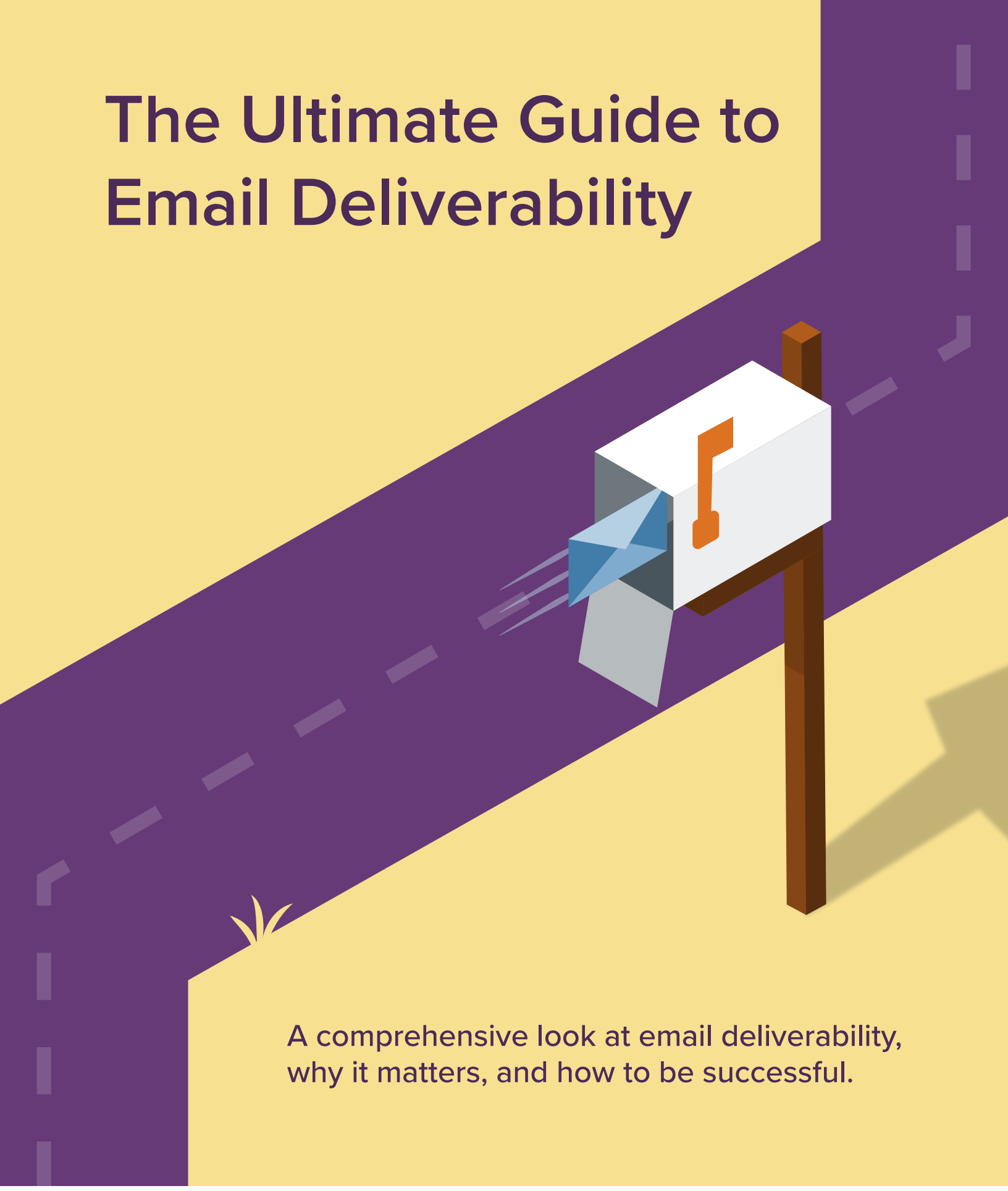
The Ultimate Guide to Email Deliverability



A comprehensive look at email deliverability, why it matters, and how to be successful.

litmus + SPARKPOST
A MessageBird company

The Ultimate Guide to Email Deliverability

A comprehensive look at email deliverability, why it matters, and how to be successful.

Table of contents

1 | What is email deliverability and why does it matter? 3

2 | Setting a strong foundation on what spam filters are and how to avoid them 4

- Internet Service Provider (ISP) filters
- Corporate filters
- Desktop filters

3 | Steps to ensure strong deliverability 6

- 12 step deliverability checklist
- Creating the right infrastructure and authentication
- IP and domains

4 | How to monitor and measure deliverability and adjust your approach 13

- Inbox placement and deliverability tools
- Pre-send guidelines
- Post-send guidelines

5 | What to do if deliverability has tanked 16

- What to check
- How to resolve spam trap issues
- 15 tips to avoid having your email blocked or blocklisted

Appendix | Deliverability terms you should know 22

1 What is email deliverability?

Each time you hit send, your emails go on a journey. Just like going to the airport, an email has a few checkpoints to make it through on its way to the intended destination. These correlate to two essential email terms—delivery and deliverability.

