SocketLabs™
the science of hitting the inbox

The Science of Hitting the Inbox

How your Choice of Platform and Best Practices Drive Email Deliverability Excellence

Email is more than a fact of business life. It's both the engine and the fuel for commercial engagement of all kinds. And, it's more problematic than ever.

Poor email practices and bad email actors have pushed the major platforms to police their traffic to the point that 20% of the world's legitimate business email is excluded before it gets to its intended recipient. That number is growing as spam, phishing scams, cyberattacks, and lax or nonexistent corporate policies force the likes of Google, Microsoft, and Yahoo to consistently ratchet up, calibrate, and evolve their filters, blocking techniques, and AI rules. They have literal armies of strategists and technologists defending their customers' mailboxes. So, what are you doing to get your millions of varied types of messages safely delivered through the fray?

If you're managing your email efforts in-house, you probably don't have your own army to fight back. Even if your overall delivery rates seem stellar, it's hard to know if it's enough, or what opportunities you are missing. What pockets of your business are less than optimal? At what cost? And how well are your email practices maximizing service levels, revenue, and ROI?

Perhaps you are seeking help from email service providers (ESPs). But, ESPs are not all the same. Sure, they all run email software on their own servers and infrastructure. And, yes, most manage and monitor performance around the clock. But, what ultimately separates one provider from another is **two important factors:**

1. The technical innovation of their solution(s)
2. The collective strength of their software and service delivery strategists in driving adherence to industry best practices

"Your choice of 'platform' and 'best practices' make all the difference in your email delivery success. Combining these with service excellence creates the ultimate communications experience."

In short, it is your choice of platform and best practices that make all the difference in your email delivery success.

Whether you manage email delivery in-house or via an ESP, successfully addressing these critical areas will help you:

1. **Grow and strengthen your sending reputation**
2. **Optimize the time and resources you spend on email delivery and analysis**
3. **Coordinate your high-volume email traffic for maximum ROI**
4. **Relieve the pressure of keeping pace with constant inbox and spam filter innovations**

Being with a provider who delivers responsive, personalized service further ensures the ideal environment for email communication success.

Put simply, your email deliverability depends on your IP reputation – a real, honest-to-goodness score that is consistently monitored and updated by the mailbox providers. This score, which is all about demonstrated and expected trust, determines if your email makes it to your recipients' inboxes, hits the spam folder, or is blocked altogether. You should think of your IP reputation score like an "email credit score" for two reasons:

1. **There are many factors (controllable sending choices) that contribute to your score**
2. **There is almost always room for improvement**

Platform

If you are trying to find a suitable long-term ESP partner, there are several important platform qualities that contribute to your sender reputation and help drive deliverability rates higher. They are:

- ✔ Technical maturity and reputation strength
- ✔ Message encryption for security and privacy
- ✔ Comprehensive authentication support
- ✔ Stream-level performance tracking and optimization
- ✔ Continuous flexibility and scalability

Technical maturity and reputation strength

Experience is everything when it comes to learning and adapting to the rules of email delivery. System availability and stability are critical but should be considered bare minimum qualifications. What you should really be looking for is an ESP that boasts experience in and for different industries, use cases, and workflow complexities. The multi-layer needs of an agency are different than those of a SaaS application. And if your development team will be building workflows around your email functionality, you need to ensure that your APIs can support customized data handling. Sending reputation is further enhanced by adherence to email management rules, such as CAN-SPAM and European GDPR regulations, so look for a compliant ESP. Finally, ESPs must actively manage their platforms to remove any mail activity that violates best practices.

"An ESP platform with a solid track record provides immediate deliverability benefits. These include a proven sender reputation and intelligent traffic shaping – based on machine learning – for tailoring deliveries to mailbox providers."

Message encryption for security and privacy

The large-scale mailbox providers make the rules. If that isn't clear yet, it's worth formally stating now. And, large-scale mailbox providers have been pushing for email encryption for more than five years.

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are methods of encrypting traffic while in transit. TLS is the successor to SSL, but the differences are negligible in most cases. By using SSL/TLS to protect your email, you maintain the confidentiality of information in your messages while in transit. With the power of Google behind it, adoption is increasingly widespread. In fact, the company's data from the start of 2014 shows a near 100% growth rate in SSL/TLS implementation across its mail streams. So, your ESP of choice needs to be knowledgable in this area, too.

