



Ebook:

THE MASTER LIST OF EMAIL DELIVERY TERMINOLOGY

ORACLE® + Dyn

 dyn.com

 603 668 4998

 @dyn

Ebook: The Master List of Email Delivery Terminology

Inbox Acceptance Isn't a Right. It's a Benefit of Doing It Right.

Despite email volume continuing to rise year over year, getting email into the inbox continues to remain a significant challenge, even for reputable senders. With Dyn Email Delivery, that challenge becomes exponentially easier thanks to reliability, scalability, and ease of use.

For over a decade, Dyn has helped those with large sending needs overcome the challenges of inbox placement for both bulk email (one to many) and transactional email (one to one) through sending on one of the industry's cleanest, cloud-based networks.

Get more email into the inbox and minimize your pain points with Dyn Email Delivery.

Table of Contents

3	Alt Tags
4	DMARC
5	Feedback Loops
6	Soft Bounce
7	Suppression
7	Whitelist

3rd Party List: A third-party list is one that is purchased, rented, or somehow obtained from an outside company. The email addresses on the list have not specifically signed up to receive mail from your company, but have opted in through the other company to receive mail. It is a best practice not to send from third-party lists unless you have trust that the email addresses on the list are expecting your mail. This can lead to high complaint rates and these lists can sometimes include spam traps or harvested email addresses.

Alt Tags: Alt tags provide alternative text on an image that is displayed if the email client is set to not display images or if a slow connection has delayed the load of an image. Example:

```

```

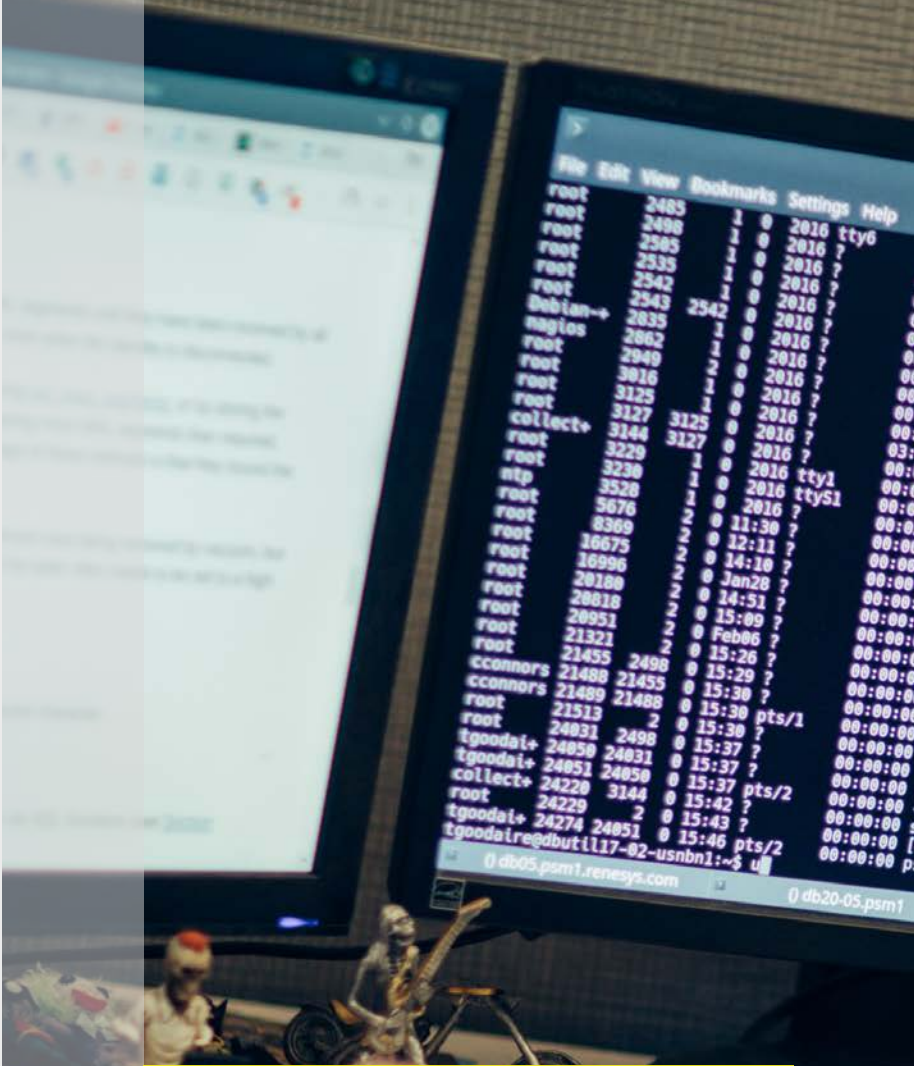
Authentication: Authentication lets ISPs and mailbox providers know that the emails you are sending are approved to be sent by the domain they are coming from and are not spam or phishing emails.