If an inbox service provider's server accepts the email (as in it doesn't bounce), it's considered delivered. The message's journey doesn't end there, though.

> Email deliverability is the rate at which your emails make it into your subscribers' inboxes instead of being labeled as spam and going to the junk folder.

A high deliverability rate means your emails often make it to the inbox. This can be in the primary inbox or a Gmail tab based on content.

So who calls the shots on whether your email gets delivered? Inbox service providers decide if your email meets their standards based on filters and protocols set in place. As Derek Harding, CTO at Trendline Interactive, pointed out, "the complexity of Internet Service Providers (ISP) filters means that it is frequently impossible to identify specific root causes for such issues."

Some factors that inbox service providers could consider when making a ruling on your deliverability include:

- Email engagement
- IP and domain reputation
- Blocklists
- Email authentication

Why deliverability matters

Nobody wants to put in all the work required to make an email, only to have it collect dust in a junk folder. If your deliverability is low, fewer customers see the messages you worked so hard to create resulting in less engagement and ultimately, fewer sales.

Plus, poor deliverability has a ripple effect. Below average open or engagement rates on a single campaign that didn't have the right positioning won't hurt your program long-term. But, a systematic deliverability issue will. And when you're putting the same amount of work into emails but fewer people see and act on them, your ROI will diminish.

To maximize your email investment and its impact, you need high deliverability.

How do spam filters work?

Put simply, filters accept an email, decide where it should go, and deliver it to the appropriate mailbox. There are a few types of spam filters:

Internet Service Provider (ISP) filters

We all know spam can be annoying. Successful email marketers realize that the ultimate goal is to send the right message, at the right time, to the right reader – as in something wanted by and relevant to the recipient. ISPs (think Google and Microsoft) play a key role in creating a good user experience by trying to blocklist unwanted emails. Once a recipient flags an email as spam, ISPs attempt to block similar messages.

All ISPs are different, but a sender's reputation will ultimately determine if an email makes it into the inbox, or the spam folder. And while the content of your emails isn't as big of an issue as it was in the past, it's still worth evaluating to make sure it's not spammy. Everything from your subject line to preheader text, body content to images, and even the URLs in your emails is scanned by an ISP filter. There are no set rules, but some general email guidelines include avoiding:

- Enticing phases like "Click here!" or "Buy now!"
- Multiple special characters in a subject line like "New feature! Come check it out!!!"
- All caps – it can give a high spam score and can seem aggressive.
- Image-only email as these can be marked as spam without real content to scan.
- Links that look like phishing attempts.
- Using link shorteners.

Corporate filters (hello, B2B email geeks)

Businesses often use gateway spam filters where email must make it past a security "gate" before the inbox. Alternatively, they can use a hosted spam filter on a third-party cloud service. Corporate filters are – shocker – often seen in the B2B email world as employees access their mail through a company-supplied email client. And while employees frequently access email through the same web-based email client that consumers do (e.g. Gmail), the engagement of the end user isn't as important in corporate filtering.

Don't get us wrong – engagement is (always) important. But engagement data (e.g. opens and clicks) is not typically shared back with the sender, so senders don't have those kinds of insights when a corporate filter is in play. In fact, business recipients can report an email as spam, but the company does not share that data through their feedback loop.

And while B2C filters are relatively passive, corporate filters actively interact with email as it comes in over simple mail transfer protocol (SMTP). This not only affects email delivery, but it can affect sender reporting and tracking too. Email veterans have all had to deal with cases where filters have followed every link in our email – and business filters are more likely to do this than consumer filters. For performance and privacy reasons, filters are selective in following links in normal email. However, if there is something more suspicious about an email stream, or there is evidence of a broader security event, then the filters aggressively check links. When the risk is losing money or having a network breach, spending a few extra seconds to check mail is well worth it.

Learn more in SparkPost's Guide to B2B Email by deliverability expert Laura Atkins.

Desktop filters (like MailWasher)

Desktop filters are installed by an individual user to their computer. These allow recipients to custom-configure how they want to receive (or block) emails to their address. Desktop filters typically have custom settings specific to each user, and they often block engagement data (e.g. opens and clicks) from the senders as well.

3 How to ensure strong email deliverability

Email deliverability is too important to leave to chance. It pays to have a plan to improve and maintain your strategy for maximum effectiveness. Your two main levers to do so are increasing engagement and reducing spam complaints. With proper email infrastructure, inbox service providers will recognize you as a reliable sender.

12-Step Deliverability Checklist

1. **Follow authentication protocol**: Authentication protocol is a key technical consideration for deliverability. Setting up your infrastructure correctly lets inbox servers know you're legitimate and worthy of the inbox. The fundamental protocols you need to have in place are:
    - Sender Policy Framework (SPF)
    - DomainKeys Identified Mail (DKIM)
    - Domain-Based Message Authentication
    - Reporting and Conformance (DMARC)
    - Brand Indicators for Message Identification (BIMI)

TIP: Taking a proactive approach with a strong foundation of best practices can help you avoid many common issues, saving you time and allowing for more focus on other areas of your campaign.

