relationship | one

A MARKETING GEEK'S GUIDE TO:

EMAIL DELIVERABILITY

A MARKETING GEEK'S GUIDE

ABOUT THIS SERIES

Email marketing is undoubtedly part of every modern marketer's daily life. While we all have experience with it, we may all struggle with a common battle - keeping our emails in the inbox. That's where this eBook comes in - it's time to tackle email deliverability.

There is a lot that goes into an email deliverability strategy, and it's not something you should go at alone. Lucky for you, our experts have you covered. At Relationship One, our mission is to "Inspire Success." We hope that reading through this eBook will inspire you to try something new, solve a problem you've been dealing with, or invent something that will take your marketing efforts to the next level.

Let our experts help you dive into an area of modern marketing that you're curious about and what the inspiration flood in.

A MARKETING GEEK'S GUIDE TO EMAIL DELIVERABILITY

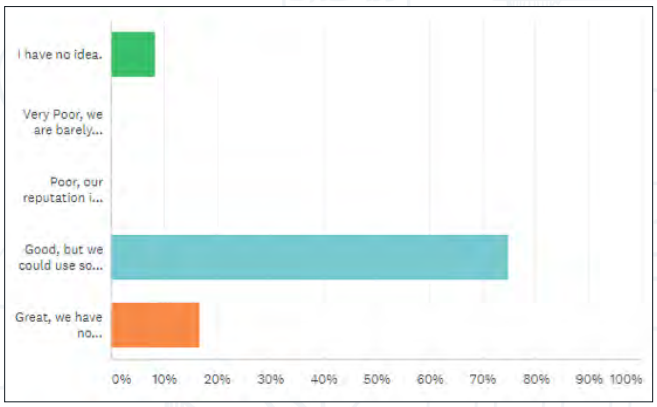
Email deliverability is a tough subject in many marketing organizations. While we know it's importance, achieving high deliverability seems like a near-impossible goal at times. With so much content out there giving tips and guidance, how does a modern marketer know where to begin? That's where this Relationship One eBook comes in handy. Let us do the work for you. We have assembled some of our best quality content on email deliverability to help start your journey. Let's get started!

CHAPTER 1:

WHAT DO YOU REALLY KNOW ABOUT YOUR DELIVERABILITY?

Few aspects of email marketing are more misunderstood than the art and science of email deliverability. Equal parts technology and logic, deliverability is a crucial component of an effective email marketing strategy.

We polled email marketers and asked them how they thought their company's deliverability was performing. Based off the results, the overwhelming majority could benefit from some improvements! Collectively, even as email marketers, sometimes we don't have the slightest idea on how our deliverability is doing, sometimes we need help, and then there are the few who are having no issues at all.



Here are a few essential tools and definitions that should stay in every email marketer's toolkit. Cheers to the inbox!

DELIVERED VS. DELIVERABILITY

In our survey, we asked email marketers to share their definition of "Deliverability". The results proved that more and more marketers are beginning to grasp the importance of this concept. Most participants responded with some iteration of "Making it to the inbox" – and this is absolutely correct!

"Delivered" refers to the number of emails that were successfully transferred to the intended recipient's mailbox provider. "Deliverability" is the measure (usually a percentage) of how many emails actually make it into the inbox.

The key difference here? The inbox. "Delivered" differs from "deliverability", because "delivered" does not necessarily mean an email made it to the inbox. A delivered email may end up in a variety of other places, such as the dreaded spam folder – but the label "delivered" does not specify that information. Conversely, "Deliverability" entails metrics for further analysis, such as open and click data, complaint data, and bounce data.

SHOULD I SEND EMAILS FROM A SUBDOMAIN?

Before we answer that question, let's discuss domains, shall we?

In the email world, we send from either an organizational domain or a subdomain. An **organizational domain** looks just like your website's domain name, such as "relationshipone.com". Receiving an email from a domain name address would show up as: example@relationshipone.com.

A **subdomain** is an extension of any particular domain name. It is created by adding a ".", or a period, with another word or letter: example@emails.relationshipone.com.

There are multiple benefits to sending from a subdomain:

- Subdomains allow a sender to separate different kinds of mail (i.e. transactional, marketing, activation), in an attempt to build and maintain separate domain reputations.
- Subdomains allow a sender to easily add DNS records.
- There is no minimum sending volume for a particular subdomain.
- A subdomain's reputation does not affect the organizational domain.

