



The 2024 Guide to *Email Deliverability*

HOW TO ENSURE YOUR EMAILS
ARE ALWAYS LANDING IN THE INBOX

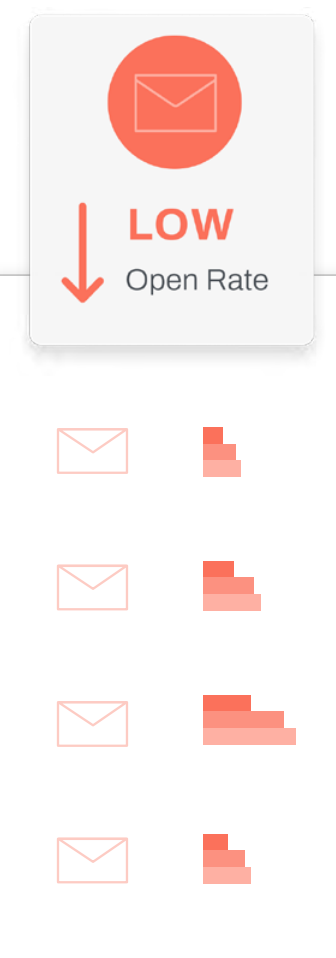


Have you ever looked at your campaign reports and scratched your head wondering why your open rates on otherwise top-performing emails look so... blah? We've all been there.

But before you start to question and reinvent your email marketing strategy – you need to look at how well your deliverability is performing.

Deliverability has become a hot topic after inbox providers like Gmail and Yahoo are beginning to enforce stricter policies for deliverability in February 2024. We'll get to that and more in this eBook.

Let's dig in.



Deliverability can be a tough nut to crack – especially depending on your level of technical expertise. One of the most common misconceptions about deliverability comes down to the definition itself. There's actually a *big difference* between **delivery** and **deliverability**.



Email Delivery

which you can easily see in your standard email reporting – shows you an email was successfully delivered to the sender. But, before you get excited, that doesn't mean the email actually landed in the inbox. An email campaign could show up on surface-level reporting as delivered, but if your spam rate threshold is high or your domain is blocklisted (formerly known as blacklisted), your emails are landing in email purgatory – somewhere behind a firewall never actually getting delivered to the recipient's inbox.



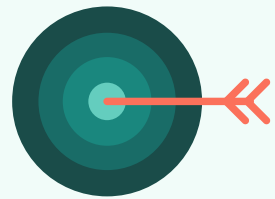
Email Deliverability

which is determined by a host of factors like sending volume, bounce rates, spam complaints and spam traps – is when the email successfully arrives in the person's inbox. It has passed all of the compliance and sending reputation checks with flying colors and is ready to be opened. It's important to note, when we say inbox, we are talking about spam folders too. Bad sending reputation – and a slew of other factors you're about to learn all about – prevents your emails from ever making their way into any part of your inbox.

In this 10-minute guide, we're going to walk you through everything you need to know about email deliverability to ensure your recipients are getting the messages you send – and you're not leaving money on the table.

Deliverability – *The Unsung Hero of Email Marketing*

Deliverability might not be the *coolest* aspect of email marketing, but it certainly is the most important.



In 2023, about **85%** of marketing email sends actually make it into the inbox.

If 25% of your revenue comes from email marketing campaigns, and one in six of your emails aren't being delivered, it will have a massive impact on your bottom line – not to mention skew your understanding of your marketing performance.

Deliverability is determined by a few different factors, including the engagement of your subscribers, the quality of your lists, spam traps, the volume of emails you send and the content within the emails themselves.

Altogether, these factors result in your sender reputation score or IP score, which is used to determine how internet service providers (ISPs) treat your email stream.

Your sender reputation score is *oh-so important* to the success of your email campaigns. The higher your score, the higher the chances your emails land safely in the inbox. The lower the score, the more likely it is that a significant percentage of your emails aren't getting delivered to your intended audience.

The best part about email deliverability and sending reputation scores is – it's totally fixable. It takes time, patience, and hard work, but you can strive to increase your deliverability rates by percentage points over time.

Before we can explain how you can fix it, let's first do a refresher on how email is delivered in the first place.



Email Deliverability *Explained*

Once you hit that send button on an email campaign, your email begins its journey to the inbox. The first obstacle it must pass through is the recipient's internet service provider (ISP), think Comcast, AT&T, Time Warner Cable, Cox Communications and Verizon (if you're in the U.S.). The ISP will accept the email as fast as possible on a first-come first-serve basis. The ISP requires your "to" field to be properly configured on your domain name system (DNS), which is used to identify the recipient's address.