2. **Follow all email permission and spam laws**: Rules about who you can email, what you need to include in each email, and your opt-out process vary by country and region. There are even non-email-specific consumer protection and data encryption rules that impact marketers. Since these rules can change, it pays to keep a close eye on regulatory updates. Also, keep in mind that you need to follow the rules where your subscribers live, not just your company's home country.

3. **Review your segmentation & targeting**: It makes sense that the more relevant your emails are, the more likely people are to engage, increasing deliverability. The key to driving engagement is precise targeting of category-specific mailings to customers most likely to purchase. By curating your audience, you offset the risk of opt-outs, spam complaints, and emotional unsubscribes (those that ignore your emails) from over-mailing non-relevant content.

TIP: Wrap increased frequency into a specific campaign type, and ask your customers to opt in to the increased frequency. Subscribers will then anticipate your emails and the special offers included. E.g. "12 days of deals" where a daily email will be sent featuring the best offers over the holiday season.

4. **Drive engagement via interactivity**: Email can be one of the many ways people are engaging with your brand but it's one of the most important. Contacts who show interest by interacting with emails give a strong signal to mailbox providers that your content is relevant and legitimate.

TIP: Implement interactive elements in email like AMP or kinetic capabilities that compel people to engage.. E.g. Ask subscribers to tap a gift box to reveal an offer. If you can't build out interactive experiences due to bandwidth, creatively use animated GIFs and landing pages as a good alternative.

5. **Audit your entire email infrastructure**: Make sure your authentication, acquisition, and unsubscribe sources and complaint feedback loops are all in proper working order to avoid any hangups. Email list hygiene should also be a priority to keep dead weight off, lowering potential deliverability issues.

TIP: Tackle list hygiene in acquisition sources through email validation to ensure malformed and other bad email addresses aren't added to your list. For those already on your list, implement a re-engagement strategy to remove any inactive email addresses. Inactives cause harm to your email reputation and even hit spam traps, causing deliverability issues. Historically, this has been done by removing those that haven't had any opens or clicks over a period of time. However, in light of iOS 15, opens are no longer reliable. Be cautious about continuing to use them as a primary sign of engagement.

SparkPost's 7 Essential Email Audits guide has some great audit suggestions (including frequency recommendations) and ways to get started.

6. **Start ramping up message volumes before big campaigns**: Mailbox filters run on algorithms that monitor send volumes and trends over time. A quick uptick in volume may cause your messages to hit the spam folder. Be conscious of when and how often you communicate.

TIP: Slowly ramp up your messaging in the weeks leading up to a big campaign (e.g. a corporate event like Litmus Live, or a big consumer spike like Black Friday). Many brands have customers that only engage during big deals and events, so treat sending to these annual additions like an IP warm-up.

7. **Re-engage inactive subscribers**: Maintaining an active and engaged list is good for business – and deliverability. Quality beats quantity when it comes to getting results. Unengaged subscribers can cause your emails to go to the spam folder. It pays to remove inactive subscribers depending on parameters that are important to your business. To remedy any dead weight on your list, deploy a re-engagement campaign to ensure you aren't hitting spam traps and getting blocklisted before your next email campaign.

TIP: Ask all subscribers that haven't clicked in the last 90 days if they want to continue to receive emails. This type of campaign will not only help you clean up your list, but the act of the click will actually boost your credibility with the mailbox providers that are looking for engagement with your emails.

8. **Plan & implement seasonal templates**: Compelling email design is critical to high engagement, and engagement is critical to good deliverability. Just as you would decorate a physical storefront for a new season, you can do the same for your emails.

TIP: Add themed imagery to the logo that might even have a small pop of animation, such as twinkling lights or falling snow in the winter. Part of your header can also include a countdown of shipping cutoff dates to ensure people know when they need to get their orders completed, or highlight the number of days before a big discount ends.

9. **Think outside the box with personalization**: A first name call-out is great at getting attention, but there are other options available. Dynamically populating your messages with product references or specificity on offer expirations and shipping deadlines, particularly on items the recipients have shown interest in previously, is a great way to tailor your emails to specific target segments for increased personalization.

TIP: Try using weather personalization to promote relevant offers, and also provide sensitive communications to areas affected by extreme weather (shipping delays, etc). You can use location personalization to share updates about changes to local events, hours, or special operating policies.

10. **Run testing for best results and make unsubscribing easy**: Being in front of the right audience with the right messaging is critical to drive results. An A/B test set up the right way can help you learn what resonates the most and where improvements can be made. Will changing the CTA button increase conversions? Is the copy informative, compelling, and prompting the action you're wanting recipients to make? There's always room to evolve your email to be more engaging and less spam-worthy.

