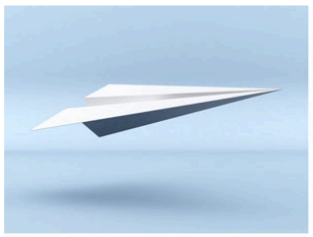
Where Does Email Go When It Isn't Delivered? Part 2

3 years ago 1 By Tariq



A sender's reputation can follow not only an IP address but a brand and a sending domain. A holistic approach is necessary when considering a sender's reputation as no one factor alone determines what that reputation is. Reputation can be broadly defined as the opinion of a community toward an object. Knowing what the community looks for when determining a reputation will allow you to maximize your delivery rates.

Spamtraps

We first eluded to spamtraps when we discussed Paid Subscriber Lists. A spamtrap is an email address that appears to be valid but is in fact used by ISPs to catch spammers. You will sometimes hear these referred to as "honey pots." Spammers use harvesting programs which scan millions of web pages looking for email addresses. These email addresses may come from old email addresses which are recycled by ISPs in order to catch commercial emailers that use old, rented, or paid subscriber lists. Some sites bury email addresses in their source code so that they are picked up by harvesting programs. The company where the email originated is then alerted to any incoming emails that go to that address at which time they contact your web host and file a spam complaint. Spam traps are bad news. Its been reported that your delivery rate can drop as many as 20 points drop with one spam trap hit. Spamtraps are one of many factors that ISPs look at when calculating your sender reputation. Not only is your delirability affected but they can result in temporary or long term blocks.

Good list maintenance is necessary for avoiding spam traps. Here are some things you will need to avoid:

- Poor List Sources - This includes avoiding paid subscriber lists as mentioned previously
- List Poisoning – Using confirmation Opt-In mailings will reduce the chances that you will receive invalid email addresses
- List Aging - Because spam traps are often used by recycling old email addresses use bounce management to remove any old email addresses and also remove any inactive addresses from your list.

Sender Authentication

This is used to prevent domain forgery and spoofing and provides a framework for helping ISPs to distinguish between legitimate email senders and spammers. ISPs Identifying and verifying a claimed domain name has been authenticated or authorized for sending from a MTA makes it possible to treat suspected forgeries with suspician, reject known forgeries, and block email addresses from known spamming domains.

- Sender Policy Framework (SPF) – a record that allows you to determine which computers can send emails on behalf of your domain. Adding an SPF record to your domain name's TXT entry, while not required, can help improve email delivery rates by reducing the chance that the emails you send will be seen as spam. It can also help prevent others from sending spam and using your domain name. This is used by Bellsouth, AOL, Gmail, and MSN/Hotmail.
- Sender ID – is very similar to SPF record except this extends the verification process to include the purported responsible address included in the header. Used by MSN/Hotmail
- Domain Keys – an authentication standard that is designed to verify the DNS domain of email sender and the message integrity. All outgoing emails are digitally signed with a private encryption key to match a public key that is published in the sender's DNS record. Used by Gmail, Yahoo, SBCGlobal, British Telecom, Rogers Cable, Rocket Mail, etc.
- DKIM – an enhanced authentication standard that allows a person to verify that a message comes from the domain that it
- Sender ID – is very similar to SPF record except this extends the verification process to include the purported responsible address included in the header. Used by MSN/Hotmail
- Domain Keys – an authentication standard that is designed to verify the DNS domain of email sender and the message integrity. All outgoing emails are digitally signed with a private encryption key to match a public key that is published in the sender's DNS record. Used by Gmail, Yahoo, SBCGlobal, British Telecom, Rogers Cable, Rocket Mail, etc.
- DKIM – an enhanced authentication standard that allows a person to verify that a message comes from the domain that it claims that it came from.

Getting Technical

Your system admin should be able to assist you with ensuring that the following technical configurations are in line as they can improve or harm your sender reputation.

- IP Address – because email originates from this address you need to establish a low history of spam complaints, spamtrap hits, and low bounce rates in order to have a positive reputation that will affect your long term deliverability. If you wish to qualify for whitelists, feedback loops, and reputation services, your IP address must have low spam complaints, unsubscription management, and proper setup for the domain associated with it.
- Sending Domain or Subdomain – Domain registration and domain age are two factors for establishing a positive reputation. Newly registered domains are regarded with suspicion as spammers often hop from domain to domain. If a sending domain has a bad online reputation it will result in low deliverability rates.
- RFC Compliance – these are information documents used as governing standards for internet traffic. RFC 2821: Simple Mail Transfer Protocol and RFC 282: Internet Message Formatare relate to email reputation.
- Reverse DNS – used to identify the domain name associated with an IP address. The IP address is the only data that can not be forged and not having this enabled is in violation of RFC standards and a requirement for many ISPs. If this is not enabled or is configured improperly you must immediately contact your server admin.
- Bounce Management – An email address is considered dead and should be removed from your list if it bounces 3 consecutive times or if the time between the most recent consecutive delivery rejection is in excess of 15 days.

Where to Go From Here

The final way to improve your deliverability is to get certified or accredited by a reputable organization. There are three different types of ways to get yourself certified! The first gets your emails automatically whitelisted or delivered to ISPs and companies that are working with the relevent program. Another audits your email practices so that you can display a seal of approval next to your sign up form. Another allows you to display an icon next to your email in your inbox that indicates that your email passed a quality test. We will focus on whitelisting programs here:

- Goodmail Systems - ISPs supporting this program ensure delivery with a "certified" icon attached. This accreditation is supported by Yahoo and AOL.
- Sender Score Certified – Acceptance in this program puts you on the whitelist that includes 240 email address as well as MSN/Hotmail and Roadrunner.
- Habeas – requires business processes and email practices. Their safelist is support by many email receivers including AOL, Earthlink, Google, and MSN
- SuretyMail – While not technically a whitelist a large number of ISPs, spam filters, and mail servers take this accreditation into account when making delivery decisions. Senders with this accreditation will see improved delivery.

If you are concerned about whether you have already been blacklisted you can go here.