From there, the email is inspected by the recipient's mail filters, as well as checks for the sender policy framework (SPF) and DomainKeys Identified Mail (DKIM) authentication, the email's header and content, blocklists and sending reputation score.

This is where things can get funky. It's within all these security checkpoints where risky emails, and straight-up spam, are blocked from entering inboxes.



Each checkpoint determines whether mail should be accepted by their network and delivered to the end user's inbox or junk folder. We are here to help you land in everyone's inbox.

But here's the rub – everybody has different email domains, ISPs and mail filters depending on their email address. This is why deliverability can be such an undertaking if you're struggling to improve your reputation scores.

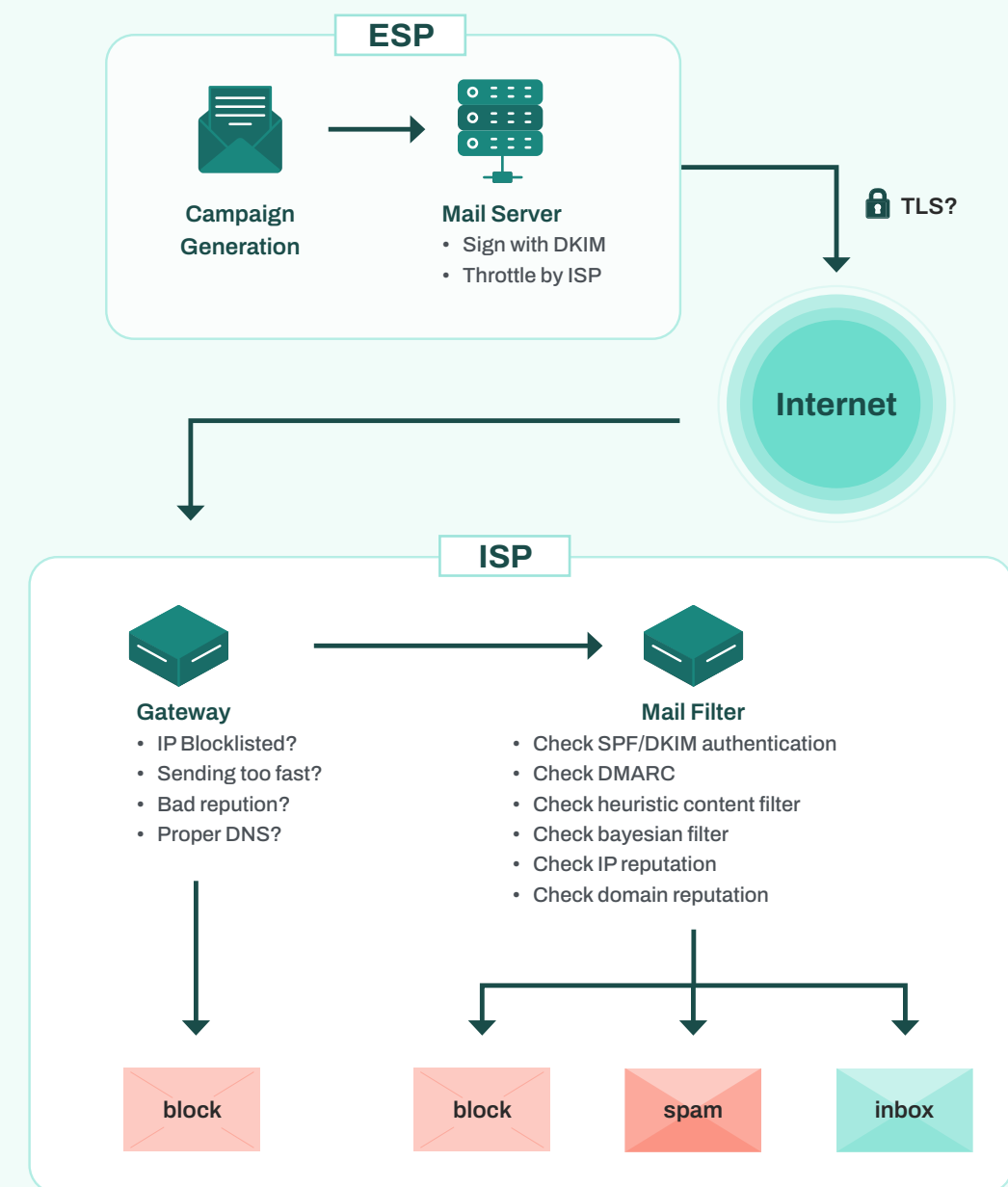
Let's say you're a restaurant and you get a lot of lunch orders from a nearby government contractor. They signed up for your mailing list using their work email because, to them, it's where they go to lunch when they're in the office.

