A comprehensive guide to email deliverability for Job Sites

Presented by: Chaitanya Chinta, Co-founder of Pepipost

Deliverability Guide for Job Sites

If you're a Job Site looking for an answer to the question, "How do I get my job alerts and other emails into my subscribers Inbox?" or "What's the best way to get my job seekers to see, open and click on my job alerts?" you are in the right place. This guide will cover the basics of email deliverability with a special focus on the intricacies found in the Jobs space, what metrics to track and how to extract maximum ROI from your email program and sustain it.

If you're familiar with the basics, you can skip the section below.

What is email deliverability?

Before we get into Jobs specific metrics, it's important to start with the basics. Simply put, email deliverability is the science behind delivering emails to the Inbox. It ensures emails sent are safe for recipients, generates interest from the intended recipient and finally, delivers to the Inbox.

Delivering emails to the Inbox is a challenge because 83% of the world's email is unwanted spam. Every mailbox provider like Gmail, Yahoo and Outlook have developed their own anti-spam technologies to safeguard users from unwanted email. Usually, the antispam systems identify patterns in an email which show signs of spam and create rules that will filter or bounce further emails with those patterns. Accuracy of these rules is usually around 99%. While that might sound like great accuracy, there are a ton of emails sent every day, so this puts a lot of genuine emails in the line of fire.

As a good email sender, we strive to be in the Inbox. Understanding each of the spam filters is a complex job, but there is an easy way to achieve the best deliverability. Any discussion on deliverability revolves around reputation.

In the next parts, we will look closely at what reputation is and how it can be built, sustained and monitored. As a bonus, if you want to switch from your current email provider to a different one (preferably Pepipost:), we have added a guide that can help you make the switch easier.

Reputation

Reputation for an email sender is similar to a credit score for a person. If the score is good, Mailbox providers respect your emails and deliver most of them to Inbox. If it isn't, your emails land in spam.

There are 3 types of reputation that mainly affect Inboxing: domain reputation, IP reputation, and content reputation.

Domain Reputation:

There are 3 domains in any Email that contribute to domain reputation.

1. DKIM signing domain: DKIM Domain is the authoritative signing domain of the email. It can be seen when we look at full headers of any email in the header called “Authentication-Results”.
2. Return-path domain: The domain used in the Returnpath header in the email.
3. FROM domain: The domain used in visible FROM address of email.

Gmail is a domain reputation heavy mailbox provider.

IP Reputation:

IP reputation is the reputation of the delivery IP of your mail stream. Lately, mailbox providers are moving to domain heavy reputation systems, but IP reputation still matters and it can have a direct impact on the Inboxing.

Content Reputation:
The body of an email also carries a reputation. While domain and IP reputations are measurable via the postmaster tools mailbox providers give, content reputation cannot be directly tracked. Instead, tt can be arrived at after multiple tests. Here are the usual pieces within the email content that contribute to content reputation.

1. Domains in the email: Link tracking domains, Image hosting domains, etc.
2. HTML structure and layout of email.
3. Text Phrases within HTML tags an email like alt tags.
4. Text Phrases in the content of email.

Building Reputation

Every sender who is sending more than a thousand emails a day carries a reputation. If you’re starting fresh, know that it takes a series of consistent good emails to build a reputation and just one bad send can ruin it all.

Inboxing is directly proportional to reputation. If your reputation is high, the probability of inboxing is high and if your reputation is low, the probability of inboxing is also low. To build and sustain reputation, you need to get 4 components right:

1. Data Collection
2. Data Segmentation
3. Content
4. Infrastructure

Data Collection is where you start the journey of building a reputation. The first question to answer is: Where are my users coming from?

As a sender, you need to look at every path a user can take to signup for your service. It could be social signups (Google and Facebook authentication), Manually entered email IDs, *Coreg signups, Third party opt-ins*, signup over an app, etc. Track them differently as each of these sources will show a difference in terms of responses, quality and might need a different treatment. Example: auto-authenticated signups like Google and Facebook are highly accurate as compared to manual fill of email ID where a user can enter a typo'd email address (like abcd@gmial.com). Beyond accuracy, Co-Reg and 3rd party opt ins will likely have different engagement patterns than 1st party opt ins. This is especially important in the jobs space where Co-Reg and 3rd party opt-ins can be fairly common.

