



**A Guide to Deliverability**

1. Key Equations

**Delivery Rate**

This metric gives an overview of the amount of messages successfully delivered to your subscriber base. We calculate this by taking the number of emails that were delivered and dividing it by the total number of sent. This figure is presented as a percentage.

**Hard Bounce Rate**

A hard bounce is caused by an invalid or expired email account. This metric will show you the integrity of your data. A high hard bounce rate indicates a necessity to investigate your data collection processes. A consistently high or incremental bounce rate over time could potentially be due to poor data processing, with email addresses that have bounced are not being removed from future mailings in a timely manner. This should always be monitored as it may cause your IP address to be blacklisted, adversely affecting future delivery of all your campaigns.

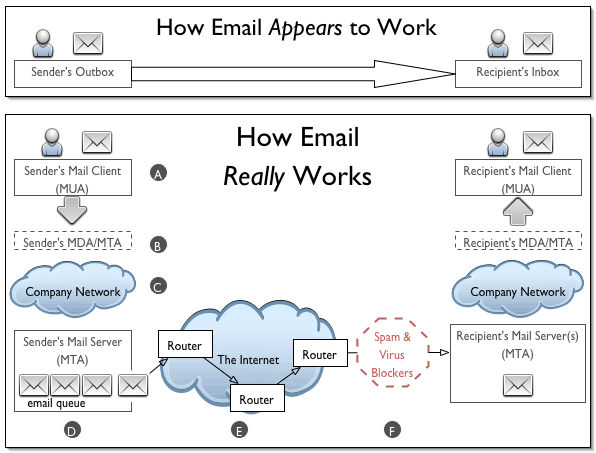
**Soft Bounce Rate**

A soft bounce might occur because the recipient's inbox is full, so a future message may be delivered or may be forwarded manually by the network administrator in charge of redirecting mail on the recipient's domain. Soft bounces also need to be monitored but the threshold for removing addresses should be more lenient than for hard bounces as it may only be a temporary issue.

2. Key Terms

**Mail Transfer Agent (MTA)**

* A Mail Transfer Agent (MTA) is a server that transfers email messages between hosts using **SMTP**.
* A message may involve several MTAs as it moves to its intended destination.
* While the delivery of messages between machines may seem rather straightforward, the entire process of deciding if a particular MTA can or should accept a message for delivery is quite complicated. In addition, due to problems from spam, use of a particular MTA is usually restricted by the MTA's configuration



**Internet Protocol (IP) Address**

* An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) connected to a network or the Internet.
* An IP address serves two principal functions: host or network interface identification and location addressing.
* In Email Marketing it is tied directly to the various forms of **Sender Authentication** that will be discussed later.

**Simple Mail Transfer Protocol (SMTP)**

* Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.
* Simply put it is the language Mail Servers use to communicate
* When a **bounce** is recorded by a Mail Server it is accompanied by a SMTP code about the nature of that bounce.

**Internet Service Provider (ISP)**

* An Internet Service Provider (ISP) is an organization that provides access to the Internet, or more particularly are usually Mailbox Providers hosting an email account for users.
* The most well-known of course being AOL, Comcast, Gmail, Hotmail and Yahoo.

**Whitelist**

* A list of IP addresses or domains that are **explicitly** allowed to send to a particular system.

**Blacklist**

* A list of IP addresses or domains that are **explicitly** prohibited from sending emails to a particular system.
* It is usually maintained by an ESP, ISP or 3rd Party provider

3. Bounces and other Errors

**Bounce**

* A bounce occurs when a Mail Server rejects delivery of an email.
* The Mail Server sends back a SMTP message with the reason for the rejection

They can normally be categorized in to 4 groups:

* Hard Bounce – The email address is invalid or simply does not exist on the receiving system.
* Soft Bounce – There is a temporary error with the email address because the server is down, the users mailbox is full or busy.
* Block – The sent message is rejected by the ISP because of poor sender reputation, unapproved Sender Authentication or due to content that has been picked up by the ISP’s or user’s filters.
* Technical – There has been a SMTP communication error between the two MTA servers.

**Filters**

A bounce occurs

4. Spam and Compliance

**SPAM**

* Spam is a word that is often thrown around and has given a bad reputation to genuine Email Marketers.
* Email spam, also known as unsolicited bulk Email (UBE), junk mail, or unsolicited commercial email (UCE), is the practice of sending unwanted email messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients.
* Basically, can be defined as **ANY** email a user does NOT want either because it was solicited or because it is not relevant to them.
* In 2008 a survey by MarketingSherpa claimed that over 50% of the time an email user click the ‘spam’ or ‘junk’ button was because the mail was unsolicited.
* There are a number of laws around the world aimed at protecting users from ‘spam’ such as the EU Privacy Directive 2002/58/EC and US CAN-SPAM.