A government contractor is going to have way, way tighter security controls than your typical customer who signs up with their personal email account, likely Gmail, Yahoo or another "free" mail provider. They might block emails that are full of large image embeds or ban emails that seem *spammy* when scanned.

As you can see, both have controls, but some domains have stronger ones depending on who owns the security of the domain.

So, you have to account for all of these nuances when you're starting to evaluate the current state of your deliverability and what improvements you need to make to get you where you need to be.

Though it may only take a few seconds, every email takes a complex journey to the inbox. [Here's what it looks like](#) ►



A Quick Overview of

Sending Reputation

Just as a person can be identified through a document like a passport, any device connected to the internet, from a cell phone to a smart appliance, will possess its own identification called an IP address.

Every email server has a unique IP address, which is used by inbox providers such as Gmail, Yahoo, and Outlook to identify, assess and evaluate the origin of an email, as well as attribute a reputation to that IP based on factors such as:

- IP age
- IP location
- Content
- Email volume and frequency
- DNS pointer records (PTR)
- Listed on any significant blocklists

Over time, your IP will build its sending reputation, which directly impacts your deliverability rates. For example, a high percentage of subscribers marking an email as spam will damage the IP's reputation, leading to low email delivery rates and harm your brand's marketing efforts.

Things like Apple Mail Privacy Protection (Apple MPP), easy-to-abandon temporary email addresses and inbox-protecting link bots have made maintaining a positive IP/sending reputation a bigger challenge than previous years. Hence why deliverability is critical to your email marketing success.



How to monitor and improve *reputation management*

Whether your reputation score is high or low or somewhere in the middle, it is vital to keep your fingers on the pulse of what's happening on a weekly basis. Here are some really, really important factors to monitor as you work to improve your sending reputation and deliverability rates.

- **Proactively monitor open rates at top domains.** Open rates should be consistent across the top ISPs. If one is significantly lower than the rest, you may have an inboxing issue at that particular ISP. Google Webmaster Tools is a free and powerful tool you can use to understand and monitor your sending reputation scores, and offers tips to improve your deliverability.
- **Keep a very close eye on critical blocklists.** If a sender appears on certain blocklists, the ISPs will flat-out block their entire mailstream, even if they're otherwise regarded as a healthy sender. You can check how your domain is performing across all critical blocklists using free tools like spamhouse.org and mxtoolbox.com.
- **Be mindful of spam traps.** Designed to catch spammers red-handed, spam traps are operator-maintained email addresses that, in many cases, have never been opted into a sender's list. Other spam traps are recycled, meaning that they signed up to receive emails, but abandoned for a significant length of time, causing the ISP to bounce. Recycled spam traps are generally indicative of an old, poor-quality list. Either way, continually messaging these addresses and routinely hitting spam traps will lead to a blocklisting.



Our best piece of advice is to continuously clean your email lists and only send emails to engaged contacts.

Engaged contacts are defined by your organization based on the volume of emails you send in a given period of time. If a contact has opened and/or clicked on an email within a period of time, you'd define that individual as engaged. Some organizations will remove contacts from lists after three months of disengagement, others are comfortable with sending emails to disengaged contacts for six months to a year – depending on their email frequency and reputation.

Breaking the rules will result in a poor sending reputation, blocklisting and a slew of issues that will impact your deliverability.

Looking at *List Management*

Since engagement is a universal factor in deliverability, list management is exceptionally important.

Email marketers need to manage and maintain their email contact list the same way you manage cleaning out your refrigerator. Old, disengaged email contacts are a lot like produce. If you push them to the back of your fridge and forget about them, they're going to spoil and create a messy cleanup.

Open rates are one indicator of your sender reputation and something everyone on your email team can monitor. If your open rates start to dip below 10%, that's a red flag for low engagement. An engaged list will typically see click-to-open rates north of 15-25%, with low opt-outs and abuse complaints. Don't assume open rates drop because a subject line has failed to get the engagement level you projected. Often, it's a sign to clean up your lists and understand where your engagement is falling flat.