TIP: Make sure you're focused on the key things necessary to run a successful A/B test and how those results can shape future communications.

11. **Keep an eye on the competition**: What campaigns did your key competitors run last year? When? How often? What did they offer? With what types of creative?

TIP: This type of information can support your big email program planning critical mid-course corrections within a live campaign. SparkPost's Competitive Tracker functionality uniquely provides applicable insights.

12. **Make it easy to unsubscribe**: If subscribers want to leave your email list, it should be easy. Additional hurdles such as asking someone to log in to unsubscribe may cause people to decide it's easier to mark the message as spam. A cumbersome process results in wasted efforts on uninterested recipients and potentially poor brand perception.

Creating the right infrastructure and authentication

In addition to the above steps, you can encrypt your emails to ensure security. It's a good idea to combine email encryption with email authentication to ensure the integrity of your email messages.

Validating the authentication of the email sender helps inbox providers confirm that your email originated from you (a real person!) and not a spammer/phisher. Three primary frameworks should be followed to be authentic: sender policy framework (SPF), DomainKeys Identification Mail (DKIM), and domain-based message authentication, reporting & compliance (DMARC). There's also a relatively newer method called brand indicators for message identification (BIMI) that has slower adoption, but it offers compelling benefits and it's picking up!

Email Encryption

Secure Sockets Layer (SSL), Transport Layer Security (TLS), and STARTTLS are standard protocols used to secure email transmissions. Essentially, they provide a way to encrypt a communication channel between two computers over the internet.

In most cases, the terms SSL and TLS can be used interchangeably. Because TLS and SSL are application-layer protocols, senders and receivers need to know that they are being used to encrypt emails during transit.

That's where STARTTLS comes into play. STARTTLS is an email protocol command that tells an email server that an email client wants to turn an existing insecure connection into a secure one.

When an email client sends and receives email, it uses Transmission Control Protocol (TCP) via the transport layer to initiate a "handshake" with the email server. During that basic setup process, the email client tells the email server which version of SSL or TLS it's running and what cipher suites (a combination of processes used to negotiate security settings) and compression methods it wants to use.

After the setup is finished, the email server verifies its identity to the email client by sending a certificate that is trusted by the user's software, or by a third party trusted by it. Doing so ensures that the email client isn't sending messages to an imposter. Once the client knows it can trust the server, a key is exchanged between the two, which allows all messages sent and received to be encrypted.

Whew! That got kind of technical – check with your ESP to see how they have you configured.

It's important to use SSL or TLS with your email setup because unsecure email is a common attack vector. Anyone who intercepts encrypted emails is left with unusable garbage text that can only be decoded with the keys by the email server and the client. This is critical to protect user names, passwords, personal details, and other sensitive information that's often found in emails. If an attacker discovers a weakness, they will exploit it by mining and selling the data.

Sender Policy Framework (SPF)

This is where senders can specify which users can send email on behalf of their sending domain. Administrators can generate a specific SPF record in their public DNS, where mail exchanges can be used to verify the message was sent by a trusted party.

At the most basic level, SPF establishes a method to verify that incoming email from a domain was sent from a host authorized by that domain's administrators. The following three steps outline how SPF works:

1. A domain administrator publishes the policy defining mail servers that are authorized to send email from that domain. This policy is called an SPF record, and it is listed as part of the domain's overall DNS records.
2. When an inbound mail server receives an incoming email, it looks up the rules for the bounce (Return-Path) domain in DNS. The inbound server then compares the IP address of the mail sender with the authorized IP addresses defined in the SPF record.
3. The receiving mail server then uses the rules specified in the sending domain's SPF record to decide whether to accept, reject, or otherwise flag the email message.

Domain Keys (DKIM)

Domain keys do two things:

1. Guarantees the sender is who they say they are.
2. Guarantees the contents of the message.

The sender can "sign" the message with a signature only they know, and the encrypted signature is then attached to the message and sent to the recipient. When the message arrives at the destination, the server asks the sender for the public key, which can then be used to verify the message is authentic and was actually sent by the sender.

This signature can then be validated against a public cryptographic key that is located in the organization's DNS record. Here's a quick breakdown of how this works:

1. The domain owner publishes a cryptographic key. This is specifically formatted as a TXT record in the domain's overall DNS record.
2. After a message is sent by an outbound mail server, the server generates and attaches the unique DKIM signature to the header of the message.
3. The DKIM key is then used by inbound mail servers to detect and decrypt the message's signature and compare it against a fresh version. If the values match, the message can be proved authentic, and unaltered in transit, and therefore, not forged or altered.

