

# Do you speak deliverability? Here is a glossary of important terms to know:

**Blacklists** – Lists of IP addresses or domains suspected of sending spam. Maintained by ISPs and service providers such as Barracuda, Frontbridge, Invalvement, Spamhaus, etc.

**Bounce Rate** – The percentage of email messages that failed to reach recipients. Divided into **a) soft bounce:** email address is temporarily unavailable (e.g. mailbox is full, server is down) and **b) hard bounce:** address is permanently unreachable (e.g. mailbox non-existent, typo in address).

**California Consumer Privacy Act (CCPA)** – In place since January 1, 2020, enhances privacy rights and consumer protection for residents of California, United States.

**CAN-SPAM** – The ‘Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003’ defines legal boundaries for the commercial usage of email, including consumers’ rights to opt-out/unsubscribe at any time.

**Click-Through Rate (CTR)** – Percentage of how many successfully delivered emails garnered at least one click. This number shows whether or not your audience finds the emails you send relevant enough to click through for more.

**Click to Open Rate (CTO)** – Percentage of people who open an email at least one time. Also named Reactivity Rate. This number indicates how effective the performance of the email was and if it created a level of interest by the recipient to click through and learn more about the content within the email.

**Complaints** – Number of times users report messages from a domain as spam (also known as Spam Reports). Seriously hurts sender reputation all the way to blacklisting.

**Delivered Rate** – Percentage of messages accepted by an Internet Service Provider. Indicates messages were not rejected but does not imply delivery to inbox.

**Delivery Rate** – Percentage of messages successfully leaving ESP servers. Important: Not the number of messages actually reaching recipients’ inboxes.

**DKIM (DomainKeys Identified Mail)** – The digital signature proving that a message actually originated from the domain name in its email address.

**Domain-based Message Authentication (DMARC)** – Protects the owner of the domain against phishing.

**Domain Reputation** – A record of sender behavior logged by their domain name (as opposed to IP address).

**General Data Protection Regulation (GDPR)** – Regulates data protection for individuals within the European Union, with enhanced rules on consent to marketing participation.

**IP Reputation** – Trustworthiness of senders determined by tracking traffic sent from their IP address.

**List Hygiene** – Continuous process of maintaining email lists with valid addresses, e.g. by deleting hard bounces, non-respondents, and opt-outs.

**Open Rate** – Percentage of your audience that opens the emails you send them. A great view rate usually indicates that subject lines resonate with your audience.

**Sender Score** – Measure of trustworthiness of an IP address assigned by an email provider or filtering system. IPs with Sender Scores below 70 points are likely to see all sent emails filtered/blocked; above 70 points, individual emails/campaigns are filtered.

**Spam** – Unsolicited email, also known as “junk” email, often sent in bulk and with malicious intent.

**Spam Trap** – After receiving continuous hard bounces to an invalid email address, ESPs can turn that address into a spam trap and report senders targeting the “dead” address as spammers (avoided by list hygiene).

**SPF (Sender Policy Framework)** – Official Domain Name Server (DNS) record indicating an IP address has permission to send your email. Messages without SPF authentication will be blocked categorically.

**Unsubscribes** – Number of users who choose to opt-out of email list.