Here are some recommendations to help you better manage your lists if you see your open rates drop.

- **Keep your lists healthy and up-to-date with suppression lists of inactive subscribers.** Yes, this does decrease the size of your list, but removing inactive and disengaged subscribers also drives up open rates and inbox placement. On the flip side, poor list quality hurts your inbox chances. Done right, list segmentation helps you send the right message to the right customer at the right time. If you're casting and blasting emails to your entire list every time you send – and seeing bounce backs and low engagement scores – you are hurting your sending reputation. It's best practice for senders to suppress inactive emails between three months and one year of inactivity, though the right time frame depends on your business model, open rates, frequency of sends, list source and age of data.
- **Pay careful attention to your user acquisition flow.** Make sure you give your subscribers a compelling reason for them to have opted in to your email, rather than forcing them to give their email address. Be upfront and clear about the types of messages to expect and the volume they will expect to receive in a week or month. They are agreeing to give up their information in exchange for something of value – don't tarnish the relationship by sending them emails 3-5 times a day if that is not what they are expecting.



- **Ensure your contacts have given the correct email address.**

Given the ease of typos, it's also important to double-check addresses for obvious keyboard mistakes, such as "gnail.com." Segment out the emails with typos and suppress those contacts when you send. If you're seeing a high volume of typos in the suppression list you create, think about asking folks to confirm their email address when they subscribe to your emails.

- **Do not purchase lists.** Purchasing lists is a huge no-no in email marketing and brands who are still purchasing lists will continue to see poor deliverability and high spam rates. Buying email lists results in high bounce rates, low engagement and ultimately compromises your integrity with the group of subscribers who did opt-in. Plus, to preserve their own sender reputation and business, most reputable email service providers (ESPs) won't allow you to send emails to email addresses that have not opted-in.

With this knowledge in mind, we have a few checklists you can use to understand where your deliverability stands, improve your inbox placement and send more targeted emails to the right contacts.

If you've found your business in a messy list situation, be patient as you work towards cleaning up your lists and improving your sending reputation. The rule of thumb is, however long it takes to get into a messy situation is about how long it will take to resolve.



Email campaign Checklist

While deliverability largely happens behind the scenes, the content of your messages does play a factor. Here are some best practices to keep in mind:

- ☐ **Make sure your HTML is compliant with the World Wide Web Consortium,** AKA the internet's main standards organization. Better known as W3C, the group's website has a helpful validator tool you can use to double-check your HTML files.
- ☐ **Avoid JavaScript in the message body.** JavaScript isn't naturally compatible with email, it may not load properly, which will diminish your deliverability chances.
- ☐ **Mix up HTML and text, rather than using one giant image.** We know it's tempting to pop in a big image you know will look great across all browsers, mailbox providers and devices. But you're putting your deliverability at risk when you're sending an email with one image file, rather than including text. ISPs flag these emails as risky and, as a result, might not make it into the inbox.
- ☐ **Use a consistent, branded "From address"** that sits on your domain.
- ☐ **Add alt text to every image.** Depending on the inbox provider, your images might not load. An alternative text image helps the reader understand what you're showing them in the event it happens.
- ☐ **Remember the ideal message width is between 600 and 700 pixels.** Your email marketing solution will recommend the exact measurements. If you throw a 1200 pixel graphic into a 600 pixel wide email, and the email technology provider isn't resizing them, the inbox provider will distort the images to full screen... which doesn't look great.
- ☐ **Never use link shorteners.** Branded short links like Goo.gl and Bit.ly are an easy way to track clicks, yes. However, they're very popular with spammers looking to direct people toward malware and viruses. As a result, they're less popular with ISPs and often blocklisted.

Email campaign Checklist (cont.)