However, if you decide to create a subdomain, proper implementation is paramount. Be sure to set up SPF and DKIM authentication for each subdomain. Both **SPF records** and **DKIM records** are DNS txt records that will help add legitimacy to your subdomain in the eyes of major ISPs.

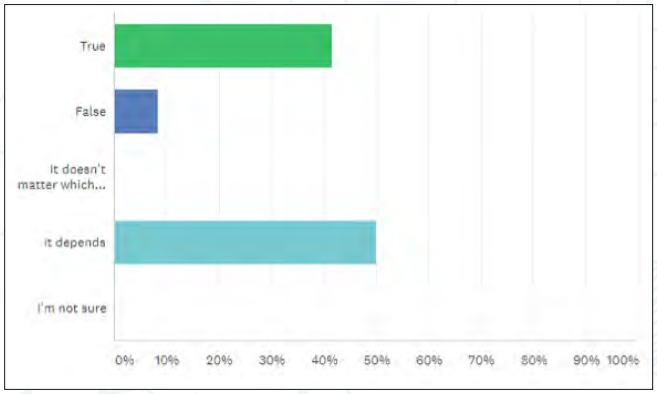
SPF (Sender Policy Framework) authentication specifies which IP addresses are able to send mail for a particular domain. **DKIM (Domain Keys Identified Mail)**, an encryption authentication method, confirms the origination of an email from an authorized network, and prevents spammers from stealing the identity of legitimate entities.

Once the subdomains have been created and authenticated, you can begin sending mail! However, we strongly discourage our clients from sending a mass email blast immediately on a new subdomain; that is considered spam-like behavior. In order to avoid looking like a spammer to ISPs, be sure to send to your list in small, gradual segments, slowly incrementing over a period of 2-5 weeks. We call this the warming process!

SHARED IP VS. DEDICATED IP

Which is better for deliverability: a shared IP or a dedicated IP?

This is a trick question. The correct answer is "It Depends." As we can see, half of survey participants answered correctly:



The decision to send from either a dedicated or shared IP depends on several factors:

SENDING VOLUME

We typically recommend a **dedicated IP** for higher volume senders:

- **B2B:** Minimum **100,000** emails per month
- **B2C:** Minimum **500,000** emails per month.

Lower volume senders would benefit from a **shared IP**.

SENDING BEHAVIOR

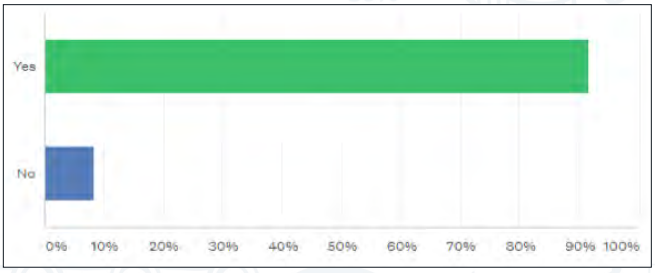
As the sole sender of a dedicated IP, you are the only one responsible for your reputation. If you're a good sender, that works in your favor! You have the authority to maintain your good standing.

BUDGET & TIME

As to be expected, a shared IP will be more affordable than a dedicated IP. A dedicated IP will also require a warming period that will take place over the course of several weeks – so if you're planning to switch, make sure you have ample time to warm!

HARD BOUNCES VS. SOFT BOUNCES

In the email world, a bounce is worth a thousand words. All email marketers should monitor and analyze both hard and soft bounces in order to gain valuable data about their sending infrastructure, campaign content, and overall inbox placement. Bounce logs are kept within your ESP or CRM and are often available to you upon request. Do you know what the difference between a hard and soft bounce is though? This was also a question in our survey.



A **hard bounce** indicates a permanent delivery failure. While an email could hard bounce for a variety of reasons, the most common causes are: an invalid email address, invalid domain, or a server rejection. We highly recommend reviewing your hard bounces and determining if they need to be suppressed from your list. It's important not to send to bad email address/domain addresses repeatedly! Retried delivery attempts will not reach the inbox and will negatively affect your reputation.