Domain-Based Message Authentication, Reporting and Conformance (DMARC)

This was created to prevent phishing attacks and was built on top of the older two frameworks. There are three parts to DMARC:

1. DMARC gives senders the option to define how the “from domain” has to “align” – strict or relaxed. If the alignment is strict, then the domain match must be exact. For example, if the from address is hello@email.com, but the actual sender was hello@sender.email.com, this would be considered an unaligned email message. If the alignment is relaxed, then subdomain matches are allowed. In our example above, with a “relaxed” policy the message would be “aligned.”
2. DMARC provides a framework to tell receivers and spam filters what to do with messages that are not DMARC-aligned. Through DMARC, they can publish a policy telling the inbox provider to “always delete unaligned email” or “always put unaligned email in the spam folder.”
3. DMARC provides a reporting feature. This allows organizations to find sources of legitimate, but non-DMARC aligned mail, so they can fix it and ensure it is aligned.

To learn more about DMARC, check out SparkPost’s guide Why Email Authentication Matters written in partnership with dmarcian.

Brand Indicators for Message Identification (BIMI)

Launched in 2019, one of the first benefits of BIMI can be seen right from the inbox – the prominent placement of the sender’s logo just to the left of the from name. This visual indicator is a huge step in standing out in a crowded inbox.

There are other benefits of BIMI as well. Aside from brand recognition, it helps prevent spoofing, since other methods of authentication (SPF, DKIM and DMARC) must be put in place before you can consider implementing BIMI. This newer form of authentication also helps build trust with subscribers and helps get more emails into the inboxes of consumers at mailbox providers that support BIMI.

IP and domain warmup

Sharing an IP address

Using a shared IP for your company email program is common, but you should weigh the pros & cons.

Pros:

- The volume has already been established for a long period of time.
- You can share your reputation, which means other low-volume sends can piggyback on your IP reputation.
- They cost less than dedicated IPs.

Cons:

- You don't have any control over the content from the other senders on the IP.
- Shared reputation means if one goes south, yours will too.

Using a dedicated IP address

This is a must-have for high-volume senders. A dedicated IP address gives you full control over your sending reputation as data, engagement metrics, and sending practices only reflect that particular IP address' reputation.

Using a new IP address

Inbox providers have no information on you, which can help classify you as a "reputable" sender. But you'll need to "warm-up" your email address before sending big email campaigns. Check your ESP help center on how to do this with your specific tech stack/email programs, but read on for a few best practices.

How to do an IP warm-up

In theory, this is a fairly easy process. A simple rule of thumb is to send 200 emails using the new sending domain/IP combination (SDIPC); then each day you can double the number of emails you sent the prior day. To improve your chances of a smooth warm-up process, you should start sending to that new SDIPC with your best and most engaged customers. Within two weeks of doubling your sending, you should be able to send over 1.5 million messages a day through that SDIPC alone. In three weeks, that number is an astounding 209 million messages a day! That amount is enough to support 99.9% of the legitimate senders of the world.

This is a common practice when switching from one ESP to another, and it's always best to chat with your ESP before beginning a new warm-up.

Sending domains

Your sending domain is simply the web address you're sending from – e.g. welovelitmus@sparkpost.com. Sparkpost.com is the sending domain here. An easy way to check your domain reputation is to visit sparkpost.com/delivery-index, enter your mailing domain, and see a quick snapshot of your deliverability in weekly increments. You'll be able to check your inbox placement across all of the major inbox providers, as well as key areas impacting your inbox reputation (including blocklists, spam trap hits, and authentication elements). You can also check your competition's sending domains to see how you measure up. It's free to use, and a great way to understand your deliverability and identify possible ways to improve it.

4 How to monitor deliverability & adjust your approach

Keeping an eye on deliverability and email program health is an ongoing practice. In order to be successful, you must not only keep a pulse on what's happening, but also continue to optimize your strategy as variables will likely continue to change, impacting your results.

Here are tactical ways to continue to fine-tune your approach.

Inbox placement & deliverability tools

On average, almost 20% of permission-based emails never reach consumers' inboxes because they are filtered as spam or junk. This translates into huge missed revenue opportunities for email marketers. Deliverability may not be the first thing you think about when executing your email programs, but it's one of the most important – even a 1% drop in deliverability can greatly impact your bottom line!

There are tools that go beyond what you can track in your email service provider, like SparkPost's Inbox Tracker, that can help you monitor things like:

- Inbox placement
- Deliverability by ISP, domain, and campaign
- Inactive subscriber rates
- Average time to receive an email by domain & ISP
- Detailed deliverability insights
- Recent campaigns with engagement & subscriber metrics
- Outlook SNDS deliverability
- Complaint, blocklist, and trap monitors
- DKIM & SPF monitoring

Deliverability monitoring is truly multi-faceted and will benefit anyone who sends email. Knowing engagement rates, what is or isn't working, and discovering underlying set-up-related issues will ensure the effectiveness of your email marketing efforts. In addition to the core metrics listed above, you should also track things such as:

- **Sender reputation**: Check key elements of your program across critical areas like configuration, IP reputation, and authentication. This helps you address any underlying deliverability issues.
- **Subject line performance**: Using your own customer data and campaign history, you can see your highest performing emotional themes over time, how character length is impacting performance, and review and compare your highest performing words and phrases.
- **Brand security**: Leveraging all-inclusive authentication reporting, you can ensure optimal configuration and protection against phishing attacks.

