Email Terminology: 20+ Terms for Marketing and Email Verification

Posted on October 20, 2021

Email as a technology may be old and gray by now, but it hasn't lost its sheen, as it remains a (if not "the") primary business communication medium. Like any Internet-based tech, however, not everyone who uses it knows everything there is to know about it.

They may not know, for instance, how email marketing can help companies thrive exactly or why email verification is important. This glossary aims to shed some light on these topics by diving into essential email marketing and email validation terms and concepts.

Email Terms Everyone Should Know About: The Basics

Before we get into email validation and marketing terminology, we need to cover the basics first, specifically the terms related to how email works.

POP

Post Office Protocol (POP) is a standard Internet protocol that allows email applications to retrieve messages. It works alongside the Internet Message Access Protocol (IMAP).

APOP

Authenticated Post Office Protocol (APOP) is an extension of POP. Apart from letting a computer retrieve emails from a POP server, APOP also provides authentication, including password encryption upon client receipt.

The "A" was added in that unlike POP, where the username and password appear as plaintext, APOP encrypts them, thus preventing hackers from seeing them using sniffer programs. APOP works the same way POP does, but a POP server also holds emails for APOP, and they sit there so recipients can read them later.

SMTP

Simple Mail Transfer Protocol (SMTP) is a protocol that mail servers use to send and relay outgoing messages from email senders to intended receivers. In snail mail's case, SMTP is comparable to the courier that takes the messages from the airport to the sorting station for the actual delivery of assigned postmen to your doorstep.

IMAP

Internet Message Access Protocol (IMAP) is an open Internet standard that describes how to access messages in a mailbox. It's a critical part of receiving emails, as it lets clients like Mail on MacOS, Thunderbird on Mozilla, and Mailspring download messages from your email account (Gmail, Outlook, Yahoo, etc.) for archiving and sorting into folders.

