Senders Glossary

Email Deliverability Glossary

Everything you need to know

senders

Introduction

When it comes to email marketing, your mission is clear: reach your audience's inbox, engage them with compelling content, and drive conversions. But what happens when your carefully crafted messages get lost in your subscribers' spam folders? That's where email deliverability comes into play. Email deliverability refers to the ability of an email to land in the recipient's inbox instead of being flagged as spam or ending up in the promotions tab. A high email deliverability rate is critical to your email marketing campaign’s success, ensuring that your subscribers can see and act upon your messages.

One of the keys to unlocking great email deliverability lies in understanding the terminology that surrounds it. This guide will equip you with the knowledge you need to understand email authentication, bounce rates, blacklists, feedback loops (FBLs), graymail, IP reputation, list hygiene, spam scores, subscriber engagement, whitelisting, and more. By learning these key terms and best practices for email deliverability, you can ensure that your emails reach your subscribers' inboxes and drive the results you need to succeed.

The Importance of Email Deliverability

Email deliverability is essential for any successful email marketing campaign. When emails don't reach your subscribers' inboxes, it directly affects the success of that campaign. Poor email deliverability will lead to lower open rates, lower click-through rates, and decreased conversions overall.

When an email is not delivered correctly, it generally means that either the recipient's inbox provider has flagged the message as spam or it's been placed in their promotions tab instead of the primary inbox. If an email doesn't make it into the subscriber's primary inbox, it drastically decreases its chances of being seen and acted upon, resulting in poor results from your campaigns.

To maximize email deliverability and ensure your messages reach their destination, there are a few best practices you should follow:

First, focus on email authentication by setting up DKIM (DomainKeys Identified Mail), SPF (Sender Policy Framework), and DMARC (Domain-based Message Authentication Reporting & Conformance) on all domains sending emails from your organization. This will help to verify the sender's identity so that you don't find yourself blacklisted due to fraudulent activities by third parties, more specifically - it will let the recipient's servers know you are you, and not someone pretending to be you.

Next, focus on reducing the bounce rate by ensuring all contact information is valid and removing any bouncing contacts from your list regularly.

Finally, maintain a clear idea about who you've emailed and how many times you've emailed them with low or no engagement. Stop emailing folks who are clearly not engaging in any way in the same way and explore out a different way to engage with them.

By following these best practices for email deliverability you can minimize spam complaints and blacklistings as well as maximize open and click-through rates from each campaign — increasing conversions and ROI from your efforts overall.

If you didn't understand any of this, don't worry.

If you're new to email deliverability you probably didn't understand some or any of these terms. This is why we've created this Email Deliverability Glossary. It is a perfect start to getting to know the subject.

Email Deliverability Glossary - Everything you need to know about deliverability

Email Deliverability

Email Deliverability is a measure of how successful an email is at arriving at its intended destination, meaning the inbox of the recipient. Simply put, it's the ability of your email to get to your subscriber's inbox instead of their spam folder.

The importance of email deliverability cannot be overstated. Without it, recipients will never even see the messages you've so carefully crafted. And without reaching their inbox, your message is not effective.

Email Deliverability Fundamentals

Delivery (or Acceptance Rate) is a metric that measures the rate of emails that are successfully delivered and accepted by the recipient's email server, out of the total number of emails sent.

Email senders should aim to achieve high delivery rates to ensure that their messages reach the intended audience. Email delivery rates can be determined by measuring metrics such as bounce rates, spam complaints, and open rates. To improve delivery rates, email marketers should focus on maintaining a clean email list, using a reliable email service provider, avoiding spammy language or content, and authenticating their emails. Tracking acceptance rates is essential for analyzing email campaign performance and making changes that will improve future campaigns.

Deliverability (or Inbox Placement) is a vital email deliverability term that measures the rate at which emails are delivered to the recipient's inbox instead of the spam folder or not delivered at all. Achieving high deliverability rates is essential for email marketing success, as it ensures that messages are seen by the intended audience. Deliverability rates can be enhanced by maintaining a clean email list, following best practices for email sending, and adhering to email authentication protocols. Email marketers should monitor deliverability rates to assess campaign performance and make necessary changes.