Monitoring Deliverability Pre-send

Check to see if you've been blocklisted

Blocklists are compilations of senders that are believed to send spam or abuse email in some way. There are a variety of lists you could find yourself on, and the impact on your deliverability depends on the size of the list.

The easiest way to see if you've landed on one of these lists is by using Litmus Spam Testing to check across multiple lists automatically. In an analysis of 1.5 million tested emails, we found that 70% of emails show at least one spam-related issue that may impact deliverability.

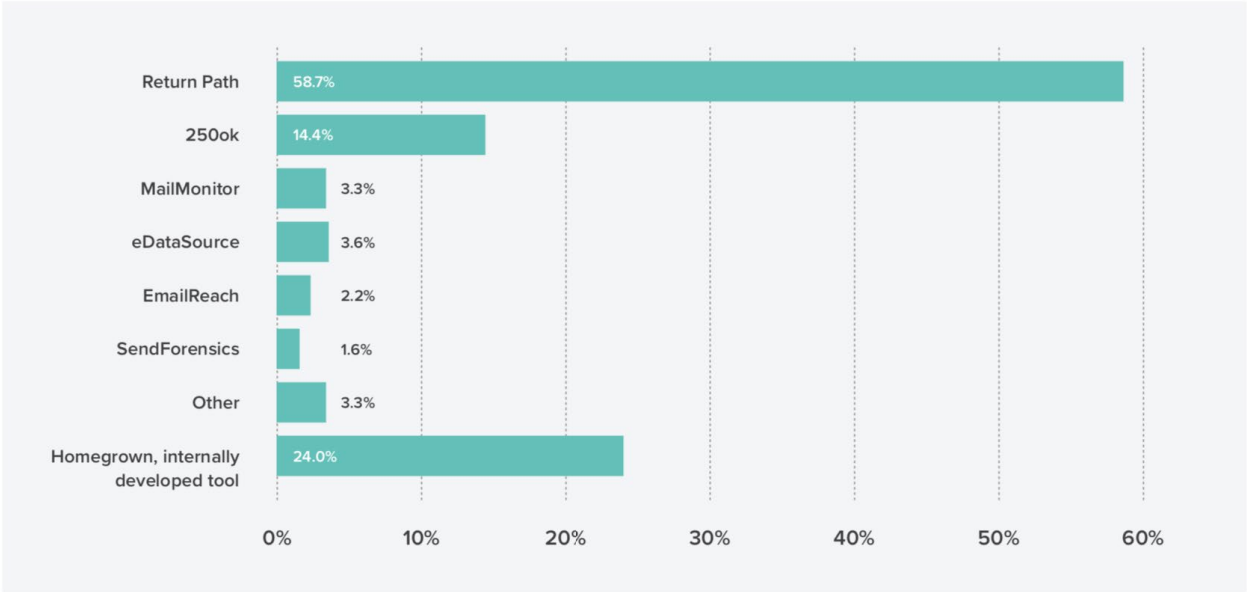
You can also manually search for your IP and domain on blocklists, including:

- MX Toolbox
- Debouncer
- DNS Checker
- Sender Score

Return Path Dominates Deliverability Monitoring Tools Used to Supplement ESPs

What service or tool does your company use to monitor its deliverability or inbox placement rate? Select all that apply. Those with at least 1% market share shown.

450 respondents



Monitoring Deliverability Post-send

Use deliverability monitoring tools

While your ESP can tell you how many emails made it to a subscriber's survey with bounce rates, most don't have deliverability scores. It's common for email teams to use third-party deliverability monitoring tools like SparkPost Inbox Tracker or internally developed tools. Over half of brands always or often monitor their deliverability rate to increase effectiveness.

Monitor spam complaints, bounces, opens, and clicks

Since your sender reputation can influence email deliverability, keeping a close eye on your analytics can help you catch issues faster. You should investigate further if you see:

- **Your spam complaints rise**. This is a sign that something about your content isn't resonating and could get you on a blocklist.
- **Your bounce rate increases**. Yes, bounce rates determine your delivery rate. But, anything that harms your email reputation could hinder deliverability in the long run.
- **Your opens or clicks decline**. The occasional lackluster campaign is okay, but downward-trending engagement could lead inbox service providers to believe your emails are low-quality.

5 What to do if deliverability has tanked

What to check

There are literally thousands of blocklists for thousands of reasons – most of which do not affect the average sender. Most large ISPs have their own internal blocklists and scoring systems, but the primary independent blocklist in use today is Spamhaus.