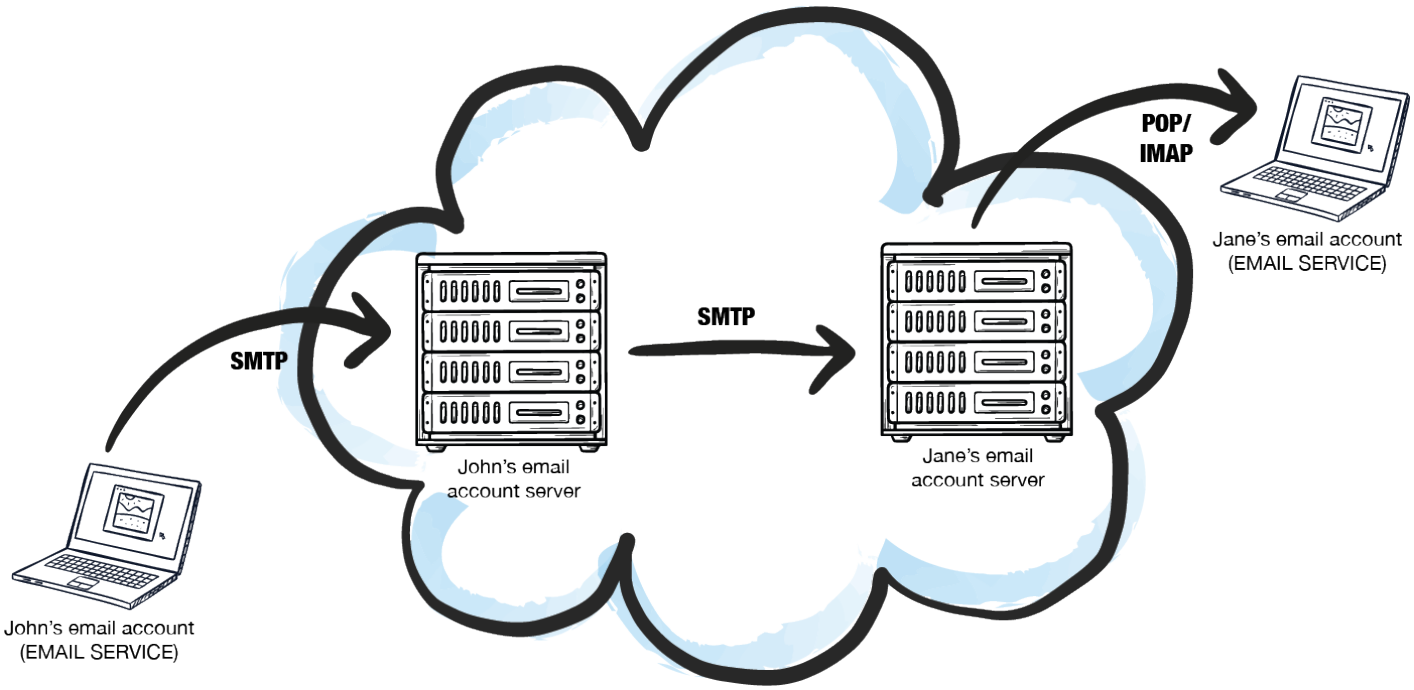
Email Attachment

An email attachment is a digital file sent via an email. One or more files can be attached to a message. It is a simple means to share documents and images with others. Some email attachments can be safe to open but others can harm your computer. They are one of the most common ways, in fact, by which cybercriminals send malware to target victims. That's why cybersecurity specialists always warn us not to download and open attachments.

Email Service

An email service is an application (Gmail, Outlook, etc.) that lets you send and receive messages on the Internet. All you need to do is subscribe to either a free or paid service.

If you're wondering how the components above work together, take a look at the following diagram.



How email works

Now that you know about the most important email terms, it's time to take a closer look at the email verification jargon and why it is essential to learn about it.

What Are Common Email Verification Terms? Why Is Email Verification Important?

Email verification terms are used to describe how emails are sent and received, and everything else that happens from both ends of the process. Here are four reasons why email verification is important.

Keep Your Reputation Intact

Email verification is critical for businesses, as it allows them to conduct their affairs smoothly while maintaining a positive reputation. For many businesses, communicating via email is the only means they can contact customers, clients, and potential business partners.

Avoid Ties to Malicious Activity

If proper verification isn't done, chances are the company could be seen as illegitimate or have ties to fraud. Businesses aren't the only ones who benefit from email verification, though, individuals do, too.

Keep Company Outsiders at Bay

In the case of financial institutions like banks or credit unions, for example, the organizations often receive a lot of emails from various sources. If they're looking to expand their client list, they could obtain contacts from third-party lists. But there is no guarantee that all of the email addresses they contain are genuine or legitimate. The business could get exposed to dangers, such as scams, hacking attempts, and phishing, all of which aim to exploit flaws in their network to steal valuable information.

Such a breach of security can be easily passed on to customers and clients affiliated with the institution. As such, even members of the general public need to verify suspicious emails to protect themselves from attacks.

Because of the aforementioned risks, certain measures should be taken to verify the nature and purpose every email address. And that is what email verification is all about. Its importance has only grown over the years with the prevalence of digital threats.

Maintain a Healthy Domain Reputation

Email verification is also an essential part of digital marketing. Proper verification when sending emails ensures messages are sent to valid addresses only, those that won't lead to hard bounces that adversely affect the success of campaigns. Learn more about email validation and connected email marketing terms in the next section.

Email Validation and Email Marketing Terms

The first step in email validation is understanding the terms and jargon associated with it. Here, we will provide a helpful and comprehensive guide to email verification terms that are often used in relation to marketing.

Abuse Email Addresses

Abuse email addresses belong to people who habitually label unwanted emails as "spam." That causes your emails to bounce. As such, their owners are risky to contact.

API

An application programming interface (API) is a program that bonds two applications together. It extracts information from one application and delivers it to users, acting like an intermediary of sorts.

An API works by calling another application, requests for specific data from it, and finally retrieves the information. An API can be used to verify email addresses in bulk.

