litmus

33 Email Deliverability Terms to Know

Email deliverability is tricky. But the more you know–including these 33 deliverability-related terms– the more empowered you are as an email marketer.

The basics

1. **Delivery**. Whether or not a receiver accepts the message you've sent.
2. **Deliverability**. The rate at which your emails make it into your subscribers' inboxes instead of being labeled as spam and going to the junk folder.
3. **Email Service Providers (ESPs)**. Technology companies that provide platforms to send commercial and transactional email on a sender's behalf.
4. **Internet Service Providers (ISPs)**. Provide mailboxes to end users as part of their paid services. These are generally cable or internet providers, such as Comcast, Spectrum, AT&T or Verizon.
5. **Inbox Providers/Mailbox Providers (MBPs)**. ISP-provided inboxes, paid or free webmail accounts, and email apps. Examples include Apple, Microsoft, Gmail, and Yahoo Mail.
6. **IP Address**. A number that uniquely identifies any device connected to the internet. "IP" stands for "Internet Protocol." Similar to how a street address helps people find buildings, an IP address helps computers find each other on the internet.
7. **Domain**. Similar to an IP address, domain names refer to locations of servers and devices connected to the internet. Domain names can represent a whole bunch of different IP addresses. For example, the domain www.litmus.com would address the collection of servers that host our website. Whether that is *www.litmus.com/blog* or *www.litmus.com/community*, the domain is the same.
8. **Sub-domain**. In our case, litmus.com is our domain name; e.litmus.com is a sub-domain of litmus.com that we use for marketing emails. Subdomains are useful, as they can be used to isolate mail streams from one another for both branding and reputation reasons.

Sender reputation

9. **IP Reputation**. IP addresses uniquely identify you and your server (see above). Reputation is attributed to an IP address based on what metrics an ISP has historically seen from that IP address and how users engage with mail that originates from it.

10. Domain Reputation. Email isn't always sent from just one IP address or provider, so using your sending domain to track reputation allows a receiver to accumulate a reputation score across the board.

11. **Domain Name System (DNS)**. This is a way of resolving a domain name into an IP address. It's basically like a telephone book that keeps track of everything.

12. **MX, or Mail Exchange, DNS Record**. This is a specific type of DNS record specifying where mail that is destined for a domain name should be sent. It denotes the host responsible for receiving mail, not the sender. Essentially, it's the server that mail for that domain is sent to.

13. **TXT DNS Record**. A place to store extra information about the domain, often arbitrary text or binary data. TXT records may be used for authentication purposes.

14. **Uniform Resource Identifier (URI)**. A domain plus more information about what we want from that server. When we think of a URL, it's actually a type of URI identifying a resource by its primary access point (its "location" on the web).

Sending emails from a cold IP address is a sure-fire way to land in the spam folder. Discover how to **warm up your IP address** and ensure your emails land in the inbox, nice and toasty!

LEARN MORE

Authentication & structure

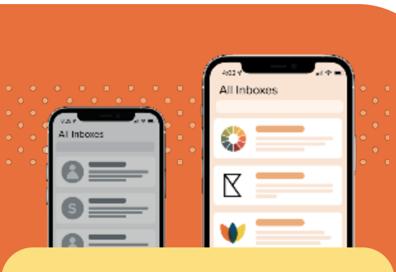
15. Brand Indicators for Message Identification (BIMI). A text record that is used to verify information about your brand that works right alongside SPF, DMARC & DKIM and signal to email clients that you are you.

16. **Sender Policy Framework (SPF)**. A sender policy framework allows mail services to double check that incoming mail from a specific domain has, in fact, been sent from that domain. SPF protects the envelope sender address, or return path. It compares the sending mail server's IP address to a master list of authorized sending IP addresses as part of the DNS Record (see above).

17. **DomainKeys Identified Mail (DKIM)**. This allows your organization to claim responsibility for your email. It's an identifier that shows your email is associated with your domain and uses cryptographic techniques to make sure it should be there.

