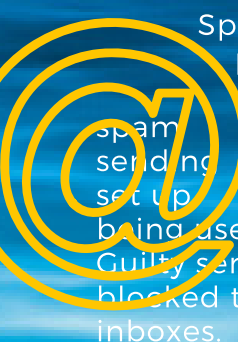
How spam traps work

It's simple. 'Someone' creates an email address and decides it is a spam trap. The email address isn't used for regular email interaction, it's not used to sign up for services or in transactions. It's basically invisible.

The inbox is monitored; anyone who sends to it must be sending spam. The spam trap owner can then list the IP address of the mail server on private or shared 'blacklists', resulting in blocking further emails.

Some spam traps are known, allowing cross-checking of email addresses to remove the risk of emailing to them.

Remember - spam traps don't opt-in to mailing lists, so if you are only growing your list by opt-in you shouldn't be sending emails to any traps.



Spam traps catch emails sent without permission and/or at high volumes, or breaking any other rule set up by the trap owner. They identify servers sending spam, and servers that are badly set up and potentially vulnerable to being used as mules for fraud attacks. Guilty servers have their IP addresses blocked to prevent their emails reaching inboxes.

Malicious vs genuine spam traps

Genuine spam traps are good news. There are spam traps that are not. They are used as a predatory way of gathering IP addresses and generating revenue through ransom, or subscription. We refer to them as malicious spam traps.

There are two main 'MOs' for malicious spam traps, both generate blacklists.

The first is a network of entities that gathers and shares IP addresses from incoming mail, and an organisation that harvests IP addresses en masse. The lists are referred to by some system managers as a screening service for incoming mail. It's expensive and time-consuming to get IP addresses off these predatory lists



Product information:
MORE Email validation API
CORE Bulk email list validation

Our professional email validation service analyses email addresses to cross-check against known spam traps and protect senders from malicious spam traps.

How does email validation detect spam traps?



FACT. No system can ever detect every spam trap. Genuine spam traps are just ordinary email addresses, there is no special code or 'tell' that is recognisable

If your mailing list is opted in, up to date and you deal with unsubscribes and bounces spam traps shouldn't worry you.

If you're thinking of sending emails to an old list you might be unlucky and find a spam trap that has been created from a recycled email address.

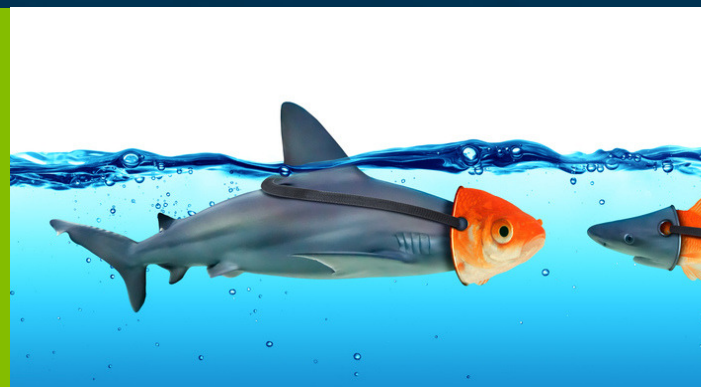
If you're sending bulk emails via an Email Service Provider (ESP) their sender reputation should be able to withstand an occasional one-off unlucky send to a spam trap. Emails sent often and at high volume from a server that's not secure are more likely to trigger an IP address block.

To detect a limited number of genuine spam traps, you'll need to validate your emails against a static list of spam traps accessed or curated by email validation companies. Detection rates can never be 100% guaranteed, as spam traps change all the time.

A limited number of reputable email verification companies check for malicious spam traps. These checks detect domains and email addresses associated with pro-actively reporting and blacklisting servers that have not sent spam, but have sent legitimate emails.

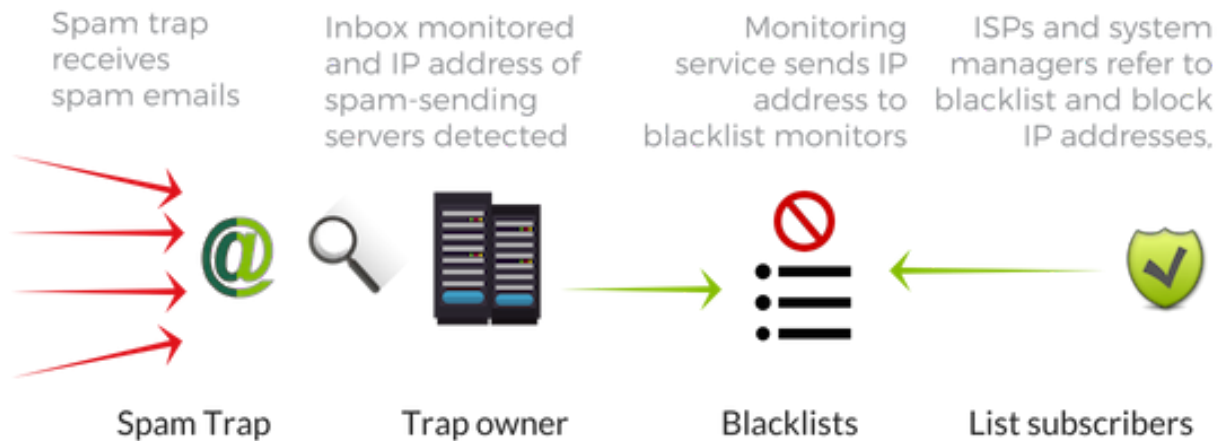
Types of spam traps:

- **Honeypots** - same as spam traps
- **Seeded list** licence controls - used to police licenced or unauthorised data usage
- **Embedded** in code - detecting email scraping and blocking incoming mail
- Individuals using an email for catching and reporting spam - low level '**squealers**'
- **Malicious** spam traps for IP ransom - the worst kind of spam trap



Malicious spam traps waste time and cost money. Learn more about them in our blog.

How spam traps work - a simple overview



How some malicious spam traps work



- Honeypots - same as spam traps
- Seeded list licence controls - used to police licenced or unauthorised data usage
- Embedded in code traps - detecting email scraping and blocking incoming mail
- Individuals using an email for catching and reporting spam - low level 'squealers'
- Malicious spam traps for IP ransom - worst kind of spam trap
- Reverse engineered spam traps - equal worst kind of spam trap!

Think of a honey trap email address in the same way as a spam trap email address. It's essentially an email address that is monitored and deliberately used to catch out, block and/or report senders of unrequested emails.

A seeded list is entirely different. When data is sold by a reputable broker, it is usually licenced. The terms of the licence typically include how often it can be used and how frequently. By seeding the list with contact details that are monitored by the broker, they can check to make sure that buyers don't stray outside the terms of their licence.

Email addresses embedded in web code or planted in data. These email addresses are only detected by systems that are web scraping or scavenging for data to use illegally.

Individuals maintaining private spam traps aren't as influential as those maintained by ISPs and the security community. If your mail is marked as spam by a recipient and they haven't unsubscribed from your list, it's good practice to remove them from the list in any case.

Malicious spam traps for IP ransom are thankfully rare. There is one prime entity that carries out this activity. UCE protect, via the IP blacklist they maintain; 'Backscatterer'. The model here is that IP addresses sending to email addresses farmed by the UCE protect network are held to ransom. If you get on the UCE protect list you will have to pay your way off. We've written articles about UCE protect for more detailed reading. Good to know here is that we monitor domains associated with this activity and mark email addresses as spam traps, we also identify UCE protect as a datapoint, to help our customers can steer clear of this harvest / ransom operation.