Each of these signup sources should go through different journeys to ensure the final user is genuine. Example: Social signup user don't need to get a signup confirmation email again, but a manual form filled email ID should get one.

Data Segmentation and Targeting is your next pitstop in building a reputation:

The questions you need to ask in this part of the journey are:

- What email is my user getting as soon as he or she signs up?
- What's the average time the user is active with my job alerts before going dormant?
- What stage of the job search process is a user in - am I sending relevant emails based on the stage of their job search?

A crucial best practice to start a user journey is to send a welcome email as soon as the user registers. A welcome email should do the following:

- Welcome the user to your brand and email program.
- Tell different types of emails he or she is going to get as part of the email program and with what frequency? Ex: Daily 2 job alerts, 1 in the morning and 1 in the evening.
- User preference center link to manage subscription and adjust the frequency. Ex: User can select the number of job alerts they want to receive from you.
- Request the user to add FROM address to address book (and with instructions to add) so that user gets your emails into Inbox.

Tip: *Get the user to reply to your welcome email by offering an incentive for the reply. Example: Get 1-week access to premium resume repository by replying to welcome email. When a user replies to welcome email, the FROM address gets added to the address book and subsequent emails from that address would land in Inbox.*

If there are multiple mail streams that a user is going to receive, you might want to convey the message with a series of messages for each mail stream.

After a couple of weeks, collect feedback from users on the quality and relevance of job alerts being sent to them. Even if 1% of users respond, it still gives a signal for improvisation. We've even seen this done by some brands in real time with upvote (relevant job) and downvote (irrelevant job) buttons on every job which can help tailor your messaging and content to that particular user.

If a user has signed up, but not uploaded a resume or has not applied for a job, target these users with specific nudges to complete the action. Gamification is a great help here.

User activity on job boards is usually very high in the first few days when the user is searching for a job and it reduces after that. Knowing that the user has accepted a job offer and is no longer looking is very important so that you can target the user with different content than job alerts. Example: Salary comparison, How to make it large in a new role, goal setting, tracking, etc. This, in turn, reduces user churn.

Another way is to ask a user who's not looking for a job anymore if he or she wishes to snooze emails for a period of 6 months and resume emailing them again at that point of time. So, you are not losing the user completely, but also not getting dinged by the ISPs for emailing unengaged users.

What is my data suppression policy?
It's important to have a policy in place the spells out after how many days of inactivity, are you going to suppress the user from further emails. Before suppressing the user, you should collect feedback from that user as to why he's unresponsive suddenly?

Content Targeting is important, but a less addressed pitstop. Spam filters break down the creative into tens (in some cases hundreds) of components and calculate reputation for each of these components. If cumulative reputation for that creatives comes as negative, your emails will not see the light of inbox.

Let's assume that you have a first party organic email program from ESP A and a third party affiliate program to generate leads from ESP B. While the domains and IPs are completely

different, if you have the same creative running between these two providers, the badness of your affiliate creative will start infecting the organic program since they share the same signature.

Best practices to ensure your content is safe:

1. Have a unique design and layout for each of your email streams. Do not mix them up.
2. If your emails are bulking from your current ESP and you are switching, try to generate a unique creative for your new ESP volume so that you carry a different signature from new email program and it gives a fresh start.
3. Keep the creatives simple and responsive.
4. Do not overwhelm the creatives with a barrage of job listings. Users do not usually go beyond 20 job listings in a single email. Too many listings can get your email clipped at gmail so that user has no visibility beyond a certain point.
5. Keep the link re-directions to as few as possible. Ideally, the redirection should be an ESP's tracking URL and then target website. Every redirection loses 5-10% of users due to timeouts etc. Spam filters don't particularly like multiple redirects as that is what spammers usually do to hide the true website under multiple redirects. If you are an aggregator of aggregators, you should check your sources to see how many redirects are happening. It may be worth building likelihood of multiple redirects into your quality score algorithm and even ask your aggregator clients to break up sources into multiple feeds based on likelihood of multiple redirects. This should be fairly simple to do by breaking into Direct Employer, Staffing, Job Board and Aggregator feeds since each of these have a different likelihood of seeing multiple redirects.
6. Personalization to the rescue. Well personalized emails generate 40% more responses in general.