Blacklist: Special lists, maintained by spam filtering companies or organizations, that attempt to identify known servers, IP addresses, and/or domains that spammers use. These lists then can be subscribed to by other mail servers to reject spammers' mail as quickly as possible.

Bulk Mail: Bulk mail is commercial mail sent out by companies. Any email marketing campaign is bulk mail (newsletters, promotions, coupons, etc.). Bulk mail is sent out to entire lists at once.

CAN-SPAM: The Controlling the Assault of Non-Solicited Pornography and Marketing Act was a law passed in the United States in 2003 to set standards on sending email.

Click: A click is defined when a email recipient clicks on a link within a message. Unique clicks only count one click per user, meaning that if one recipient clicked a link multiple times, only their initial click is counted.



Whether you click the unsubscribe link or the spam button makes a difference. Be sure to click unsubscribe instead of spam if you're just sick of receiving a newsletter that you signed up for.

Complaint: When an email recipient hits the spam button in their inbox, an email provider’s spam filtering will often record this as a complaint and prevent future email from that sender from reaching the inbox. Some email providers will provide a feedback loop of complaints, so that senders can be informed and keep their lists clean. Complaints should be kept as low as possible. Otherwise, the IP address may be blacklisted.

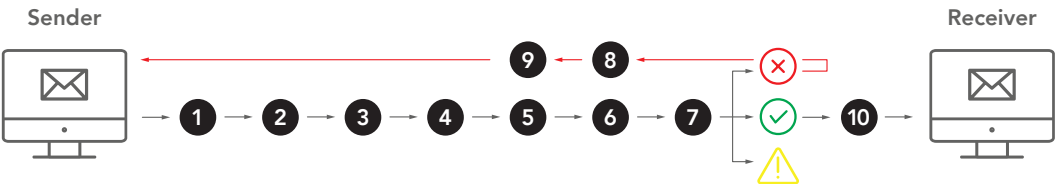
Content Filters: Content filters are spam filters that review the content of an email to attempt to make a decision on whether that email should go to the spam folder or inbox. These systems often scan for keywords, text-to-image ratios, templates, and other content based items.

Dedicated IP Pool: One or more IP addresses set aside for use by a single company, sender, or domain for sending email.

Deliverability: The measurement of a message’s ability to successfully be delivered to the intended recipient. Inbox deliverability refers to the amount of actual inboxes that the message reached, excluding delivery to junk folders.

DKIM: DomainKeys Identified Mail is an email authentication framework system that allows mailbox providers to validate mail from your domain against a public (DNS) and private (embedded within the email) key, thus validating mail from your domain, protecting your brand and customers.

DMARC: Domain-based Message Authentication, Reporting & Conformance is a standard using SPF & DKIM to authenticate email sends in order to help eliminate phishing emails.



The DMARC Processs

- 1 Email deployed by sender
- 2 Mail server inserts DKIM Header
- 3 Email sent to receiver
- 4 Standard validation tests (IP blocklists, sender reputation, rate limits etc.)
- Validate and apply sender DMARC policy:
- 5 Retrieve validated DKIM domains
- 6 Retrieve "envelope form" via SPF
- 7 Apply appropriate DMARC Policy
- If failed/quarantined:
- 8 Failure Report
- 9 Update periodic aggregate report
- If passed:
- 10 Standard inbox processing before delivery to sender. (anti-spam filters, etc.)

DNS: Domain Name System helps your ISP communicate with network servers when you are trying to reach IP addresses that your computer or recursive ISP server does not have in memory. DNS can turn an IP address into a host name or vice versa.

Double Opt-In List: Recipients that are double-opted in have gone through an initial signup (first opt-in) and then received an email in which they take a second action (second opt-in), most often by clicking a link where their intent to opt-in to your email list is confirmed.

Engagement: Engagement refers to how recipients of email interact with messages they receive. An engaged user opens the email, reads it, and maybe clicks a few links. An unengaged user either never opens a message, or quickly closes or deletes it after opening.

ESP: Email Service Provider refers to the company that provides the capabilities for end users to send email.

Feedback Loops: Feedback loops are channels of communication between mailbox providers and email senders that allows those providers to communicate any message that was identified as spam by a recipient. These need to be manually established at each mailbox provider that allows for feedback loops.