Mailing to spam traps is the single most common cause for a blocklisted IP address, and there are four main types of spam traps to be aware of:

- **Typo Traps**: When an email address that's hosted on a domain looks like a real mailbox provider, like "wayne.campbell@gmai.com." Typo traps usually end up on your list when a real person tries to sign up for your mailings but makes a mistake when entering in their email address. (However, some typo domains are actually owned by the Mailbox Provider.) These addresses signal that you should work to simplify and optimize your sign-up flow. They are most likely caused by human error, which leads us into the next type.

- **Pristine Traps**: Email addresses that have never had real active mailboxes associated with them. They are published and embedded into websites so that poor list acquisition processes or spammy senders can be easily identified. These traps are considered the most serious since they are indicative of very bad list acquisition practices, as there is no legitimate way that a pristine could have entered a list.

- **Recycled Traps**: Emails/domains that previously were a legitimate recipient but went fully idle (not accepting mail) for a period of time (typically at least a year) before being repurposed as a trap. These are not only linked to poor acquisition issues, but also indicate that you may not be removing unengaged recipients from your list, a very serious list maintenance concern.

- **Parked Traps**: These are not actually a trap, but they behave like one and can also be indicative of list maintenance issues. Domains are 'parked' at a registrar or monetization site (like namecheap or above.com). Other parked domains get 'leased out' to commercial trap providers as part of their trap networks. This practice captures similar 'unleased' domains.

If you do have a blocklist that shows up in your bounce logs causing a bounce rate above 1%, we recommend opening a support case with your email provider to investigate further.

How to resolve spam trap issues

1. **Identify the source or mailstream that has an issue**
   - Check any recent changes to your acquisition process.
   - Stay away from purchased or rented lists.
   - Ensure all sign up processes include email verification.
   - Protect your signup process from bot activity.

2. **Remediate the issue**
   - Eliminate any recently purchased or rented lists and monitor the resulting decline in spam trap hits.
   - Improve your sign up process to:
     - Include an address verification check for typos or hard bounces.
     - Require that the address be typed in twice to avoid address typos.
     - Include reCAPTCHA on your sign up forms to avoid abuse.
     - Use double opt in (spam traps will never confirm the opt-in).

3. **Communicate the issue and details of the remediation to the trap provider**
   - Once you have identified and resolved the cause, you can then reach out to the trap owners and mitigate any blocklists if necessary.
   - It is important that you describe your findings and the resolutions in detail, and then ask if there is anything else you should do to resolve the issue. This will then leave it open for them to mitigate or provide you with more detailed information.

Spam score

Two of the most critical pieces in generating a high spam score are your subject line and the email's written content. We've already discussed avoiding the use of subject lines that look spammy, but certain phrases can group you into different high-level categories. These categories are then assigned points by email filtering programs. If any message gets assigned too many points (default is usually 5.0), it gets sent to the spam folder.

But don't fret – you can test your emails through SpamAssassin to view how "spammy" they are. SpamAssassin scans elements such as subject lines, headers, attachments, punctuation, spam-related text, and messaging to give a spam score. Generally, emails with a score above 5 are considered spam.

Here are a few examples:

- Mortgage email → 0.297 points
- Contains words that imply urgency or importance → 0.288 points
- Money back guarantee → A whammy at more than 2 points.

Check out this free SpamAssassin tool to get a good idea of your spam score.

Feedback loops

Many inbox providers supply a Feedback Loop (FBL) notification system that gives marketers insight into the subscribers who are clicking the “report spam” button. Usually you are automatically added into these FBLs, but there are some inbox providers where you need to manually register an email with the inbox provider to receive FBL reports. The report shows each time a recipient clicks the “report spam button” resulting in a system-generated abuse report, which it sends to the provided email address. This is one of the most useful resources available to marketers in regards to gaining insight into what email behaviors are being seen by subscribers as spammy.

DMARC reports

We touched on DMARC above, but in addition to authenticating your email, it’s also a great monitoring tool. Once you’ve published DMARC records, DMARC data will typically begin to generate within a day or two in the form of reports that give you insight into the way your domains are handling email. These reports are XML-based and can be difficult to read and make sense of, especially when they can number in the thousands.

But with DMARC data flowing, you can begin examining what sources are sending email on behalf of your domain and if those sources are legitimate. From there, it’s a matter of compliance, making each legitimate email source DMARC-compliant by deploying SPF and DKIM technologies, as well as learning more about the importance of SPF and domain management, and having a process around it in your organization.

DMARC gives organizations important visibility over your email domain and the ability to identify and audit all usage by third-party platforms. Your IT organization may know and condone some shadow IT platforms that use your email domain as part of the from address, but they may be unaware of many other platforms that also do.