Different types of content we've seen job boards targeting their users with:

- Signup confirmation & Welcome series.
- Periodic Job alerts.
- Mid Out campaigns: Users who have not filled in the profile completely, get an alert to complete the profile.
- Transactional emails like Resume shortlisted, Interview scheduled, Job selected or rejected etc.
- Knowledge series : Resume writing tips, Average industry salary standard for the role user has applied for, Success stories, Tips to crack interviews, Complimentary educational courses that can enhance the current profile of user etc.
- Journey-based emailers: To track user journey within the system to carefully guide to execute the next logical step.
- Feedback Mailers.

How many different mail streams do you send?

Monitoring Reputation and email program in general:

The regular metrics to monitor reputation are the following
Inbox Placement rates: Track in your own seed accounts or use an external provider like G-Lock apps, 250 OK etc

Gmail Postmaster: Gmail has a postmaster page where every sender can track their domain and IP reputation at Gmail. Available at gmail.com/postmaster.

Returnpath's Senderscore: Senderscore is a score assigned to an IP on a scale of 0 - 100. 0 being bad and 100 being good. While the significance of sender score is reduced greatly these days, it still gives a sense of the quality of mailing going from an IP address. Especially, if you are on a shared pool, tracking this gives a deeper idea on quality of infra.

DNSBL Monitoring: MXtoolbox and MultiRBL are online tools where you can check if your domain or IP address are listed in any of the DNSBLs globally. While only a handful of them are really effective and impacts on reputation and IPR, others still give you a perspective.

Authentication: Ensure that your emails are authenticated properly, with SPF and DKIM pass.

Feedback Loop complaints: These are users marking your emails as spam in Gmail, Yahoo, Hotmail etc. The average has to be less than 0.1%, but note that mailbox providers do not and need not report all the spam complaints.

Open rates and Click Rates: The engagement metrics that need to be monitored are the number of opens and clicks to the total amount of emails deployed. Calculate the percentage for them and compare it to the industry standard.

Unsubscribes and Bounces: The number of unsubscribes, as well as bounce ids, need to be monitored as an increase in the percentage of these metrics will showcase as negative factors for mailbox providers and it will lead to a dip in your domain reputation.

While the above metrics are important to monitor, you should also track the following closely as possible.

Delivery Speed: If your email provider is delivering at 100K emails an hour, is it consistent or do you see any throttling by the mailbox providers. If a mailbox provider is throttling you, there is something negative about the campaign you deployed and it has to be looked at. If throttling is consistent, it will have an impact on performance, reputation, and deliverability.

Tools to monitor your reputation:

There are two different breeds of tools that can be used to monitor reputation - Mailbox providers own tools and third-party reputation monitoring services.

- Gmail Postmaster (http://gmail.com/postmaster/)
- Mail.ru (https://help.mail.ru/engmail-help/postmaster)
- SNDS (https://sendersupport.olc.protection.outlook.com/SNDS/index.aspx)
- Senderscore (https://www.senderscore.org/)
- DNSBL Check : https://mxtoolbox.com and https://multirbl.valli.org.

Industry Inboxing and Open Rates:

We've compared the performance of multiple job portals across the globe to understand the performance of each mail steam that can help you benchmark against the rest.