Platform

Comprehensive Authentication Support

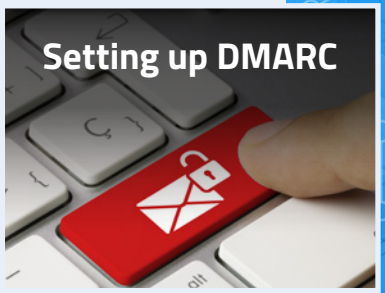
There are two additional steps your ESP should be taking to tighten up the security of your messages in transit and build your sender reputation. These are:

1. Implementing DKIM and SPF Authentication
2. Setting up DMARC

DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF) are forms of email authentication. SPF proves to ISPs that your mail is from you, and you are who you say you are.

DKIM uses an encryption key and digital signature to defend against malicious modification of your in-transit email messages by ensuring that what arrives in your recipient inbox was not faked or altered. In the meantime, an SPF record is an email authentication protocol that allows you to specify which IP addresses are authorized to send email on behalf of your domain.

"Mailbox providers prefer to receive authenticated email because authentication makes it easier to block harmful uses of email, such as phishing and spam."



If yours is a compliance-driven organization, Domain Message Authentication Reporting & Conformance (DMARC) support is necessary to help detect and prevent email spoofing (for example, to prevent a phishing scam that looks like the email is coming from your bank or PayPal, prompting you to click on a link to reset your password or to give them your information).

DMARC unifies SPF and DKIM authentication into a common framework and ensures that legitimate email is properly authenticated against these standards. Specifically, DMARC allows a domain owner to publish policies in DNS and tells remote mailers what to do with messages that do not align with these polices. If mail coming from your domain is suspected of being fraudulent, the messages are usually blocked (this is dependent upon how DMARC is configured, but a general rule of thumb).

Platform

Stream-level Performance Tracking and Optimization

Your ESP must absolutely be able to help you adjust and hone your email programs over time, using quantitative and qualitative methods to keep deliverability rates high as mailbox providers continuously change the rules of the game. Doing so requires understanding how and why certain messages are failing to reach the inbox, and then responding as necessary. **First and foremost, your ESP must attack the issue from a best-practice-based perspective** (this approach of segmenting and tracking email performance will be discussed later in this ebook). **Second, your ESP must help you understand how well your individual messages perform and where further optimization is possible.**

"Control of the technology stack, a high rate of innovation, and a willingness to customize the client experience are essential qualities for an ESP, given the pace of change surrounding email communications."

Continuous Flexibility and Scalability

Every company's communication needs and goals are different. That's why flexibility is critical. As your business grows, so does the number of email streams that your ESP must handle. You need confidence your provider can seamlessly expand and evolve with you.

A healthy email ecosystem provides options for customization, offering more than just a one-size-fits-all approach. There should be guidance on how to use this flexibility to optimize message delivery. Be sure you can discuss customizations or system configurations that can improve your experience. For example, setting custom sending domains and IP whitelists are great choices to help build the corporate brand and the reputation of your messages with inbox providers, but these features need to be properly configured before you get started. And as your business grows, scalability becomes very relevant. Can your ESP easily meet the sending volumes you may require?

The Cost of Poor Email Deliverability

While long-term repercussions of increased costs, reduced service levels, and lost revenue are indirectly attributable to poor email deliverability, there are also more immediate and tangible negative outcomes for your email communications. Here are five common results of poor email deliverability:

1. Emails don't ***reach*** the intended inbox and are never opened or read.
2. New or existing customers don't get important updates from you.
3. Customers miss important transactional emails like receipts and order confirmations.
4. Your brand reputation goes down because your name is often found in the spam folder.
5. Competitors with better email deliverability get more attention!

Best Practices

You can always take actions today that will improve your IP reputation and enhance your future deliverability.

The following are key strategies and deliverability recommendations that our strategists often see go unappreciated by many organizations – and which a good ESP should help you monitor and address:

1. Carefully segment your email streams
2. Apply strong and authentication and security
3. Tightly define your message and campaign audiences
4. Compose messages that are both engaging and compliant
5. Warm up your IP addresses and new email patterns
6. Monitor all messages for deliverability, open rates, and engagement

Carefully segment your email streams

The simple rule is, the more granular the better. Starting at a high level, you should separate marketing and transactional email streams. When the major inbox providers encounter messages that are obviously marketing, they will often defer or limit the rate at which they are accepted and delivered while they monitor recipient reaction. If transactional messages are mixed into the same email stream, these higher priority messages may also suffer the same limitations.

