Essence of Email

Introduction to Email Deliverability

Table of Contents

What is Deliverability

Deliverability is the ability for your email to be delivered, accepted by the ISP's, and put into the inbox. This description is deceptively simple, however, as the topic of deliverability can get really technical really quickly. On the whole, like SEO (arguably more so), email deliverability is somewhat of a black box. There are no "definitive" ranking factors and exact weights given to each factor that goes into determining ultimately whether or not you get into the inbox. Whereas SEO is primarily driven by Google's decree, email deliverability is a more varied landscape, as there are many more email clients and third parties at play, each with a different version of their algorithms for determining inbox placement & positioning of your emails.

Why Should You Care

Building and maintaining good deliverability is critical for your email marketing program because it is the first step for getting in communication with your subscribers. You can have the greatest marketing campaigns ever, complete with killer copy and irresistible imagery...but if your subscribers never see your emails in their inbox, it's all for naught.

According to Return Path's Q4 2012 benchmarks, the average inboxing rates for the United States is 82% and Europe is 84%. Latin America is 72%, with Asia-Pacific and Africa trailing at 65% and 28% respectively.

This means if you are an "average" sender about 20% of your emails never made it to the inbox. If you are worse than average...well, you get the point.

Factors that Affect Deliverability

Nobody really knows the exact weights for each deliverability factor, but let's dive into some of the major ones that impact your sender reputation:

1. Authentication

There are multiple authentication frameworks in place used by ISP's to determine if the email is coming from the legitimate sender. Several key infrastructures used are:

- DKIM - DomainKeys (Yahoo!) + Identified Mail (Cisco)
- DomainKeys - Yahoo!
- SenderID - MSN/Hotmail
- SPF (Sender Policy Framework) - Directly maps sending IP address to whether or not on list of allowed senders

Your email service provider (ESP) will likely handle most of these authentication processes for you or are able to help you set them up.

2. Spam Trigger Content/Spam Filters

The following practices increases your chances of tripping spam filters:

- Spammy words and notations such as: free, viagra, ALL CAPS, !!!!
- Large file size
- Low text-to-image ratio, i.e. too many images relative to HTML text

Some better known spam filter providers include: Barracuda, McAfee, Postini, Cloudmark, and Spam Assassin.

3. Blacklists & Spam Traps

There are also multiple industry blacklists. Some of the major ones include:

- SpamHaus
- Spamcop
- MAPS
- SORBS

You can check if you are on any blacklists by going to one of the resources in the next section. If you do find yourself on one or more blacklists, you'll need to take the steps they detail to get yourself removed. Many times your ESP can help you out with the process.

A spam trap is basically a booby-trap email address. There are "pristine" spam traps created by ISP's or blacklists that are essentially fake email address that are never subscribed to any email lists, and mainly only accessible by bots crawling a page. The intention behind this is to catch anyone sending to an address that never opted in, and is most likely bought or rented.

ISP's also sometimes create recycled spam traps, where they take old, very inactive email addresses and turn it into a spam trap. This practice is used to ensure senders are following good list practices (another reason to regularly clean your list).

The impact of "hitting" a spam trap is immense. Basically, your deliverability can tank overnight, which could take awhile to recover from. We've seen 95% inboxing drop to 60% immediately after hitting a spam trap, with the consequences carrying on over a few weeks despite our follow up efforts.

Quick note: Unsubscribes do not hurt your deliverability.

4. User Engagement - open/click, whitelisting, starring

ISP's (Yahoo!, Gmail, Hotmail, etc) are increasingly giving more weight to "engagement" metrics to both determine inbox placement (whether your email is put into the inbox) and inbox positioning (the position inside the inbox).

Engagement ratios such as open rates and click rates, as well as other positive user actions like whitelisting (adding to address book), starring, or marking as important all play a role in shaping your engagement profile. The emphasis on engagement is another reason why you need to follow best practices to send relevant, targeted email to a clean email list of subscribers.

5. Bounce Ratio

A "bounce" happens when the ISP's servers rejects your incoming mail. There are two major classes of bounces.

A **hard bounce** is an outright, permanent rejection by the recipient server. This is typically caused by invalid email addresses (nonexistent or misspelled domains for example).

A **soft bounce** is a delayed rejection by the recipient server. The outgoing mail was initially accepted, but later returned back to the ESP after processing. Typical reasons for a soft bounce are "server temporarily unavailable" or a full inbox by the recipient.

From the standpoint of your sender reputation, your hard bounce ratio is the one that will negatively impact your deliverability. Your ESP should automatically clean any hard bounced email addresses.

Soft bounces don't tend to count against you, but do drive up your CPM costs, so it's a good idea to clean consecutive soft bounces (3~5 in a row).

6. Complaint/Spam Ratio

When a user marks one of your emails as spam (also known as a complaint), it sends a major red flag signal to ISP's that your mail is unwanted.

If your email list is large, there's no real way to prevent spam complaints completely. Luckily ISP's don't look at absolute complaint numbers as much as the complaint ratio, or the total number of spam complaints compared to the volume of mail you send. A good rule of thumb is to keep your complaint ratio below 5 in 1000, or 0.5%.

7. IP Address Reputation

Your sender IP address (or pool of IP addresses) reputation is highly important for determining your deliverability. Historically, ISP's have given a lot of weight to your IP reputation, although recently there's been increasing emphasis being placed on domain-level reputation as well.

The default is you are part of a shared "pool" of sender IP's established by your ISP. This means you are sharing that range of sender IP's with multiple other people. Because the IP pool is used by multiple senders, this means the actions (both good and bad) of a single sender will have an impact on the deliverability of the other senders within the shared pool because deliverability is determined partially by IP reputation.