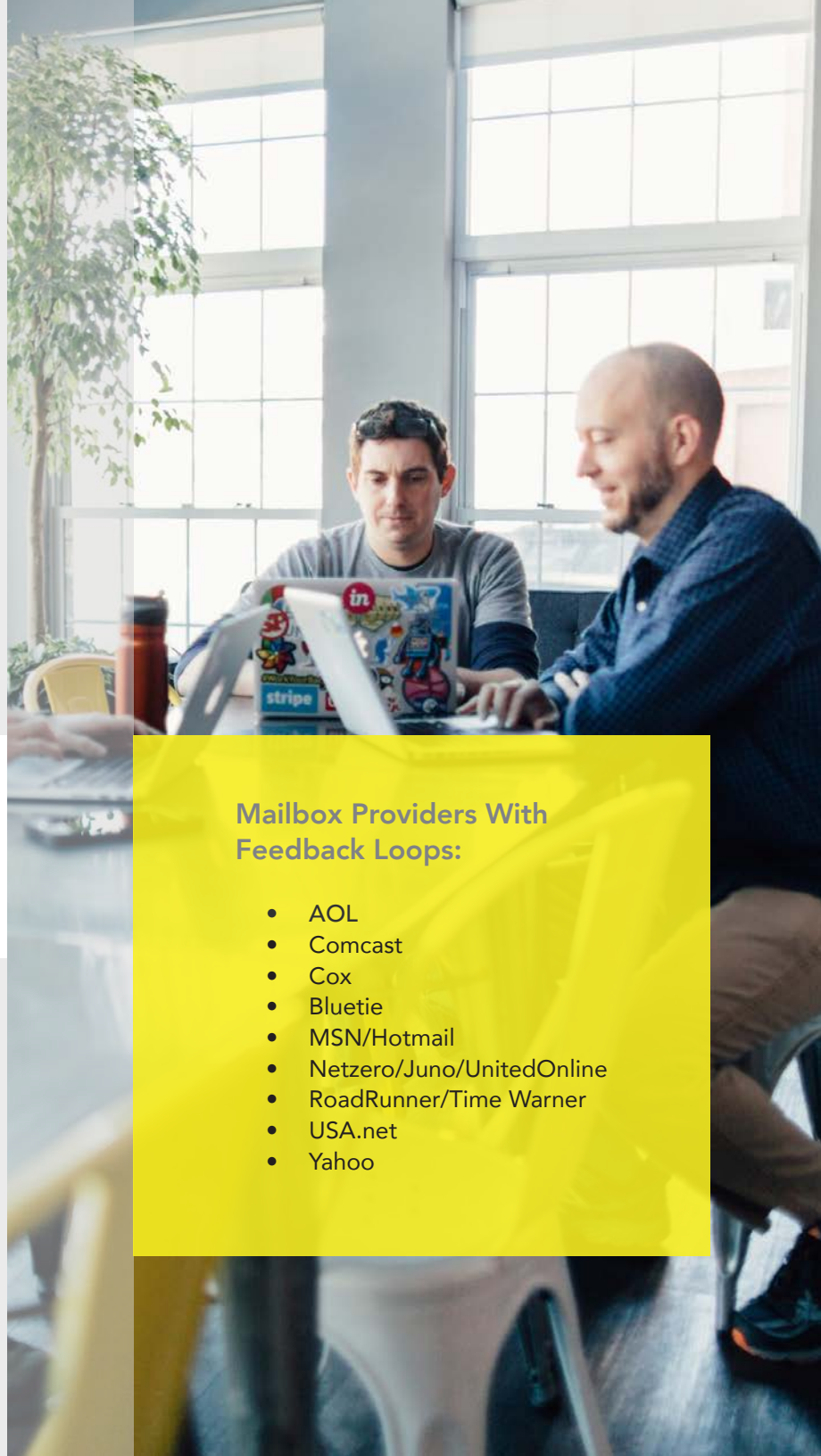
Hard Bounce: Hard bounces occur when a mailbox provider indicates that the email address you used is not valid. Most often, this happens because the email address does not exist. You should not try to email this address again in the future.

IP Address: An Internet Protocol address is a unique identifier for any device within a network on the Internet.

ISP: Internet Service Providers are those providing their customers access to the Internet. They are also commonly called mailbox providers (e.g. Comcast, AT&T, Verizon).

Mailbox Providers With Feedback Loops:

- AOL
- Comcast
- Cox
- Bluetie
- MSN/Hotmail
- Netzero/Juno/UnitedOnline
- RoadRunner/Time Warner
- USA.net
- Yahoo



List Maintenance: Maintain your email lists by removing hard bounces, people who unsubscribe, and possibly creating suppression lists for unengaged users. List maintenance is crucial for keeping a good sender reputation and deliverability high.