Inbox Providers are companies that offer email services to users, allowing them to create and manage their email accounts. These providers operate email servers that manage the delivery of emails to the recipient's inbox. Some popular inbox providers include Gmail, Yahoo Mail, and Microsoft Outlook. Email marketers need to be mindful of inbox providers' email filters and rules, as emails that don't adhere to their policies may end up in the spam folder. Good relationships with inbox providers can increase email deliverability rates and improve overall email marketing success. To make sure messages reach their subscribers' inboxes, email marketers can follow inbox providers' best practices, such as avoiding spammy content, keeping their mailing lists clean, and respecting subscribers' privacy.

Email Service Providers (ESPs) are companies that offer email marketing services, allowing businesses to send large volumes of emails to their subscribers. ESPs provide tools for managing subscribers, designing and sending emails, and tracking and analyzing email campaign performance. They typically operate email servers that are optimized for deliverability, allowing them to help businesses achieve higher email deliverability rates. Some popular ESPs include Mailchimp, Constant Contact, and Campaign Monitor. ESPs often have pricing plans based on the number of subscribers and features included, making them accessible to businesses of all sizes. By using an ESP, businesses can streamline their email marketing efforts, improve email deliverability, and achieve greater campaign success.

Understanding Spam

Spam refers to unsolicited, unwanted emails. Spam is a message that is sent to a large audience of people who did not request it. The impact of spam on email deliverability is significant since it often causes recipients to report the email as spam or unsubscribe. Spam emails can negatively impact email deliverability and sender reputation.

Spam folder is a folder within an email inbox that contains messages that have been marked as spam by the email provider. These messages are generally filtered out of the inbox and into the spam folder, where the recipient can either delete them or review them separately from their regular email. The spam folder is designed to protect email users from unsolicited or unwanted emails and improve the overall email experience. However, it is still possible for legitimate emails to end up in the spam folder, which is why it is important for email marketers to focus on achieving high deliverability rates to ensure that their messages reach the intended audience.

Spam filters are used by inbox providers to prevent spam emails from reaching subscribers' inboxes. They use various criteria to identify spam emails, including sender reputation, email content, and email volume.

Spam filter triggers are specific words or phrases that trigger email filters to mark emails as spam and send them directly to the recipient's spam folder or reject them entirely. These triggers can include certain phrases like "free", "discount", or "guaranteed", as well as excessive use of punctuation, all caps, or too many images. Email senders need to be mindful of these triggers and avoid using them in their email content to improve email deliverability rates and avoid being flagged as spam.

Spam complaint occurs when a recipient reports an email as spam. High spam complaint rates can damage the sender's reputation and negatively impact deliverability rates. Email providers use spam complaints as a signal of spammy behavior and may penalize the sender by blocking their emails.

Spam score is a rating that measures the likelihood of an email being identified as spam by inbox providers. Spam scores are calculated using a variety of factors, including the email content, the sender's reputation, and the engagement rates of the audience.

Graymail refers to the emails that recipients have subscribed to but may not have the time or interest to read. They are not quite spam, but they aren't valuable to the recipient either. Examples of graymail include newsletters that are no longer relevant, promotions from brands that the user has not interacted with, and other untargeted marketing messages. While graymail doesn't generally cause email bounces, it can still hurt your deliverability rates if recipients mark your messages as spam.

Spam filtering is the process inbox providers use to detect and block unwanted emails based on sender reputation, content analysis, and engagement metrics. Filters assess factors such as email authentication, complaint rates, and suspicious patterns to determine whether an email should reach the inbox or be flagged as spam.

AI-driven spam filters use machine learning to analyze emails in real-time, adapting to evolving spam tactics. Unlike traditional rule-based filtering, AI continuously refines its detection models based on recipient behavior, message patterns, domain reputation, and historical engagement data. This makes inbox placement more dynamic, requiring senders to maintain strong engagement and consistent email authentication.

Advanced spam filtering goes beyond basic keyword detection by using AI-powered analysis, behavioral tracking, and predictive filtering. These systems evaluate email structure, historical sender reputation, and embedded link behavior to determine legitimacy. As filtering becomes more sophisticated, deliverability depends on engagement-based strategies, clean list management, and proper email authentication.