Blacklist or Blocklist

A blacklist or blocklist is a well-known and self-explanatory term in the email world. Ending up on a blacklist means getting barred from communicating with users. It works by blocking the domain, IP address, or email address of a blacklisted person, business, or company.

Blacklisting differs from greylisting as you'll see in the next section.

Bounce Rate

The bounce rate refers to the percentage of all the emails you send that aren't delivered or blocked by intended recipients' inboxes. Bouncing commonly occurs when you send out emails en masse using a sloppy or not so well-maintained distribution list. Maintaining an acceptable bounce rate is achievable through regular distribution list cleanups aided by an email verification tool.

Bounce Handling

Bounce handling is simply the process of keeping your bounce rate to an acceptable level. Bounce handling can be automated. A bounce handler, an application that automates bounce handling, sends several bounce messages to the intended recipient to check if the bounce is temporary or permanent. If the bounce is deemed temporary, the email address remains in the distribution list. If deemed permanent, however, the email address is automatically taken out of the list.

Bulk Folder

The bulk folder is where all messages marked as spam go to automatically. Marking emails as "spam" is done by either the inbox's owner or the service provider. Bulk folders are also known as "spam folders" or "junk folders."

The domains of email senders whose messages end up in bulk folders, unfortunately, get tagged as spammers by email service providers (ESPs). That could cause the senders to end up on spam blocklists.

Catch-All Email Addresses

Catch-all email addresses are designed to collect or catch all messages sent to users of the same domain name whose addresses may have been misspelled. In many cases, the inboxes connected to such email addresses also catch messages meant for former employees of the concerned organization.

All in all, catch-all inboxes are typically used by organizations that don't want to miss any emails intended for them.

Deliverable Emails

Deliverable emails refer to messages that can be delivered to their intended recipients.

In email verification, the term "deliverable" translates to email addresses that are valid—properly formatted, has corresponding inboxes and mail exchanger (MX) records, and aren't disposable.

Disposable Email Addresses

These refer to addresses that expire after a set period of time. They are typically used for registering on forums, to download software, post comments on websites, and other short-term purposes. They are also known as "temporary email addresses."

Double Opt-In

A double opt-in occurs when users sign up for an email marketing list then confirm their subscription by clicking a link embedded in an email from the platform. Only after confirming will they be officially added to the list they subscribed to. As such, double opt-in is also known as "confirmed opt-in."

The double opt-in approach reduces the chances that invalid email addresses are included in email marketing databases, helping organizations avoid spam traps and protecting their sender reputation. You're also bound to end up with users who are truly interested in your offers, giving you better marketing results.

Email Delivery Rate

The email delivery rate is an important metric that shows how many of your emails have been delivered. This measurement directly impacts your business's open and click-through rates, which in turn affect marketability.

Email Deliverability

Email deliverability refers to a company's ability to deliver emails to subscribers' inboxes. It lets email marketers gauge how likely it is for their marketing emails to reach their intended targets' inboxes. It improves their throttling and reduces their bounce rates. And the lower their bounce rate is, the less likely they'll end up on spam blocklists and the better their sending reputation gets.

Organizations that suffer from email deliverability issues typically send emails without using custom authentication, employ the single opt-in approach, send marketing messages from free domain email addresses, make it hard for users to unsubscribe, use URL shorteners, and lack subscriber engagement. These companies could do with the help of email verification or validation software.

Email Verification

Email verification, also known as "email validation," is a process that checks if an email address is both active and available for email reception. It is a critical component of cleaning up email lists to ensure that companies only reach out to safe, verified, and validated email addresses.

Email Verification Software

The next step in properly verifying email addresses is using specialized software. Such a solution comes in various forms—an API or a web-based tool. Regardless of format, however, it helps users ensure they only deal with legitimate, verified, and active email addresses.

Greylisting

Greylisting is an anti-spam method that allows email users to prevent unwanted messages from getting into their inboxes by temporarily rejecting emails. A selected sender is typically one the user is unfamiliar with. Some email systems may continue to try and send an email even while greylisted, which may result in bouncing.