Type of mails	Inbox Placement Rates	Average Open rate
Signup Confirmation emails	97%	72%
Periodic Job Alerts	92%	16%
Mid - Out campaigns	90%	10%
Resume Shortlisted type trans emails	92%	47%
Knowledge Series	91%	9%
Journey-based emailers	93%	22%

Guide for switching ESPs

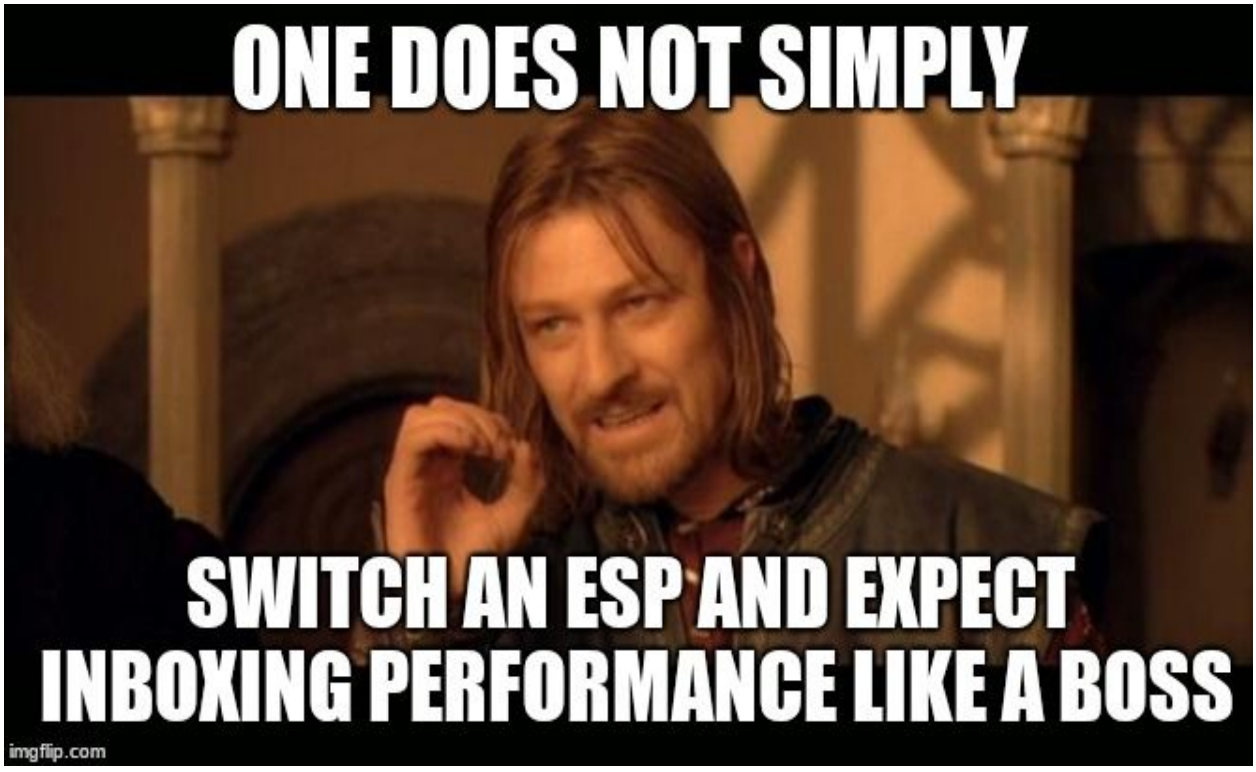
Having that exasperated feeling when the current ESP (Email Service Provider) you are using is not providing the best return to you in terms of your investment?

Has the inboxing percentage of your job alert emails dipped and you are witnessing the engagement metrics suffer? Is your current ESP not able to scale up on your overall database?

Is your company new to the Email marketing field and you wish to start out on the best possible foot to gain some website traction and conversion with your candidate users?
This guide is for Marketeers as well as Transactional mailers looking to switch their mailing vendor or those that are new to Email Marketing field and wish to start using an ESP.

The below points should help in terms of providing the guidelines to follow for smoother transition and keeping it stable for a longer period of time.

The guidelines have been created with an overall view of Email Marketing in terms of your marketing strategy as well as the Email Deliverability which would ensure that your new mailing platform is inboxing your mails.