A **soft bounce** indicates a temporary delivery failure. Typically, a soft bounce will indicate whether:

- There could be a rate limiting issue
- The recipient's mailbox may be full
- The sender may be blocked by an ISP
- The message may be too large

UNSUBSCRIBE VS. COMPLAINT

As an email marketer, which would you rather receive from a subscriber: an unsubscribe or a complaint?

By far, an **unsubscribe** is the more favorable outcome. Not only is an unsubscribe option legally required for email marketing emails, it weighs far better on your domain's reputation than a complaint. Furthermore, it is important to place the unsubscribe link in a place in the email where it can be clearly seen by the recipient – not written in text that is the same color as the email's background or hidden in an image. If a reader cannot easily unsubscribe, they may complain in frustration!

Complaints occur when a recipient marks an email as spam. That recipient should be automatically removed from your sending list – for repeatedly sending to a user that has complained will cause ISPs and Blacklists to take notice and will negatively influence your reputation.

While complaints are unfortunate, they can be informative! Setting up a **feedback loop** is a wise way to monitor complaints. Feedback loops forward user complaints to the sender, allowing you as the sender to see the reason why they complained, (i.e. irrelevant content, too many emails, uninterested, etc.) and then make appropriate changes to your content, list practices, or sending behavior! Not all mailbox providers have a feedback loop, but most of the major ISPs do provide one.

FREE TOOLS TO MONITOR DELIVERABILITY

- **Google Postmaster Tools:**
  - Gives insight into your Gmail reputation
  - Monitors User Reported Spam, IP Reputation, Domain Reputation, Feedback Loop, Authentication, Encryption, Delivery Errors
  - https://postmaster.google.com/
- **Microsoft SNDS:**
  - Gives insight into your Microsoft reputation.
  - Monitors complaint rates, mail volume, spam trap hits, and filter rating.
  - https://sendersupport.olc.protection.outlook.com/snds/
- **Office 365 Header Analyzer:**
  - Provides insight into header values and reputation values for Office 365 emails.
  - Allows you to review BCL, SCL, and PCL values from Office 365.
  - https://testconnectivity.microsoft.com/?tabid=mha
- **Below are some other good sites to monitor your reputation:**
  - **Barracuda** – http://barracudacentral.org/lookups
  - **Proofpoint** – https://ipcheck.proofpoint.com/
  - **Watchguard** – http://reputationauthority.org/
  - **Webroot** – http://www.brightcloud.com/tools/url-ip-lookup.php
  - **Mailspike** – http://mailspike.org/iplookup.html
  - **Symantec** – http://ipremoval.sms.symantec.com/lookup/
  - **Trend Micro** – https://www.ers.trendmicro.com/reputations

The main point? Make monitoring your deliverability a priority.

Get familiar with the technical aspects of authentication. Analyze hard and soft bounces regularly to gauge why emails are not being delivered. Do your research before switching IPs or adding a subdomain. And finally, make it easy for users to unsubscribe. We want to send to people who actually want to receive our emails. Those will be the people who engage with the emails and help to build a good reputation.

CHAPTER 2:

THE TWO BUILDING BLOCKS OF EMAIL DELIVERABILITY

Organizations invest a lot of time, money, and heartache to craft the perfect campaign, but spend little time optimizing email deliverability. This isn't ideal. With only 85% of all emails making it to recipients' inboxes (2018 Deliverability Benchmark, ReturnPath), all that effort could be wasted when over 1 in 10 emails aren't even seen by your intended audience.

So what can you do to improve the chances of all your emails being delivered to the sweet, sweet inbox? When it comes to email deliverability, there are two things that ISPs want you to prove. These are:

1. Are you who you say you are?
2. Are you sending emails that people want?

PROVING YOUR CREDENTIALS

Because everyone uses email, email is one of the most common avenues for scams. And one of the most common methods used by scammers to con the public is phishing, where the scammer pretends to be from a reputable, well-known brand in order to get the target to reveal personal information. For scammers, it's purely a numbers game. The more emails they send out, the more likely they are to hit a target.

To prevent this, ISPs use a variety of methods to verify that the organizations sending large amounts of emails are who they say they are. If your marketing organization sends out a lot of emails per month on a dedicated IP (i.e. you have a branded email domain and internet address that is used solely for sending out your emails), you'll want to ensure that you use these verification methods. They are the first step to ensure that your emails are accepted by the ISPs for delivery into the email inbox.