To create stream separation, you can start by using different root (or "from") addresses for each type, for example using "orders@yourdomain.com" for transactional messages and "promotions@yourdomain.com" for marketing messages. Many organizations, large and small, segregate distinct streams of mail by sending them from their own IP address. This physical separation prevents any inbox confusion, allows each stream to develop its own reputation, and simplifies performance tracking process.

Differentiating between message types

Before you can endeavor to drive email deliverability and engagement, you must recognize and understand the difference between **the two types of high-volume email messages.** They are:

- **Marketing email**, which are promotional and include coupons, sales notifications, and newsletters
- **Transactional email**, which are sent programmatically from an application to a recipient (and via an SMTP Relay or email API) and include password resets and order receipts

To learn more about the handling differences between marketing and transactional messages, check out this blog post: ***Marketing vs Transactional Email (All You Need To Know)***

Best Practices

Apply Strong Authentication and Security

The currency of email communication is almost always **some degree of personal and/or private information, so messages naturally require at least a minimum level of security.** Moreover, you simply cannot ignore the basic security standards that will help ensure deliverability of time-critical content and information. Implementing industry authentication standards, such as SPF, DKIM, and DMARC, provides protections that make your messages more trustworthy in the eyes of mailbox providers. By embracing these practices, you'll send the necessary signals to all mailbox platforms that your mail originates from a trusted source and has not been tampered with in transit.

Tightly Define Your Message and Campaign Audiences

Contrary to popular belief, **increasing your message volume doesn't equal email campaign success. In fact, it can be quite the opposite.** A high volume of email sent to "the wrong audience" (those who are not an ideal fit for the information or service offering that's being presented) can be extremely detrimental to email deliverability. The result of this lazy targeting approach is that the receiving individuals have a much higher tendency to categorize your incoming messages as spam or unsubscribe from your mailing list altogether. As this occurs, the reputational damage that is caused reduces your status with mailbox providers and causes further restrictions on the deliverability of every subsequent message you push out.

Driving transactional email to the inbox

Within limits, transactional email represents an enormous opportunity for further recipient interaction because they are already voluntarily and actively engaged with you and your products and services. So, it's critical to follow best practices and then carefully monitor deliverability, open rates, and engagement. It's essential to know if your recipients are moving your messages to the spam or junk folder. That's because **if there are enough spam complaints to tip your rate over 0.1%, your reputation will decline, and future emails may be automatically kicked to the spam folder.**

To learn more about fortifying your transactional emails, check out this blog post: ***Top 6 Transactional Email Best Practices***

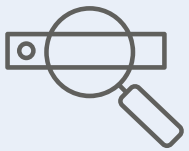
Best Practices

Compose Messages that are Both Engaging and Compliant

There are countless best practices that fit under the overarching theme of good email design. They're all aimed at meeting legal requirements and fostering positive recipient engagement. Positive engagement, in turn, is a significant driver of reputation, which will boost future deliverability rates. At a minimum, you need to build programs that:

- **Follow local email laws**
  The United States, Canada, and the EU have different laws surrounding email spam – and many EU countries have their own additional standards and rules. As the sender, it's incumbent upon you to know and follow applicable regulations. In other words, ignorance is not a defense. It's important to note that the recipient's location, and not your sender location, determines the laws that must be followed.

- **Clearly identify the source and reason for your email**
  Your message should clearly answer the basic questions of: Who is sending this message? What is the purpose of this message? Why am I receiving this message? This is especially true if it has been a while since the user last interacted with you. It's also advisable to use a "from address" that is easily understandable and relatable (such as "*orders@yourdomain.com*") and to brand your messages by including your company name, logo, and colors.



- **Feature prominent unsubscribe buttons**
  An easily visible and accessible unsubscribe link or button will have enormous positive impact on your deliverability. Even if the recipients have opted in, some of them will want to opt out at some point. For marketers, this is more than just a good idea, it's a requirement to stay in compliance with CAN-SPAM laws.

- **Use a "reply to" address**
  A "reply to" address tells your recipients that you want to hear from them –and you do. In recent years, this metric has become a major factor in helping mailbox providers, especially Gmail, determine how to handle messages. So, there's a deliverability benefit to receiving replies to your transactional email. More importantly, the mere presence of a "no-reply" address could negatively impact your deliverability.

- **Ensure recipient consent and consistent list scrubbing**
  Using bulk email lists or sending unsolicited messages to unfamiliar or guessed email addresses is simply dangerous. That's because the mailbox providers will take notice of the inevitable spam complaints, blocks, and unread message deletions – and ding your reputation accordingly. Conversely, they will also note and reward you if your email has high clicks, opens, saves (when users store them in a folder for future viewing), and forwards.