One does not simply..Sean Bean knows it as well.

According to Return Path's Global Deliverability Benchmark [1], 600bn emails were categorised as spam in 2018, coupled with that , the continuous stringent changes in spam filters across ISPs , has made it more challenging for Inboxing mails.

The following points if followed resolutely will prepare you better for the upcoming transition and make it a win-win situation in-terms of ROI and inboxing with an onboarding ESP :

Address the pain points:

If you are switching your mail provider, you need to ensure that you don't commit the same mistakes as you did with the previous one. Therefore, you need to address the shortcomings and avoid the same footprints with the new vendor.

Whether it is the email ids you need to segment better or monitor and work with the domain reputation with ISPs, these weaknesses need to be removed with a fresh start from a new vendor.

Domain Matters:

If you were using a sending domain beforehand which was bad reputed and hence your mails were in spambox , or the domain did not have a good history with ISPs, it is prudent to change to a new domain with new provider. The new domain needs to be previously registered with a DNS provider for at least 90 days so that the ISPs will have some history to build on for this specific domain.

Get this domain re-directed to your website domain so that your users can directly associate your mails with your brand website.

If you do not have any previously registered domain, then you will have to register a fresh domain and get the DNS records added to it.

If the sending domain is not damaged but you were just not happy with your previous vendor's performance in terms of engagement or conversions, then you can continue with the same domain with a new provider, piggybacking on the already reputed domain you possess. In order for this strategy to be successful, you should stop mailing from the previous vendor completely and shift all the volumes to the new one.

Warmup for ISPs:

For any new domain or IP address to start sending your mails, they need to develop some reputation with different ISPs. The initial mailing needs to be done at a constant volume for the IP and the domain to be warmed up and attain a high reputation with different postmasters of ISPs eg: Gmail , Yahoo , Outlook etc.

You should be monitoring your domain reputation incase of Gmail on a day to day basis to check on any dips or spam complaints that could be hampering your inbox performance.

The warmup process should take a period of 21 days to 1 month depending on the volume which is expected to be mailed in a single campaign.

Factors for determining a successful warmup :

- Scale up on the active engaged users entirely in a single campaign eg; if your overall database is 500k then the ability to send 500k in a single day with 90% + inboxing.
- Good engagement metrics in terms of opens and clicks according to industry standards or above.

- Domain reputation is high in Gmail postmaster .

- The active ids targeted achieves good conversions / website traffic / leads etc for you to track.

Thus after having your IP and domain warmed up , you shall be good to go for resuming your regular volumes for sending campaigns and getting a sizeable conversion from them.

- **Target relevant data**:

The email ids that you shall begin with, should be your best performing segment of all your database. This segment should ensure that you are getting very high engagement from the start of your warmup process.

The targeting of data can be done generally the following order of preference:

1) Opens and clicks from your mailing in the past 30 days.

2) Latest registered / subscriber users for past 30 days.

3) Latest transacted users for past 30 days

4) The rest of the database for past 6 months, collected with permission from users.

Several segments can be done based on users, as they can be targeted according to their preference of products/information .

The entire blacklisted data from previous vendor needs to be provided to the new one for blacklisting at their end so as not to target these users.

Creative layouts:

The HTML creatives that you need to use for your campaigns from new vendor should be different than the ones used before and which have not performed. Following the same campaign format will continue the spam pattern with new domain as well as ISPs have a bad mailing history pattern with the old creative layouts which were spamming.

The creatives need to have a healthy combination of images + text (60/40) . You can also experiment with other types of layouts which suit your business requirements.

The footer needs to be a customized footer which has your brand name and an actionables for the users to set their preferences.

Mail Infrastructure:

When you switch to a new vendor, you need to ensure that all the DNS records are reflecting for the said domain and all the necessary settings (SPF, DKIM , DMARC, TLS) have been enabled for the mailing infrastructure.

What IP addresses have been assigned for delivery , are they shared or dedicated?

If they are shared, what is the percentage of distribution in volumes for that IP?