Reputation and Monitoring

Feedback Loop (FBL) is an automated system used by inbox providers to alert email senders when a recipient presses the "mark as spam" button. This feedback is sent to the sender so that they can adjust their sending behavior accordingly and improve their deliverability rates.

Engagement metrics refer to the measures of how recipients interact with email messages. They include indicators such as open rates, click rates, reply rates, and conversion rates. These metrics are important for us to understand the success of an email marketing campaign and determine the effectiveness of a message's content, subject line, and overall strategy. By analyzing engagement metrics, marketers can tailor their future email campaigns, segment their lists, and ensure they're sending targeted, relevant content that will resonate with their audience.

Seed list is a pre-determined list of email addresses used to monitor email campaigns' deliverability. Seed lists are usually used for testing before a campaign is sent out to the full email list.

Seed testing is a form of testing that involves sending email messages to a set of test email addresses, known as "seeds." Seed testing can help email marketers assess deliverability rates and identify potential issues before sending messages to their full email lists.

Email reputation is a score assigned to a sender's domain and IP address based on engagement rates, complaint levels, and compliance with best practices. Internet Service Providers (ISPs) and spam filters use email reputation to determine whether to deliver an email to the inbox, promotions tab, or spam folder.

A strong email reputation results in higher inbox placement and better engagement, while a poor reputation leads to increased filtering, blocked emails, or blacklisting. Maintaining low spam complaints, proper authentication (SPF, DKIM, DMARC), and high engagement rates is critical for protecting email reputation.

Reputation monitoring is the practice of regularly monitoring and tracking a sender's email reputation to ensure optimal email deliverability. There are a variety of reputation metrics that can be measured, including sender score, IP reputation, domain reputation, and complaint rates. By analyzing reputation metrics, email marketers can identify potential issues and proactively address them before they negatively impact deliverability. Reputation monitoring can be achieved through a variety of tools, including email service providers and deliverability monitoring platforms. By regularly monitoring email reputation and taking proactive measures to maintain a positive reputation, email marketers can improve their email deliverability and ensure that their messages are reaching the intended audience's inbox.

An email deliverability consultant is an expert specializing in diagnosing and resolving issues that affect inbox placement, sender reputation, and overall email performance. Their role involves in-depth analysis of bounce rates, spam complaints, authentication protocols (SPF, DKIM, DMARC), engagement metrics, and blocklist status to identify deliverability challenges.

A deliverability consultant ensures that email-sending infrastructure aligns with industry best practices through strategic list management, domain reputation monitoring, and warm-up protocols. They also provide compliance advisory on GDPR, CAN-SPAM, and other regulatory frameworks, mitigating risks associated with poor sender reputation. By optimizing authentication, monitoring deliverability signals, and implementing corrective measures, an email deliverability consultant enhances email performance and ensures long-term inbox placement stability.

List Management

Whitelist is a list of IP addresses and domains that have been identified as legitimate and trusted senders. Email filtering systems use whitelists to allow emails from these sources to bypass spam filters and be delivered directly to recipients' inboxes. Emails from these addresses and domains are less likely to be blocked or sent to the spam folder.

Blacklist is a list of IP addresses and domains that have been identified as sending spam or unwanted emails. Inbox providers use blacklists to block emails from these addresses and domains. Being blacklisted can severely damage your email deliverability and should be avoided.

IP blacklisting is a process where an email sender's IP address is added to a list of blocked IPs, preventing them from delivering emails to specific email providers or domains. This may occur due to issues like high email bounce rates, sending spam or misleading content, or sending emails to non-opt-in email lists. When an IP is blocked, emails sent from that IP will not be delivered to recipients on that blacklist. This can have serious consequences for email marketing campaigns as it can lead to poor deliverability rates or even complete email delivery failure. To avoid IP blacklisting, businesses should ensure that their emails adhere to email providers' guidelines, maintain a clean email list, use proper email authentication protocols, and monitor their email campaign performance regularly.