Because these methods require changes to your organization's Domain Name Server (DNS), you'll need to work with your IT team to get them implemented. For Oracle Eloqua users on a dedicated IP, two of the methods (SPF and DKIM) should have been part of your Branding and Deliverability set-up; however if you're experiencing deliverability issues, it's always good to do a double check to ensure that everything is good.

SENDER POLICY FRAMEWORK (SPF):

This protocol uses a txt record on your DNS that lists the IPs that are authorized to send from your email domain. When ISPs receive an email from your platform, they check this txt record to ensure that the IP that sent the email is actually allowed to send on your behalf.

DOMAIN KEYS IDENTIFICATION MANAGEMENT (DKIM)

DKIM uses encryption to enable organizations to take responsibility for sending an email and lets ISPs ensure that the email hasn't been altered during transmission. It does this by using a pair of encryption keys, one kept privately by your organization, and another that is made publicly available to ISPs. When your platform sends an email, the private key is used to encrypt parts of the email's technical information (known as the header) to form a digital signature. When the email is received by the ISP, it reaches out to your DNS to get the public key, which it then uses to decrypt the signature. If the decrypted signature then matches the elements in the header, the ISP knows that the email hasn't been tampered with.

DOMAIN-BASED MESSAGE AUTHENTICATION REPORTING AND CONFORMANCE (DMARC)

DMARC builds upon SPF and DKIM to authenticate whether the email was actually sent from the owner of the friendly from-address. It does this by comparing the email domain in the from-email domain against the domain set in SPF and DKIM. It also provides a way for email senders to tell ISPs what they want to happen when an email fails this test and gives a feedback mechanism.

Note: DMARC set up is not included in standard Branding and Deliverability setups. It also requires a tool to process the feedback reports from DMARC

ARE YOU SENDING EMAILS PEOPLE WANT?

Outside of any technical issues that may be causing deliverability problems, your emailing behavior is going to be the key to getting your emails into your recipients' inboxes. Every time you send an email, ISPs use the results to track your sender reputation both of your email domains and the IPs. This reputation takes time to build and can be pretty easy to destroy if you're not careful.

Factors that ISPs use to judge reputation are:

- Sending Volume (Do you send a consistent volume of email? Spammers tend to have massive swings)
- Engagement (When you send emails, how do people engage with them? Opens and clicks are just a few of the metrics that contribute to this)
- Spam complaints (Do people hit spam when they receive your email? This is one of the reasons that making it easy for people to unsubscribe is vital. You'd rather they do that than hit spam)
- Hard Bounces (Does a high percentage of your emails consistently hard bounce?)
- Blacklist status (Does your IP or Domain appear on any of the industry lists of IPs or domains that send unsolicited email)
- Spam traps (Have you sent messages to email addresses that were set up to trap unsolicited emails)

As you can probably tell from this list, developing a strong sender reputation relies on elements that are firmly in marketers' control: Data hygiene and segmentation. Coupled with a solid double-opt-in process, there's a lot that marketers can do to ensure that their emails have the best possible chance of being seen.

Remember earlier when we mentioned Google Postmaster tools? Let's take a deeper dive.

CHAPTER 3:

STAY "IN THE LOOP" WITH GOOGLE POSTMASTER TOOLS

The dreaded spam complaint. If unsubscribes are email's version of breaking up, then spam complaints are the restraining order. Through these complaints, inbox providers can adjust their filters to better serve and protect their users. In return, certain inbox providers offer a process where email senders can receive notifications as these complaints come in, referred to as a Feedback Loop.

For those who've gone through Oracle Eloqua's Branding & Deliverability configuration process, the Oracle Deliverability team applied for all available Feedback Loops in order to have complaint data reflected in Insights (Spam Unsubscribe), as well as auto-magically opting respective complainers out from receiving future Oracle Eloqua communications.