- ☐ **Avoid images hosted on shared domains.** Using image files hosted on shared domains carries over the sending reputation of all domains with access. They're often used by thousands of senders and if one of them is on a blocklist, that can impact everyone else. The easy fix here is to host your emails within your email marketing platform to ensure pristine deliverability.
- ☐ **Optimize your subject lines for engagement and delivery.** There are a lot of dos and don'ts when it comes to subject lines and spam complaints. Make sure you're following the rules when you're writing subject lines. It goes without saying – no one likes a bait and switch, so make sure your subject lines aren't clickbait. If they are... you're putting your brand at risk for spam complaints.
- ☐ **Include a proper business name and address, as well as a functioning and easy-to-spot unsubscribe link.** Ah, yes, CAN-SPAM is still alive and well, but don't forget to adhere to this compliance mandate. Pretty much every single email sending provider covers this action for you. If you're setting up a new email marketing solution for the first time, this is a critical step.
- ☐ **Adhere to Google and Yahoo's new inbox privacy protections,** going into effect February 2024. There are three new requirements every bulk email marketing sender (more than 5,000 emails a month) needs to adhere to. We have an entire eBook dedicated to helping you understand how to address these changes. The TLDR version is you need to:
 1. Add a one-click unsubscribe script to the header of your emails
 2. Keep your spam rate score below 0.3%
 3. Enable two-day unsubscribe turnaround times – previously 10 days

CHECKLIST

Reputation Management

We cannot stress this enough: it is very important that your email lists contain contacts that have explicitly subscribed to receive communications from your brand. And, it is even more important that the messages you send your subscribers are what they agreed to in the first place. When you start to blur the lines between what people signed up for and what you're actually giving them – you are putting your reputation at risk. It takes one email and one click of a spam complaint button to damage your sending reputation.

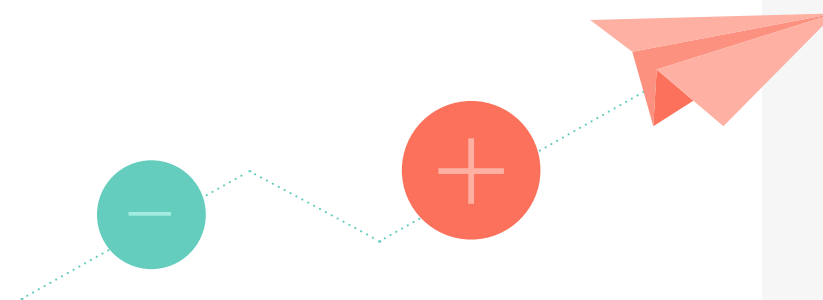
- ☐ Proactively monitor all email sends, inbox deliverability rate and spam complaint rate.
- ☐ Enable real-time ISP block alerts.
- ☐ Monitor critical and impactful blocklists 24/7.
- ☐ Monitor drops in delivery rates and open rates. Look for changes in open rates at top ISPs to ensure your mail is delivered to the inbox and not the junk folder
- ☐ Ensure you're following the ISP's acceptable usage policies, as well as any legal regulations.

CHECKLIST

List Management

List management is a critical component of deliverability. It's up to you to manage your list, and build segments for engaged contacts and segments for ideal customer profiles. Here are a few tips to better manage your lists.

- ☐ Always track acquisition source and audit trail of permission.
- ☐ Use reCaptcha on sign-up pages to prevent bots from attacking your forms.
- ☐ Ask subscribers to add you to their safe senders list or address book.
- ☐ Review hard bounces so you keep your overall bounce rate under 1%. This is especially important for welcome series, as these messages are the first touch and will likely have the highest hard bounce rates.
- ☐ Generate reports to provide insight into bounces, complaints and unsubscribes... and use those reports to segment and remove folks from your lists.
- ☐ Use a preference center to capture user preferences and allow subscribers to manage the frequency and types of emails you send.



GOOGLE/YAHOO CHECKLIST

February 2024 Inbox Privacy Changes

On October 3, 2023, Google and Yahoo announced three big changes bulk senders (individuals and brands that send more than 5,000 messages a month) must comply with by February 2024. These changes include new standards for:

☐ Email Authentication

Starting in February 2024, all bulk senders must set up SPF and DKIM and publish DMARC policies. If you're unsure of how to configure your SFP, DKIM, and DMARC policies, we recommend you speak with your IT team. This is set up on your company's domain name system (DNS), which is typically managed by IT.

☐ Unsubscribe links

Gmail and Yahoo announced recipients must be able to unsubscribe with ease – and senders must process and honor unsubscribe requests within two days. All bulk senders must adhere to specific one-click unsubscribe protocols, which include adding a specific one-click unsubscribe code in your email headers.

☐ Spam rate thresholds

New spam rate thresholds are coming. According to Google, all bulk email senders must establish and stay below a “clear spam rate threshold of 0.3%” in order to be delivered to inboxes. Meaning if your spam rate threshold is more than 0.3%, your emails will never even make it into the spam folder, let alone an inbox. Yahoo also announced they will also enforce this spam rate threshold.