Domain Blacklisting is a process where a domain name associated with an email address is added to a list of blocked domains by email providers or spam filters. When an email sender's domain is added to a blacklist, it may prevent them from delivering emails to specific email providers or domains, leading to poor email deliverability rates or failed email delivery altogether. The reasons for domain blacklisting may include issues like sending spam or misleading content, high spam complaint rates, or sending emails to non-opt-in email lists. To avoid domain blacklisting, businesses should regularly monitor their email campaigns and comply with email providers' guidelines. They should also maintain a clean email list, use email authentication protocols like SPF, DKIM, and DMARC, and provide a clear opt-out mechanism for subscribers wishing to stop receiving emails.

Email Warming

Email warming or email warm-up is the gradual process of building up the reputation of a new email address or improving the reputation of an underperforming one. This is achieved by gradually increasing the volume of emails sent over time and gradually introducing more robust email content and list segments. A proper email warm-up can help avoid sending your emails to spam folders. A successful email campaign takes time and patience, and email warming is a crucial component of the process.

Warm-up schedule is a plan that outlines the gradual increase of email volume and frequency over a given period of time. It is an essential part of the email warming process, which helps to establish a positive sending reputation and improve email deliverability. The specific details of a warm-up schedule will depend on a variety of factors, including the sender's email list, email content, and sending habits. Generally, a warm-up schedule involves progressively increasing the number of emails sent each day or week while monitoring engagement and deliverability metrics. Adhering to a warm-up schedule can help ensure that email campaigns are delivered successfully and effectively reach their intended audience.

Filtering and Testing

Email filters are used by email providers (ISPs) to determine whether an email should be sent to the recipient's inbox or to their spam folder. Filters use a variety of factors to make this determination, including the sender's reputation, the email's content, and the recipient's engagement history.

Deliverability monitoring refers to the process of regularly monitoring and assessing the success of email deliverability. The goal of this monitoring is to ensure that emails reach the intended recipients' inboxes rather than being classified as spam or undelivered. Deliverability monitoring involves tracking key metrics such as bounce rates, spam complaints, and inbox placement rates. It also often involves using email deliverability tools to identify and address any issues that may be negatively impacting deliverability. By regularly monitoring deliverability and making necessary adjustments, marketers can optimize their email campaigns and improve their chances of successfully reaching their audience's inboxes.

Email deliverability is crucial to the success of any email marketing campaign. Understanding the terminology around email deliverability is the first step in ensuring your messages reach your audience's inbox. From authenticating your emails with DKIM and SPF to monitoring your IP reputation, there are many tools and practices you can use to increase your email deliverability rates. This glossary provides a brief overview of some basic terms which we will discuss in more detail later.

Data and Privacy

First-party data refers to information collected directly from users through their interactions with a brand, including email engagement, website activity, and purchase history. Unlike third-party data, which is sourced externally, first-party data is owned and controlled by the sender, ensuring higher accuracy, compliance with privacy regulations, and stronger email performance.

In email deliverability, first-party data is critical for maintaining a high sender reputation. Emails sent to verified, engaged recipients reduce bounce rates, minimize spam complaints, and improve inbox placement. ISPs evaluate engagement metrics such as open and click rates to determine sender credibility, making first-party data a foundation for sustainable email marketing success. As third-party tracking diminishes, leveraging first-party insights is essential for optimizing email campaigns, maintaining compliance, and achieving long-term deliverability.

The post-cookie era refers to the shift away from third-party cookies as a tracking and targeting mechanism in digital marketing. With major browsers phasing out third-party cookies due to privacy regulations like GDPR and CCPA, businesses must rely on first-party data and alternative tracking models to maintain audience insights and campaign performance.

This transition reinforces the importance of consent-based marketing and authenticated sender practices for email deliverability. In the post-cookie era, without third-party tracking, brands must focus on email engagement signals—such as open rates, clicks, and replies—to optimize inbox placement. Strong domain reputation, proper authentication (SPF, DKIM, DMARC), and strategic list management become even more critical as inbox providers increasingly prioritize direct user interactions over external data signals.

Third-party cookies are tracking files placed on a user's browser by a domain other than the one they are visiting. These cookies have traditionally been used for cross-site tracking, ad targeting, and audience profiling. In email marketing, third-party cookies allow brands to track recipient behavior beyond email interactions, such as website visits and ad engagement, enabling more precise retargeting.