These laws vary from country to country but there are a few key points that should be considered the cornerstone of any responsible Email Marketer:

* Establish affirmative consent in the form of an Opt-In – Many less reputable companies will attempt to buy email lists in order to increase their own. In almost all cases this end up having the opposite affect by increasing complaints, unsubscribes and generally damaging your Sender Reputation.
* Make the process to unsubscribe easy – Don’t be afraid of your subscribers unsubscribing. If they want to get of your list it probably means that they don’t find you content very relevant, are not engaging with your email program and are almost certainly not improving your revenue.
* Make it clear who the email is from – If they have Opted-In your susbcribers should be familiar with you brand so make it clear to them. It is also good practice to make it easy for them to contact you either by replying to the email or by you making your visible mailing address available to them.

**Spamtraps**

* Many ISP use 3rd party Partners to help them manage potential spam.
* The most widely used of which are SpamHaus,…
* Despite their reputation these partners can NOT afford to be ignored. A SpamHaus block for example can result in **40-70%** of your mail being blocked by the major ISPs and will of cause a suspension of your sending privileges by you ESP.
* Spamtraps are usually e-mail addresses that are created not for communication, but rather to lure spam and normally come in 2 forms:
* **Standard Spamtrap** – In this case an email address is allowed to become redundant (usually by allowing the inbox to reach capacity) in order to cause a soft bounce message to be returned to the senders ESP. After allowing this state to continue for a prolonged period of time the email account is the cleared to allow ‘new’ messages to enter the inbox. The idea being that any responsible sender should have responded to the persistaent soft bounces and desisted from sending this account a long time before.
* **A Honey Pot** - In order to prevent legitimate email from being invited, the e-mail address will typically only be published in a location hidden from view such that an automated e-mail address harvester (used by spammers) can find the email address, but no sender would be encouraged to send messages to the email address for any legitimate purpose. Since no e-mail is solicited by the owner of this spamtrap e-mail address, any e-mail messages sent to this address are immediately considered unsolicited.

**Spam Filters**

* These can be applied at 3 stages – at time of deployment by the sending ESP, by the ISP as it comes through to their MTA or by an individual user’s personal filters.
* Filtering methods can be broad grouped in to 3 categories:
* **Heuristic Filtering -** Heuristic filtering works by subjecting email messages through thousands of pre-defined rules each of which assigns a numerical score to the probability of the message being spam.

**This is why there are certain key words that should be avoided e.g. $$$, “sex” etc.**

The result of the final equation is known as the Spam Score. The spam score is then measured against the user’s desired level of spam sensitivity - whether low, medium or high sensitivity.

Setting a higher level of sensitivity leads to more spam being captured, but has the adverse effect of filtering legitimate emails as spam. This is known as a false-positive.

* **Volume Control Filtering –** This works at an IP level and simple limits how many emails an ISP is willing to accept from a specific IP before it starts returning all incoming email.
* **Bayesian Filtering -** Bayesian spam filtering is a statistical technique of e-mail filtering. Bayesian classification work by correlating the use of tokens (typically words, or sometimes other things), with spam and non-spam e-mails and then use this to calculate the probability that an email is or is not spam. In short it is a system that learns – so the more individuals who flag your email as spam the higher the chance that the entire system will start to automatically block your emails.

**Anti-Spam Laws**

* **United Kingdom**
* **UK Companies Act of 1985**
* **UK Companies Act of 2006**
* **UK Statutory Instrument 2003 No. 2426**

<http://www.legislation.gov.uk/uksi/2003/2426/contents/made>

* **EU Privacy Directive 2002/58/EC**

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML>

* **Data Protection Act 1998**

<http://www.legislation.gov.uk/ukpga/1998/29/contents>

* **Around the World**
* **US/NA: CAN-SPAM Act of 2003**

<http://www.fcc.gov/guides/spam-unwanted-text-messages-and-email>

* **Canada: CASL (Canadian Anti-Spam Law)/FISA**

<http://lois-laws.justice.gc.ca/eng/AnnualStatutes/2010_23/FullText.html>

* **Germany**: **Act Against Unfair Competition**
* **Australia: Australia Spam Act 2003**

<http://www.acma.gov.au/webwr/consumer_info/frequently_asked_questions/spam_business_practical_guide.pdf>

Information about the laws in other countries can be found here: <http://www.spamlaws.com/>