18. Domain-Based Message Authentication, Reporting, & Conformance (DMARC). Designed to combat phishing, DMARC gives you insight into the abusive senders that may be impersonating you—and can help you identify them. It allows a sender to indicate that an email is protected by SPF or DKIM. The sender can then receive a report back on any messages that failed the authentication and identify if anyone using the domain could be a spammer.

BIMI allows you to display a sender logo with your emails, when verified under a set of BIMI specifications. It's a way to verify information about your brand. Discover how to be BIMI-ready with our guide to getting started.



DOWNLOAD

Subscriber behavior & engagement

19. **Spam Complaints.** When your recipient marks your email as spam. It could be the recipient felt you didn't have permission to email them, you were emailing too frequently, or were sending irrelevant content.

20. **Feedback Loops.** Allow the sender to receive a report every time a recipient clicks on the "mark as spam" or "junk" button. To maintain a clean email list, you can then suppress, or prevent, unwanted messages from appearing in that particular inbox. Subscribing to feedback loops and using this data to quickly remove folks no longer interested in your email helps to maintain a positive reputation. (It's also part of fixing your sender reputation).

21. **TINS (This Is Not Spam)**. By marking something as NOT spam, your subscribers may save you from the spam filter. This requires them to go into their spam folder and manually allowlist your address.

22. **Allowlist**. The opposite of a blocklist, this means your server is considered spam-free or is an "approved sender." It's often used by email applications to allow users to mark whether or not they trust emails from specific senders. This overrides some of the filtering that may exist from the ISP. You can also apply for allowlisting programs that a few ISPs offer.

23. **Spam Traps**. Spam traps are commonly used by inbox providers and blocklist providers to catch malicious senders. But, quite often, legitimate senders with poor data hygiene or acquisition practices end up on the radar as well. A spam trap looks like a real email address, but it doesn't belong to a real person and isn't used for any kind of communication. Its only purpose is to identify spammers and senders not utilizing proper list hygiene.

24. **Typo Traps**. A type of spam trap. 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. These addresses are most likely caused by human error.

25. **Recycled Traps**. Another type of spam trap. Emails/domains that previously were a legitimate recipient but have been fully idle for a time period (typically at least a year).

Subscriber behavior & engagement *cont.*

26. **Pristine Traps.** Another type of spam trap. 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.

27. **Parked Traps**. Not actually a spam trap, but behave like one. Domains are 'parked' at a registrar or monetization site.

28. **IP Blocklisting**. When you send an email, it will originate from an IP address. When an IP is blocklisted this indicates to anyone who utilizes that blocklist to block the mail originating from that IP address.

29. **Domain Blocklisting**. If your domain appears frequently in emails that hit spam traps, there may be a chance that your entire domain will be blocklisted. This can be even more damaging as the block is not localized to just an IP address, thus affecting you across all your sending platforms.

Find out why emails go into the spam folder and most importantly how to avoid it in our webinar featuring experts from Salesforce, Yahoo, and SocketLabs.

LEARN MORE

Tracking performance

30. **Hard Bounce**. Hard bounces occur when the receiving server is either unable to deliver or rejects the message. Hard bounces typically indicate permanent delivery issues. It can also occur when there is no mail server at that address, or the domain doesn't exist at all. This can be caused by anything from typos to deleted user accounts. In most cases, if you receive a hard bounce, immediately removing them from your list is the best course of action. (This doesn't necessarily mean deleting them; you can deactivate them or add them to a suppression list).

31. **Soft Bounce**. A soft bounce means that the recipient exists, but for whatever reason, they couldn't receive your message. Soft bounces typically indicate temporary delivery issues. Though this isn't your fault, you should eventually consider them to be the same as hard bounces. It could also mean the email you sent exceeded the maximum size the subscriber's inbox allows. In addition, Rate-Limiting or Throttling might be at play. If you send large volumes of email to the same ISP, you might start being throttled.

32. **Spam Complaint Rate**. How many people report or mark your email as spam, calculated by number of spam complaints / number of emails delivered x 100. Anything above 0.1% is concerning.

33. **Inbox Placement Rate (or Deliverability Rate)**. How many of your emails land in the inbox vs. the junk or spam folder, calculated by number of non-junked emails delivered / number of emails delivered x 100. Less than 80% is considered low.