You can also elect to set up a dedicated IP (DIP) address just for yourself. This usually carries some upfront cost, and takes more guidance to "warm up" your IP address before sending. The major benefit of a dedicated IP is you exclusively control your sender reputation on it. This means other bad senders cannot pollute your reputation. On the other hand, if you don't follow pristine sending practices, it might actually be worse for you to be on a DIP. Depending on your volume and needs, the dedicated IP route may make sense for you.

8. Sender Domain Reputation

ISP's are increasingly putting more weight towards domain-level reputation in addition to the traditional IP-level reputation. This essentially means that your (authenticated) sender domain reputation (like email.retailer.com) will become "portable" even if you are moving around ESP's/using different IP addresses.

Domain reputation is not likely to replace IP address reputation, but rather used in conjunction to develop an overall view of your sender reputation. The same best practices apply.

9. Send Volume Trends

The consistency of your send volume also plays a part in determining your deliverability. In general, you want to keep you volume fairly consistent, as huge spikes or dips in volume sends a negative signal to ISP's. This applies across campaigns and also on individual campaigns. For this reason, it is a good idea to throttle your mailing (discussed in the best practices section).

Additionally, certain times of the year (such as holiday season) sees an overwhelming amount of mail. During these times, even if you are a good sender, ISP's may "defer" your mail due to the sheer load on their servers. Thus, it's important to be aware of when peak sending volume times are, and structure your sends accordingly.

> Insider's tip: If you are a poor sender, your ESP may (without you knowing) put you into a "dirty" pool of sender IP's with the other poor senders, so as to not contaminate their more pristine pools.

How to Benchmark Your Deliverability

ReturnPath is the industry leader for deliverability services. Their "seedlists" are the highest accuracy way so far to gauge true inboxing rates across a variety of ISP's.

To get a gauge on your current sender reputation, you can use ReturnPath's SenderScore (which is akin to a credit score). A score of 90+ is good, 50-80 could definitely use improvement, < 50 something is definitely wrong.

You can look up your SenderScore and blacklist status for free after registering an account at: http://www.senderscore.org/

To see specifics for % inboxing and % spam, you'll need to pay for RP's services.

To get a deeper gauge of domain-specific elements, you can use: http://www.dnsstuff.com/

Quick Note: The "delivery rate" shown in your ESP's dashboard is most likely not reflective of true inboxing. It typically just shows the percentage of non-hard bounced emails. So even if you are seeing a 98% "delivery rate", you may be inboxing at 65%.

Best Practices

1. Seek Permission - Whether you are capturing emails at checkout, through a site overlay, or some other source, you need to explicitly ask for permission. They more aware your contacts are that they are being opted in to your list, the lower chances they will automatically press that spam button or ignore your emails. In general, make sure to get some form of permission before sending marketing messages to your contacts.

2. Maintain a "Clean" List - This is arguably the most important aspect of ensuring good deliverability. At the end of the day, all of the advanced technical measures are aimed to reduce spam and reward good senders. Keeping a clean list is integral to protecting your reputation in the eyes of the ISP's, which will help maintain strong deliverability for your email program.

Maintaining a clean list means following best practices such as suppressing inactive contacts, getting deliberate opt-ins, segmenting the frequency of your sends, and sending compelling & relevant content to your list.

3. Regularly Monitor Your Deliverability - Deliverability is not a one-off action. Because so many factors are at play, you will inevitably see fluctuations in your deliverability. This is why it's important to do regular check ups on your current status to make sure you catch and diagnose problems early on.

4. Throttle Your Mail - As mentioned before, throttling your mail on individual sends can help improve your deliverability. Throttling means instead of sending all of your email at once to your list, you and sending it over a period (4 hours for example), so that the ISP's are seeing a more steady trickle of email coming in instead of one huge spike.

5. Make Sure Your Content is Clean - Spam trigger words, too many images, large file sizes can all trip spam filters. On your campaigns, keep an eye towards minimizing these spam triggers. Most ESP's have some form of a built-in tool to help with this.

Quick Note: Sometimes we've seen more hip & cool companies such as funny t-shirt companies using various forms of profanity in their emails. While we may find humor in this, the spam robots don't. It's better to keep the bad words to a minimum.

6. Never, Ever Buy a List - Just don't do it. Ever.

7. Don't Bury Your Unsubscribe Link - You don't have to advertise your unsubscribe link loudly, but you need it to be clear. Not only is an unsubscribe link required by CAN-SPAM law, it can also help your deliverability. Remember, unsubscribes do not count against you, but if you make it overly difficult for your contacts to unsubscribe, they may default to the spam button instead, which most definitely does hurt your deliverability.

8. Be Consistent In Your Sending - Just as consistency in business helps establish your reputation as a business person, consistency in your email sending helps solidify your sender reputation. In general, aim to be consistent in your from name, sender domain, send volume, etc.

9. Use a Private Sub-Domain - Using a private sender sub-domain, such as email.mystore.com, can help establish your domain-level reputation. ESP's will usually provide a default sender domain if you don't have a private sub-domain, but remember these won't be transferrable if you ever decide to switch providers.

10. Consider Using a Dedicated IP - If you are sending a good amount of volume and have the guidance to maintain a DIP, you should consider switching over. With a dedicated IP, you'll have full control of your own sender reputation without worrying about it being tarnished by other senders' bad practices.

Deliverability is one of those unseen elements that will govern the success of your email program.

“For Email Deliverability, Prevention > Cure.”

- Essence of Email

Summary

1. Benchmark your current inboxing status
2. Exercise good list practices such as getting permission & regularly cleaning your subscribers
3. Understand how complaints, bounces, and spam traps impact your email deliverability.

Resources

1. http://www.senderscore.org/
2. http://www.dnsstuff.com/
3. http://mxtoolbox.com/blacklists.aspx