However, as privacy regulations like GDPR and CCPA strengthen consumer data protections, and major browsers phase out third-party cookies, their role in email marketing is diminishing. This shift pushes senders to rely on first-party data and engagement-based metrics—such as opens, clicks, and replies—to optimize deliverability and inbox placement. With email providers prioritizing direct interactions over external tracking signals, authenticated sending practices and strategic list management are becoming essential for maintaining sender reputation and avoiding spam filters.

B2B Email Deliverability

B2B (Business-to-Business) refers to transactions, marketing, and communications between businesses rather than between a business and individual consumers (B2C). In email marketing, B2B focuses on engaging professionals, decision-makers, and stakeholders within companies. Unlike B2C email marketing, which targets mass audiences, B2B email strategies prioritize personalization, relationship-building, and providing value-driven content such as case studies, whitepapers, and industry insights.

B2B emails often encounter stricter deliverability challenges, as corporate email systems use advanced filtering mechanisms to block unsolicited messages. Proper authentication, sender reputation management, and engagement-driven outreach are essential for ensuring successful inbox placement and avoiding spam filters in business environments.

B2B email deliverability refers to the ability of emails sent to business recipients to successfully land in their inboxes instead of being blocked by corporate spam filters, firewalls, or security gateways. Unlike consumer email providers, business email systems such as Microsoft Exchange, Google Workspace, and enterprise-level filters impose stricter security protocols to protect organizations from phishing and spam.

Key factors affecting B2B email deliverability include sender reputation, domain authentication (SPF, DKIM, DMARC), list quality, and engagement signals such as replies and forwards. Cold emails and outbound campaigns face additional scrutiny, requiring gradual warm-up strategies, compliance with opt-in regulations, and highly relevant messaging to avoid being flagged as spam. Maintaining a strong IP reputation and domain health is crucial for ensuring consistent inbox placement in B2B email marketing.

B2B email marketing campaigns are structured outreach efforts targeting business professionals to generate leads and build relationships. Unlike B2C campaigns, which focus on consumer engagement at scale, B2B email marketing requires personalization, high-value content, and credibility to reach decision-makers.

Deliverability in B2B email marketing presents unique challenges, as corporate email servers use stricter spam filters and security measures. Senders must maintain a strong domain reputation, implement proper authentication (SPF, DKIM, DMARC), and ensure list hygiene to prevent high bounce rates. Engagement signals such as opens, clicks, and replies are key factors in achieving inbox placement, as business email providers prioritize relevant, trusted communications.

As third-party tracking declines and privacy regulations increase, B2B marketers must rely on first-party data and permission-based strategies to maintain deliverability. A focus on segmentation, engagement, and sender reputation ensures consistent inbox placement and long-term success.

B2B outbound refers to proactive email outreach where businesses initiate contact with potential clients, leads, or partners rather than waiting for inbound inquiries. This includes cold email campaigns, sales prospecting, and targeted networking outreach. Unlike inbound marketing, which attracts prospects through content and organic channels, outbound email marketing relies on strategic targeting, personalization, and follow-up sequences to generate interest and engagement.

Because unsolicited emails are subject to strict filtering and compliance regulations, B2B outbound email deliverability requires a clean sender reputation, proper domain authentication, and precise audience segmentation. Emails must be relevant, non-spammy, and aligned with the recipient's industry, interests, and business needs to maintain a high response rate and avoid blacklisting.

B2B outbound marketing strategies involve structured approaches to reaching potential business clients through cold emails, direct outreach, and personalized follow-ups. Unlike inbound marketing, which passively attracts leads, outbound strategies require active prospecting, engagement tracking, and continuous optimization to drive results.

A well-executed B2B outbound marketing strategy relies on precise audience targeting, message personalization, and maintaining a warm sender reputation to ensure high deliverability. Avoiding spam filters requires a strong domain reputation, authentication protocols (SPF, DKIM, DMARC), and compliance with data privacy regulations such as GDPR and CAN-SPAM. Ongoing list validation, engagement monitoring, and iterative improvements help maximize conversions while preserving sender credibility.

senders

www.senders.co