litmus

35 Email Deliverability Terms to Know

Email deliverability is tricky. But the more you know–including these 35 deliverability-related terms–the more empowered you are as an email marketer.

1. **Email Delivery.** Whether or not a receiver (mailbox provider) accepts the message you've sent.

2. **Email 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.

Sender Reputation and Authenitcation

3. **IP Reputation.** IP addresses uniquely identify you and your server. 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.

4. **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.

5. **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).

6. **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.

7. **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.

Sender Reputation and Authenitcation *cont.*

8. **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.

9. **DNS Record.** A naming database where your domain name is located and translated into an IP address. Basically, it's where all of your authentication protocols live.

10. **MX (Mail Exchange) Records.** A DNS Mail Exchange (MX) record tells mail servers where to direct an email message in accordance with the Simple Mail Transfer Protocol (SMTP). This is the back-end magic that connects your message to the right email address. Failure to configure your MX record correctly could result in a higher bounce rate or delivery issues, which in turn impact your deliverability.

11. **IP Warming.** The process of slowly increasing the volume of email you send from a new domain or IP address. Whether you're switching to a new email service provider (ESP), getting started sending emails for the first time, or going through a merger or acquisition, IP warming can help maintain your deliverability.

12. **DNS Pointer Record (PTR Record).** DNS PTR Records help you match IP addresses to sender domain names. When you run a reverse DNS lookup with your IP address, the PTR record finds the domain name. (This is the opposite of an "A" record, which gives you the IP addresses associated with a given domain name.)

13. **Greylisiting.** An email security practice mail servers use to protect their users from senders they haven't received mail from before. Rather than completely block your message, your email will be temporarily rejected.

14. **Email Sender Reputation.** A score that Internet Service Providers (ISPs) assign to an organization that sends emails. ISPs evaluate your sender behavior, your infrastructure, and your subscriber behavior to determine your sender reputation.

Email Performance and Subscriber Behaviour

15. **Open Rate.** Measures how many of your delivered emails were opened. This can be a useful indicator of your subject line and preview text performance.

16. **Click-Through Rate (CTR).** Determines how many clicks your emails received. You can calculate click-through rate by dividing the number of emails clicked by the number of emails delivered. Taking opens out of the equation gives you a more accurate picture of email engagement.

17. **Rendering Issues.** These occur when email clients change the display of how your email appears that make it difficult or impossible to interact with. Rendering issues can make your email campaigns look a little spammy to ISPs.

18. **User Engagement.** Refers to how your subscribers view and interact with your emails. Think of your user engagement metrics as that sweet spot in the middle of the funnel, which includes open rate, click rate, and read time. ISPs look at your user engagement to determine your inbox placement—the more your subscribers interact with your emails, the better your deliverability will be.

19. **Unsubscribe Rate.** Measures how many people opt-out of your emails. Depending on your email platform, an "unsubscribe" could be if someone actually opts out or if they click your unsubscribe link but don't follow through.

20. **Feedback Loop (FBL).** Feedback loops allow the sender to receive a report every time a recipient clicks on the "mark as spam" or "junk" button. Subscribing to feedback loops and using this data to quickly remove folks who are no longer interested in your email helps maintain a positive reputation.

21. **Spam Complaints.** When a recipient marks your email as spam. This is an example of negative engagement—you're probably not a spammer, but for whatever reason, your subscriber doesn't want to see your emails anymore. This is why it's so important to make it easy for subscribers to unsubscribe. While no one likes a high unsubscribe rate, a high spam complaint is much worse for your overall deliverability.

22. **Bounce Rate.** This is how many of your sent emails weren't delivered. This can be for temporary reasons like a too-full inbox (soft bounces) or permanent reasons like an incorrect email address (hard bounces).

23. **Soft Bounce.** A soft bounce means that the email recipient exists, but for whatever reason, they couldn't receive your message. Soft bounces typically indicate temporary delivery issues, so keep an eye on an email address that keeps bouncing—you may need to clean it from your list.

Email Performance and Subscriber Behaviour *cont.*

24. **Hard Bounce.** These occur when the receiving server is either unable to deliver or rejects the message. It can also occur when there is no mail server at that address, or the domain doesn't exist at all. A hard bounce indicates a permanent reason that an email can't be delivered, so you should remove them from your email list with immediate effect.

25. **Inbox Placement Rate (IPR).** Tnbox placement rate shows the percentage of emails that get delivered to a subscriber's primary inbox, rather than the spam folder or other folders like Gmail's Promotions Tab. It's important to track all of these metrics when thinking about your deliverability. But if you were going to pick one to focus on, it's your inbox placement rate (IPR).

List Management and Hygiene

26. **List Hygiene.** List hygiene, or list management, is the practice of maintaining an email list of subscribers that actually want to hear from you. Proper list hygiene requires regular checks of your email list for typos, outdated email addresses, or subscribers who have stopped engaging with your emails altogether.

27. **Opt-In.** Another way of saying that someone has subscribed to your list. The right opt-in practices can prevent list hygiene issues in the first place—like watching for common typos like "gmial" instead of "gmail." There are two kinds of opt-in practices, single opt-in and double opt-in:

List Management and Hygiene cont.

28. **Single Opt-In (SOI).** This is when someone subscribes to your mailing list without confirming their email address. Once they type in their email address and click "subscribe," they're in. This is a popular acquisition method because it reduces the number of steps subscribers have to take to sign up, but it can make it more difficult to catch typos, bounced email addresses, or spam traps.

29. **Double Opt-In (DOI).** Also known as confirmed opt-in (COI), double opt-in is when someone subscribes to your mailing list and then must confirm their email address in a two-step process.

30. **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.

31. **Opt-Out.** Opt-out is another word for unsubscribing, or when someone requests to no longer receive your emails.

32. **Spam Folder.** Also known as the "junk" folder or spam filter, it is designed by ISPs to filter out suspicious emails. Spam filtering has become so sophisticated that sometimes email marketers can get caught, too. If you're consistently landing in the spam folder, you need to evaluate your email marketing strategy.

33. **Blocklist.** A blocklist is a list of IP addresses or domains that are known to be associated with malicious spammers.

34. **Allowlist.** Allowlist, previously known as a whitelist, is the opposite of a blocklist. Your subscribers can save you from the spam filter by explicitly telling their mailbox provider that they want to receive your messages.

35. **Email Throttling.** Email throttling is when an ISP limits the amount of emails accepted from a sender during a certain time period.