Inbox providers included are:

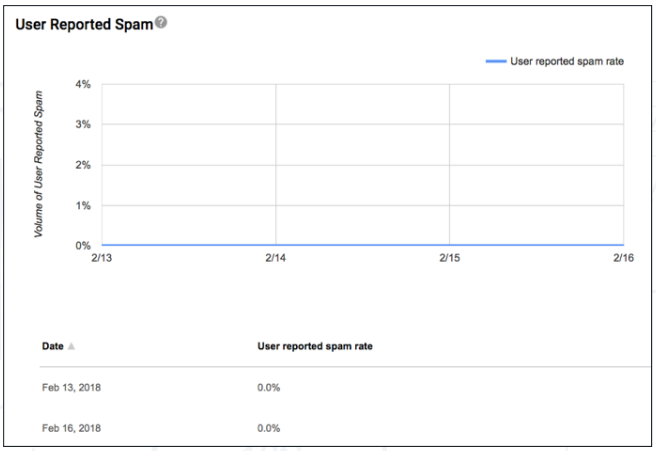
- AOL
- BlueTie
- Comcast
- Cox
- Earthlink
- FastMail
- Hotmail
- Laposte
- Locaweb
- RackSpace
- RoadRunner
- Synacor
- Telenor
- Terra
- Tencent QQ
- UnitedOnline (offers a Trusted Sender List)
- net
- Xs4all
- Yahoo! (requires DKIM setup)
- Zoho

For some Oracle Eloqua users, there may be a glaring omission, Gmail. This is due to Gmail not offering a traditional feedback loop. Although the opt-out will be reflected in your system, these spam complaints won't be present in Insight reporting*.

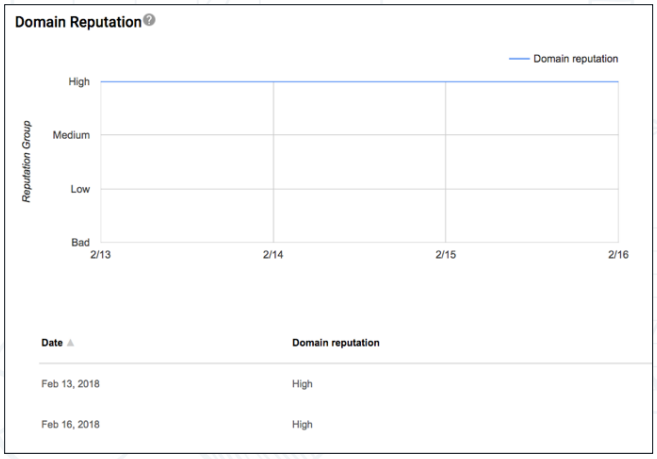
**Per Oracle, occasionally you may notice a couple of complaints appear in your reports for Gmail. These complaints are recorded when a recipient replies to a message with "spammy" words that their system senses and categorizes as a spam complaint. They add, this is a rare but possible scenario.*

So, how can one go about monitoring their Gmail performance? Well, for high-volume senders who leverage dedicated IP addresses (not shared range), you can monitor Gmail's Feedback Loop along with a suite of other diagnostic dashboards via Google Postmaster Tools (https://gmail.com/postmaster/). For traffic that passes SPF or DKIM authentication, you'll find data within the following dashboards:

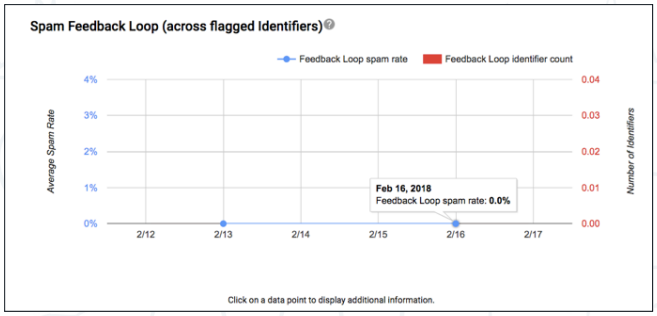
Spam Rate – highlights the volume of user-report spam vs. email sent to inbox (DKIM authentication required)



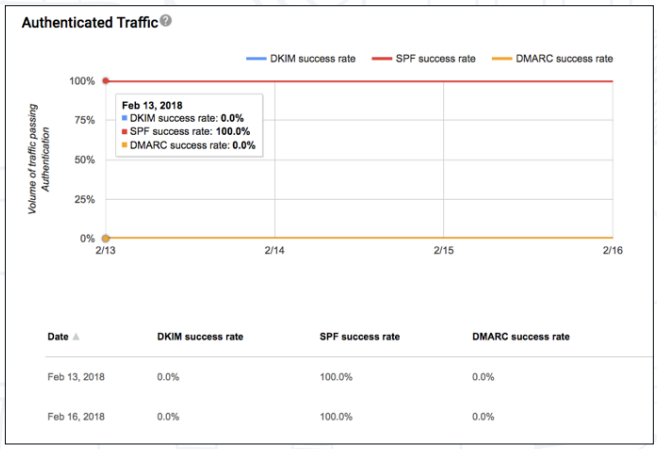
Domain & IP Reputation – insight as to whether Gmail spam filters might mark emails from Domain or IP as spam or not.