Greylisting typically works by rejecting an email and informing its sender that he/she may try again after 1–15 minutes. If you suspect that a recipient has greylisted your address, try to manually resend the email and see if you get a similar message. If you do, then you've been greylisted by that user.

Conversely, you can employ an anti-greylisting technology sold by some companies. These tools are handy for those who are worried their mailing lists contain users who have greylisted them but are not sure who they are and don't have the time to find out.

Hard Bounce

This kind of issue occurs when the email you sent gets rejected permanently. The email address, in this case, could be invalid or nonexistent.

Hard bounces can increase your bounce rate. It is, however, possible to keep messages from bouncing through email verification. The process can help digital marketers keep invalid and nonexistent email addresses out of their campaign distribution lists.

List Cleaning

List cleaning, also known as “email scrubbing,” is a process where users scan their email marketing contact databases for bad or invalid addresses. There are at least two ways to perform list cleaning. One is by doing it yourself aided by a bulk email verification tool. Users can feed their distribution list into such a solution, which then identifies invalid addresses for deletion.

The other way is by hiring a third party that provides list-cleaning services. There are several to choose from.

MX Record

An MX record is an important Domain Name System (DNS) record. It works by redirecting emails to designated mail hosts, which indicate who the messages should be delivered to.

Role-Based Email Addresses

Role-based email addresses belong to people that hold a specific position or are part of a particular group or department within an organization. They use strings such as “sales@,” “team@,” or “contact@.” Many business or corporate email addresses use said formats.

SMTP Bounce Codes

SMTP codes come from different mail servers. They tell senders why the emails they sent bounce. They are thus very helpful in understanding why email marketing campaigns don’t succeed.

Soft Bounce

Soft bounce occurs when the email you sent gets to the recipient’s mail server but not his/her

inbox for various reasons. One could be that the inbox is full. Another could be because the mail server is down.

Spam Filtering

Spam filtering refers to detecting unsolicited, unwanted, and malware-laden emails called “spam” to prevent them from getting into inboxes. ISPs use spam filters to ensure they don’t spread spam. Small and medium-sized businesses (SMBs) also use them for employee and network protection.

Spam filtering is applied to both incoming and outgoing emails.

There are various kinds of spam filters, depending on what the users want to keep out of their systems or network, namely:

- **Content filters:** These scan the content of messages for words that are commonly used in spam emails. Examples include “best offer,” “deal,” and “earn extra income.”
- **Header filters:** These test the email header source to look for suspicious information like known spammer email addresses. These email addresses are usually included in blocklists as indicators of compromise (IoCs).
- **Blocklist filters:** These prevent emails from blacklisted IP addresses from bypassing your network defenses. More advanced filters also check the reputation of each IP address that anyone in your network comes into contact with.
- **Rule-based filters:** These apply the security rules you designed to thwart emails from specific senders or containing specific words in their subject line or body from reaching users’ inboxes. They differ from the three other filters in that they are based on general principles as opposed to specific rules that you came up with in response to your organization’s experience.

Spam traps

These are email addresses that have been abandoned by their owners and subsequently

repurposed into traps for spammers. They are commonly employed by ESPs and blacklisters and exist solely to catch spammers. They aren't owned by real people despite appearing as valid email addresses on email verification tools.

Toxic Email Domains

A toxic domain is one known for abuse, bot-created emails, and spam. It may be marked with a "toxic" flag of some sort by ESPs.

Whitelist

The opposite of a blacklist. Whitelisting email senders shows how much you trust them. Being on a company's whitelist means that your domain, IP, and email addresses follow email marketing best practices and so are consequently trusted.

Email Verification Software

The next step in the process of properly verifying your email address is the use of specialized software. Software like this can provide you with a variety of tools to help ensure that your business only deals with legitimate, verified, and active email addresses.

Before your organization considers using email verification or validation software, you need to brush up on email basics, including the email terminology and email marketing terms, that all aim to improve your sending reputation and cyberdefenses—two indispensable approaches that will protect your employees, systems, and network from all kinds of email-based threats.