Most of these changes have been best practice for years. By following the recommendations in this guide, and working with your email marketing provider (hopefully Marigold!), you'll be able to handle this disruption with ease.



Wrap Up

We're quick to dismiss poor email performance as a failed campaign without considering if the open rates, click-through rates and performance numbers are low because a large percentage of emails say they were delivered but are stuck somewhere between you hitting send and landing in the inbox.

If deliverability isn't a top priority in 2024, it needs to be.

Any dip in deliverability will translate to a dip in sales, sign-ups, conversions, views, or whatever the end goal of your email may be.

Don't forget. Data and privacy rank among the top concerns for both consumers and brands as they navigate the new world of email marketing. Remember, your subscribers want to hear from you – that's why they signed up for your emails in the first place. If you respect the value exchange and share information, promotions, offers and content they have expressed interest in – your sending reputation will improve over time. If you choose to collect email addresses and aggressively send subscribers campaigns without them understanding what they were receiving in the first place – your deliverability is going to plummet.

Don't leave money on the table. [Contact Marigold](#) to learn how we work with organizations of all sizes to improve their email marketing deliverability and reach the right audience with the right offer.

Where *relationships* take root.

Marigold's approach to relationship marketing stands alone in a world of one-size-fits-all marketing technology companies. Our solutions are designed for your specific size, industry, and maturity, giving you the technology and expertise you need to grow the relationships that grow your business, from customer acquisition to engagement to loyalty. And, with a team of strategists that provide insights into what's working, what's not, and what's changing in your industry, you're able to maximize ROI every step of the way.



Glossary of Terms

Bounce: When an email is undeliverable, it bounces, which can fall into two categories:

- **Soft Bounce:** These occur when the ISP is blocking your email due to reputation issues or because of something temporary, like a full inbox or a down server. If you see a major spike in soft bounces at any ISP, you should address it immediately. Users who have soft bounced are still valid and should be included in your next send.
- **Hard Bounce:** When you send a message to a nonexistent or invalid email address — think typos or a deactivated account — it will hard bounce. This is a permanent failure, and a metric that factors into sender reputation, so these users should be removed from your list.

Delivered: A message is considered delivered when the ISP has successfully accepted the message. This does not equate to the message being delivered to the inbox, however.

Domain: Referring to the locations of servers and devices connected to the Internet, domain names can represent various IP addresses, such as sailthru. com.

Domain Name System (DNS): This system maps a human-friendly domain name into a server IP address, almost like a telephone book. An MX type DNS record specifies where mail destined for a particular domain name should be sent. A TXT type DNS is used to contextualize information about the domain for authentication purposes.

Domain-Based Message Authentication, Reporting & Conformance (DMARC): DMARC allows senders to see how their domains are being used to send email and tell the world how to handle illegitimate messages they appear to have sent. Sitting on top of SPF and DKIM, DMARC is used to eliminate fraud and can protect senders and subscribers from phishing and spoofing.

DomainKeys Identified Mail (DKIM): This is used as a form of authentication to digitally sign a message, ensuring the sender has permission to use the domain and that the message wasn't tampered with in transit.

Glossary of Terms

Email Service Provider (ESP): Allows brands to send email campaigns to a list of subscribers. Subscribers opt into the list through what is known as the value exchange.

Feedback Loop: For the ISPs that offer this service, feedback loops allow senders to receive a report every time someone marks their email as spam or junk, helping them identify issues early.

Inbox Placement Rate: When mail is accepted into an ISP's network, this figure refers to how many messages are delivered to the inbox.

Internet Protocol (IP): A number assigned to any device that's connected to the Internet, your IP address is how the ISPs identify you and your server.

Internet Service Provider (ISP): An internet service provider (ISP) is a company that provides access to the internet. ISPs can provide this access through multiple means, including dial-up, DSL, cable, wireless and fiber-optic connections. Companies include Verizon, Comcast, AT&T and Time Warner Cable.

Sender Reputation: This is literally a score tied to you as an email sender, dictating the majority of email filtering.

Sender Policy Framework (SPF): Identifying whether a sending server has permission to send mail from a particular domain, SPF is used to authenticate the Return- Path From address, which normally only appears in message headers.

Subdomain: This is an extension of a brand's web domain, usually email.brand.com. Typically used for a brand's marketing emails, subdomains are often seen in the "from" address.