Best Practices

Warm Up Your IP Addresses and New Email Patterns

IP warming is the process of gradually increasing the volume of emails sent from an IP address over time. It's part art and part science. A rather conservative and very general method used to warm an IP address is to equally distribute sending across all mailbox providers. For example, if you're sending 100,000 emails in a month, you might divide those 100,000 emails to send equally each day and to each mailbox provider. So, you might send 1,111 to your Gmail addresses, 1,111 to Yahoo! addresses, and 1,111 to Verizon addresses until you hit 100,000 messages that month. This safe and calculated approach will help your IP address stay under the radar of providers' spam traps and content filters. This same approach applies when sending any new stream of email traffic. Mailbox providers will always be skeptical of new traffic patterns until they can be proven safe. As the providers observe that your deliverability/engagement rates are healthy, your reputation will grow, and you can increase your sending volumes.

Monitor All Messages for Deliverability, Open Rates, and Engagement

Because transactional emails are wanted and expected, many organizations think they don't need to be checked for opens, clicks, bounces, and complaints. But, you can still learn from the behaviors of your transactional email recipients. Plus, even the best quality email (transactional or marketing) can land in the spam folder—and, that's certainly something you need to know about so that it can be quickly resolved. **Delivery confirmation is essential if your messages are offering information regularly shared with customers (i.e. account summaries or reports) or are being sent as an automated response to a customer request (i.e. password resets or technical support tickets).** In these, and many other cases, delivery and engagement can be the difference between keeping and losing a customer. Further, optimizing inbox rates will help reduce the need for manual interventions, as well as your operational costs.

To learn more about email delivery best practices, check out this blog post:
What Affects Email Deliverability (Top 3 Best Practices)

Get Email Delivery Down to a Science

A pioneer in the ESP market, SocketLabs® offers you the ideal combination of technical platform and best practices expertise.

Further separating us from the pack is that we support each solution with world-class, personalized service. Our support and consulting teams help companies in virtually every industry innovate the way they separate, analyze, visualize, and manage email strategy to maximize audience engagement and achieve business goals. We help clients avoid the pitfalls that erode email effectiveness through our high-touch user experience, powerful proprietary software, and unique consultative methodology. More important, we invigorate SaaS platforms, mobile apps, and custom applications by plugging them in to an unmatched email experience based on SocketLabs' proprietary science.

"Our founders have been creating cutting-edge email solutions for over 20 years and built a customer support organization that considers 'responsiveness and satisfaction' key performance objectives."

Our ground-breaking, customer-first spirit continues to drive consistent inbox optimization improvements in the face of constant change.

Recent innovations include:

- ✔ Intelligent traffic routing based on over a decade of delivery data
- ✔ Advanced encryption standards to prevent "man-in-the-middle" cyberattacks
- ✔ Simplified email link encryption
- ✔ Automated engagement tracking security features

SocketLabs' proprietary cloud-based technology blends **three critical components** to form a uniquely powerful email delivery ecosystem:

1. **The Hurricane™ Mail Transfer Agent (MTA)** – Our proprietary high-volume email delivery engine
2. **StreamScore™** – Our unique stream-specific email authentication, performance, and quality analytics tool
3. **SendFlex™** – Our robust multi-stream account and traffic configuration system

We complement and expand on this strong technical backbone with our highly responsive, hands-on customer service team, which consistently boasts a **98% satisfaction rating.**

Learn More About the SocketLabs® Difference!

Contact us today to request a solution demonstration or discuss your email challenges, at sales@SocketLabs.com or www.socketlabs.com.

SocketLabs is a B2B technology firm that provides flexible SaaS and on-premises solutions for solving a variety of complex email delivery challenges for both transactional and marketing messages. We are a pioneer in the Email Service Provider (ESP) market with a decade-long track record of excellence. Our unique, proprietary mail transfer agent (MTA) technology is trusted by clients around the globe who invigorate their SaaS platforms, mobile apps, and custom applications by "plugging in" to an unmatched email experience. Our founders have been creating cutting-edge email solutions for over 20 years and have built a customer support organization that considers "responsiveness and satisfaction" as our key performance objectives.

Email us!

support@socketlabs.com

Call us!

USA:
800.650.1639
International:
484.418.1285

Chat with us!

www.socketlabs.com/chat