Mailbox Provider: A mailbox provider, commonly also ISPs, are those that provide end recipients mailboxes to receive and send email. Common mailbox providers are Yahoo!, Gmail, AOL, and Hotmail.

MTA: The Message Transfer Agent is a software application that transfers and routes email from sender to recipient.

Open: An email is considered open when a recipient of an email clicks an email message in their inbox to see the body of the message. Unique opens excludes the multiple number of times a single recipient may open a message.

Postback URLs: When activated, any time an email is bounced or spam complaint is received, these URLs are activated to execute any custom script on your servers you would like.

Phishing: Phishing is when an ill-intentioned party tries to gain sensitive information like passwords or credit card information by falsely appearing as a trusted brand. A common phishing ploy is when phishers masquerade themselves as banks to gain account information.

Rented/Bought: Rented or bought refers to lists that have been created by 3rd parties that your company pays for to acquire a large list of email addresses.

Reputation: Sender Reputation is how ISPs view your sending habits. A good reputation consists of low bounce rates and low complaints.

Seed Account: Seed accounts are email addresses where you have access rights to the account itself. They are used to measure whether your message is delivered to the spam folder or the inbox. This provides insight into the deliverability at that mailbox provider.

Sender ID: Sender ID is a way to validate that emails are being sent by verified domains. It does this by checking the email sender's IP address against the domain's recorded owner.

Shared IP Pool: One or more IP addresses set aside for use by multiple companies, senders, or domains for sending email. Generally, senders with smaller sending habits share an IP address pool.

SMTP: Simple Mail Transfer Protocol is used to send and receive email.

Soft Bounce: Soft bounces occur when a mailbox provider indicates that the email address you used is not valid at this time. Most often, this happens because the inbox is currently full or cannot be reached. You may try to email this address again in the future.

Spam: Spam is any message received that is not wanted by the recipient. Spam is often thought of as messages about schemes or health supplements, among many other unwanted messages.

Spam accounts for about 70% of emails sent today.

Spam Trap: Spam traps are email addresses that are placed on websites, not opted into any email list, for the purpose of finding spammers who gather lists of email addresses for marketing. Sending any email to these spam traps can cause your IPs or Domain Names to be blacklisted, heavily impacting your deliverability.

SPF: Sender Policy Framework is an email validation system that allows mailbox providers to validate mail from your domain against the IP addresses sending the mail. If a mail server doesn't appear in a domain's SPF record, but is attempting to send mail from that domain, it is most likely spoofed or unapproved mail and can be rejected by the ISP.

Spoofing: Spoofing is the act of making an email address look like a different sender than the actual sender. Spammers use spoofing to get by spam filters by sending mail through a more reputable "From" address.

Suppression: A suppression list contains email addresses that should not receive email. Commonly, unsubscribed email addresses are placed into a suppression list so that they will not receive future messages.

Text-to-Image Ratio: The ratio of text-to-image space in an email. Having too many images or too large of an image in an email can cause the spam weight of the email message to go up, causing it to go to the spam folder.

Transactional Mail: Transactional mail is any message sent that was triggered by an action from the recipient. Examples are commonly receipts, but can also be account notifications, shipping notifications, password resends, etc.

Unsubscribe: When a recipient of your message requests to be removed from any future communication, this is called unsubscribing. Unsubscribes do not negatively affect your sender reputation.

Warming IP: When senders first start sending mail, they must warm up the IP address they are using so that they can be deemed as a reputable sender. The process happens slowly over time by sending out a low volume of messages and then building up over time.

Whitelist: A list of senders who have been approved by a recipient. Adding a sender to a recipient's whitelist will make it easier for the sender's email to hit the inbox.

X-header: Non-standard header items that can be customized and sent along with email messages to retain specific details that are important to the sender, ESP, ISP, or the recipient. These can be used to tag, categorize, and segment email in Dyn's Email Delivery.

Have questions regarding your email delivery infrastructure? Learn more at: dyn.com/email



Rethink DNS.

Oracle Dyn is global business unit (GBU) focused on critical cloud infrastructure. Dyn is a pioneer in DNS and a leader in cloud-based infrastructure that connects users with digital content and experiences across a global internet. Dyn's solution is powered by a global network that drives 40 billion traffic optimization decisions daily for more than 3,500 enterprise customers, including preeminent digital brands such as Netflix, Twitter, LinkedIn and CNBC. Adding Dyn's best-in-class DNS and email services extend the Oracle cloud computing platform and provides enterprise customers with a one-stop shop for infrastructure as a service (IaaS) and platform as a service (PaaS).

Copyright © 2015, 2017. Oracle and/or its affiliates. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. 1003-1

ORACLE® + Dyn

🏠 dyn.com

☎ 603 668 4998

🐦 @dyn