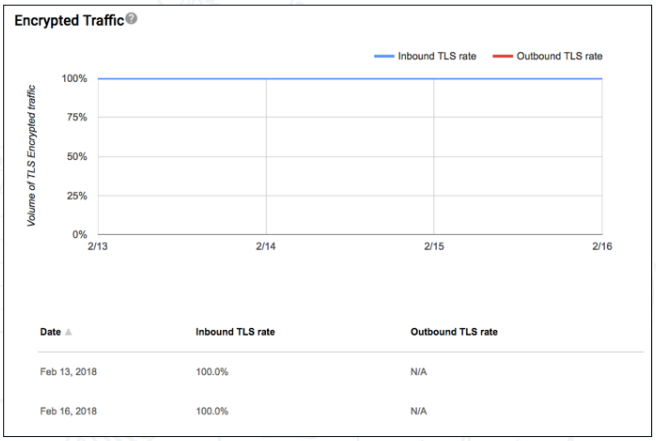
Feedback Loop – shows average spam rate across all identifiers flagged on a given day and the number of unique identifiers flagged by FBL per day (when applicable) over time.



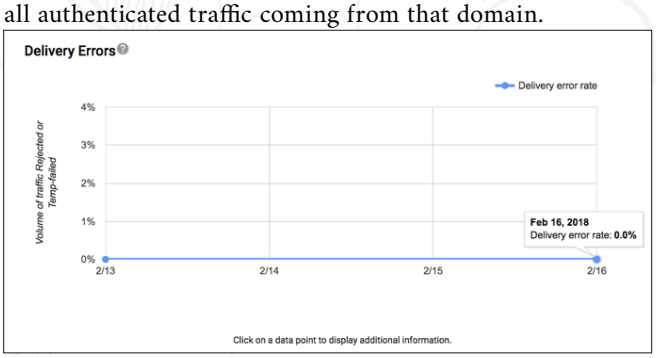
Authentication – captures traffic that passed SPF, DKIM, and DMARC over all received traffic that attempted authentication.



Encryption – features TLS encrypted traffic vs. all mail received from that domain, and consists of two distinct graphs within the same dashboard. By default, all Eloqua senders have TLS enabled for Gmail and all outgoing mail. There is nothing you need to do to enable this on your end.



Delivery Errors – presents rejected/temp-failed traffic vs all authenticated traffic coming from that domain.

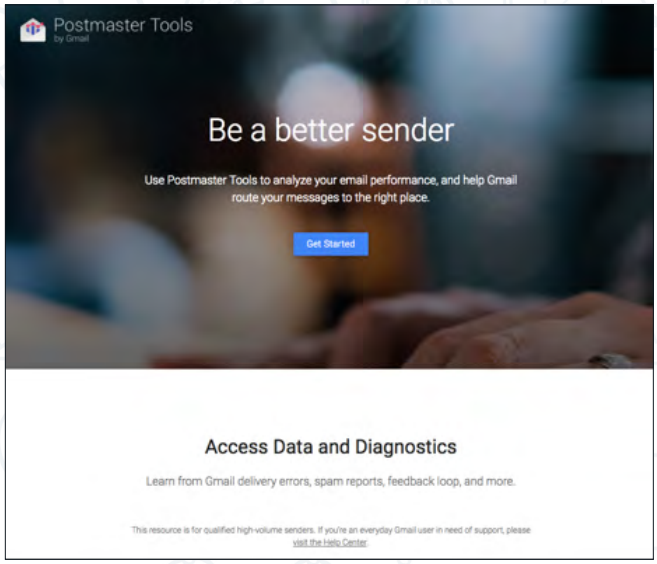


If you're still reading, you're now thinking, "great, how do we get setup?" If you have a Gmail account, then you have two options:

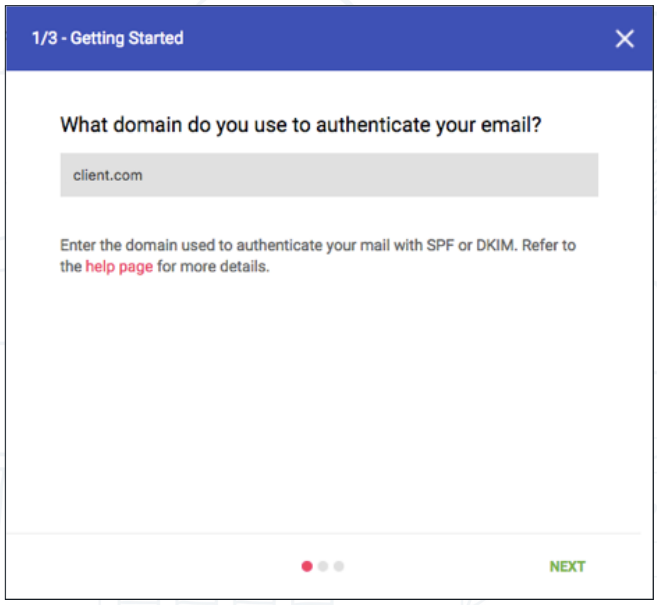
A. Oracle Deliverability Team – open an SR and request. They'll need the domains you require access to, your account short name, and the email addresses of all those who need viewing rights for these reports.

B. Set up Postmaster Tools yourself through the steps below (it's super simple, I promise):

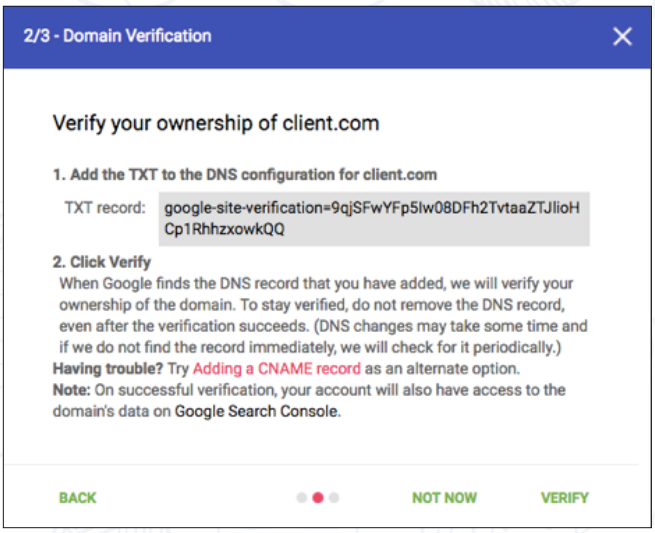
Step 1. Navigate to https://gmail.com/postmaster/ and click Get Started



Step 2. Enter the domain/sub-domain you use to authenticate your email (e.g. client.com, example.client.com).



Step 3. Copy the TXT record and add it to your DNS configuration. Once configured and propagated, click "VERIFY." Note, you can continue the Postmaster Tools configuration while waiting simply by clicking "NOT NOW."



Step 4. Once verified, give it a couple of days of high-volume sends in order for data to be reflected in Postmaster Tool dashboards.

Closing Tips/Notes:

- Once you verify your root domain via the DNS TXT records, you can add any subdomain without having to add additional records.
- Create a net new Gmail address to be shared by all users, rather than sharing your personal login information.
- To set expectations, note that the feedback tool only includes aggregated spam statistics, which cannot be traced back to the email address of the individual recipient who marked the email as spam.

As the adage goes, "it takes years to build a reputation and just minutes to ruin it," so stay at the forefront of your sender reputation with Gmail by utilizing Google Postmaster Tools.

WRAPPING THINGS UP

"You've Got Mail!" Or should we say, "Your Customer's Got Your Email – In Their Inbox!" You've done it, you've equipped yourself with some of the best tools and tips for email deliverability. Now, it's time to put them into action in your organization. You'll never worry about your customers missing an important message again!

We always love teaching and encouraging our fellow modern marketers. If you are working on email deliverability strategies and are looking for some assistance, please contact us. We would love to help out!