Tips to avoid having your email blocked or blocklisted

Don't

- Don't buy email lists. Ever. The people on these lists are likely to mark your unsolicited emails as spam, and there's a good chance that a spam trap is included in the list. Sending email to a spam trap will usually land you on a blocklist – and right into the spam folder.
- Don't repeatedly send the same or similar content. Every email you send should consist of unique content. Not only will this help keep you off blocklists, but it will also keep your subscribers engaged.
- Don't string readers along with vague content. Include a clearly written subject line and call to action.
- Don't send attachments. (Attachments are meant for 1:1 emails.) Sending attachments may get your email blocked, but not blocklisted. The effect on deliverability may be the same, but the remedy is to simply not send attachments rather than working to get removed from a list.
- Don't use punctuation (such as exclamation marks) or words that are often used by spammers. These include free, win, and opportunity.
- Don't blind carbon copy (BCC) your list.
- Don't use too many images. Strive for a healthy balance of images and text to avoid triggering spam filters.
- Don't use all caps in your subject line – or any other part of your email. Instead, use bold, italics, and underline to show emphasis.

Do

- Do use double opt-in to confirm email list subscribers. This helps ensure subscribers are signing up with their own email addresses and that those email addresses are valid.
- Do include information on how to unsubscribe in every email.
- Do watch your sending frequency. Send email regularly while being careful not to overwhelm readers. (We recommend sending a message at least once every six months to keep your email list fresh. Unless you are a daily sender like Groupon, most email senders should avoid sending more than once or twice a week.)
- Do send email from a legitimate address that is checked by a real person. Email addresses with random letters and numbers trigger spam filters and can lead to your email being blocked.
- Do ask subscribers to add your email address to their contact list.
- Do practice good list hygiene. Regularly clean your email subscriber list to avoid repeatedly sending email to bad or non-existent email addresses.
- Do protect your email server from malware. An infected email server can be used as part of a botnet to send spam.

If you need help measuring your inbox performance, get a demo of Inbox Tracker and see first-hand how you can leverage the most accurate data sources on the market.

Closing Thoughts

Deliverability can be challenging to understand, but it's a critical part of a healthy email marketing program. Before your subscribers can open (and hopefully click!) on any emails, they must first receive them in their inboxes. Understanding the factors that go into successful email deliverability and implementing best practices that set up your organization, and your campaign, for success maximize your efforts and your results.

Need help evaluating your email deliverability?

Get an automated check to see if you're blocklisted, see how your emails hold up against authentication, inbox placement, score-based filters and if you might get caught in a spam filter. Plus, get access to hands-on advice to fix deliverability issues.

Start your free trial with Litmus

litmus

Meet Litmus

Here at Litmus, we're passionate about everything email marketing. And our mission is to help brands access what they need to send better email, faster. We share best practices and trends through a variety of formats to help you and your team stay at the forefront of the industry. We also provide software that makes creating high-performing email easy. Marketers pair Litmus with existing email service providers (ESPs) to ensure accelerated campaign performance, reduction in errors, easier collaboration across departments, and help keep your emails out of the spam filter. With Litmus by your side, you'll have the tools and insights you need to provide your customers with a great email brand experience for every subscriber — and an incredible ROI.

SPARKPOST

A **MessageBird** company

Meet SparkPost

SparkPost is an email optimization platform trusted by the world's largest brands, including The New York Times, Zillow, Adobe and Booking.com. SparkPost helps senders reliably reach the inbox with powerful solutions to help plan, execute, and optimize email programs.

SparkPost is the world's largest sender sending 4-5 trillion emails annually – and also boasts the world's largest data footprint to help enterprise-level brands make data-driven decisions to improve email performance. Learn more at www.sparkpost.com or connect via Twitter, LinkedIn or the SparkPost blog.

Deliverability Terms You Should Know

Brand Indicators for Message Identification (BIMI): a text record that is used to verify information about your brand that works right alongside SPF, DMARC & DKIM and signal to email clients that you are you

DomainKeys Identification Mail (DKIM): standard that guarantees the sender is who they say they are and guarantees the contents of the message

Domain-Based Message Authentication, Reporting and Conformance (DMARC): created to prevent phishing attacks, enables you to see who is sending email on behalf of your domain—your brand—and prevent spammers from using it to send fraudulent email

Feedback Loop (FBL): a notification system that supplies marketers with insight into the subscribers who are clicking the “report spam” button

Internet Service Provider (ISP): provide mailboxes to end users as part of their paid services. These are generally your cable or internet providers, such as Comcast and Verizon

Secure Sockets Layer (SSL): often used interchangeably with Transport Layer Security (TLS) as they are both standard protocols used to secure email transmissions

Sender Policy Framework (SPF): where senders can specify which users can send email on behalf of their sending domain

Simple Mail Transfer Protocol (SMTP): an email communication protocol for sending email messages from one email account to another over the internet

STARTTLS: an email protocol command that tells an email server that an email client wants to turn an existing insecure connection into a secure one

Transmission Control Protocol (TCP): what an email client uses to initiate a “handshake” the the email server

Transport Layer Security (TLS): often used interchangeably with Secure Sockets Layer (SSL) as they are both standard protocols used to secure email transmissions

Share the email love

Share this ebook with other industry leaders to help them get more out of their email. Then, sign up for our newsletter to get up-to-date trends, email strategies, event invitations and more to help your business deliver profitable results.

Stay ahead of email trends