Email strategy:

It is paramount that the Marketeer lay out a plant for the following in terms of Email marketing strategy:

- What is your business objective with Email marketing?

- What do you wish to gain in terms of your campaigns? Is it just retention or acquisition as well?

- Do you have a proper campaign calendar prepared for a month of your upcoming promotions?

- What is the larger vision you are looking at in terms of engaging with your email users?

- Do you have a clear plan for engaging with your customers in different stages of the buyer's life cycle journey?

If you have these questions figured out , then it will be easier for the onboarding ESP to perform and work with you in terms of your objectives and requirements.

This is a key part which many Marketeers are oblivious to, but it plays a vital part in how you engage as a brand with your customers and build trust and a relationship with them.

Email Deliverability doesn't have to be a major challenge when shifting ESPs and if the above points are followed with proper co-ordination with your ESP, then it would be possible to maintain trust with your customers and build long lasting relationships with them through your campaigns.

References:

1. ReturnPath,2019, *The 2019 Hidden Metrics of Email Deliverability*, https://returnpath.com/downloads/the-2019-hidden-metrics-of-email-deliverability/

Appendix:

If you are not familiar with deliverability metrics, we suggest giving the below section a read through, but if you are already familiar, please skip to the next section.

Deliverability 101

Let’s get familiarized with the basics of email and why it’s important to understand them.

IP Address: IP is an address assigned to any computer on the internet. The server delivering your email will also have one or more IP addresses associated with it.

When you deliver an email from an ESP, you will be assigned one of two types of IPs:

Dedicated IPs: The IP addresses are dedicatedly assigned to you. If your sending volume is more than a million emails a month, you can choose to be on dedicated IPs. If it's over 10 million emails a month, it’s recommended that you’re on dedicated IPs.

Shared IPs: These IP addresses are assigned to you, but also deliver email for other brands. If you’re a small sender with less than a million emails a month, you can be on a shared pool of IPs. But, as a sender, you need to be aware of the quality of shared IPs you are on.

Sub Domain: For a domain called “example.com”, a subdomain would look like “email.example.com”.

DNS: DNS stands for Domain Name System. It's a framework that makes the internet a human-friendly place. Any internet connected devices are identified by an address called an IP

address (It looks like 23.55.11.22). DNS ties a human-readable name called domain (google.com) to the IP address. It is like a yellow pages book for the internet.

SPF: SPF stands for Sender Policy Framework. It allows the owner of a domain to designate IP addresses which are allowed to send emails.

DKIM: DKIM stands for DomainKeys Identified Email. It is an email authentication method that allows the receiver to check that an email was indeed sent and authorized by the domain owner. This is done by giving the email a digital signature. This DKIM signature is a header that is added to the message and is encrypted to make it secure.

DMARC: It stands for Domain-based Message Authentication , Reporting and Conformance. This is an advanced authentication technique which requires SPF and DKIM to fully authenticate an email and its origin. It is passed when SPF and DKIM record are passed and the owner of the domain can receive detailed reports of the domain from DMARC reports so as to prevent email spoofing.

Warmup: This is a process which needs to be followed for different mailbox providers (Gmail, Yahoo, Outlook, etc) when we are starting to mail promotional content from a hitherto unused domain or a domain which was inactive for a long time and is now being used to send promotional mailing.

We send a constant volume of emails over a period of time, increasing it steadily inorder to build reputation with ISPs for your delivery IP address as well as sending domain.

DNSBL: It stands for Domain Name System Blackhole List. It is used to curb email spamming. It is a software that maintains a list of ip addresses and domains location-wise who are spamming from that location. Due to the recurrent spamming, the entire network is blacklisted by the software.

Hard Bounce: It is defined as an email which is sent back to the sender as the email address is targeted is invalid.

Soft Bounce: It is defined as an email which reached the recipient email server but is sent back to the sender due to reasons like “the inbox of recipient is full “ or routing/network issues.

Spamtrap: Spamtraps are basically honeypot ids which are injected in a list by ISPs inorder to check if a particular sender is using third party agency lists and is a spammer.