A Helpful Guide to the Most Important Email Verification Terms

What Are Email Verification Terms, and Why Are They Important?

Email Verification Terms (EVTs) are used to describe the sending and receiving of emails, as well as everything else that happens in this process.

This verification is very important for businesses to conduct their affairs smoothly and maintain a positive reputation. In many instances, communication by email is the only means of contact with customers, clients, and potential business partners.

If proper verification isn’t done, it can increase the chances of the company being seen as illegitimate or of the company actually being engaged in an act of fraud.

This is also important for the security of both businesses and individuals. Financial institutions like banks or credit unions will often receive a lot of emails from

various different sources whenever they attempt to look for new transaction applicants.

Of course, there is no guarantee that all of them are genuine or honest responses to a potential business opportunity. Businesses are exposed to a great danger in the form of scammers, hackers, and phishers looking to exploit flaws in their security system to steal valuable information about themselves and their customers.

Such a breach of security can be easily passed on to customers and clients affiliated with the company. Personal information can just as easily be impacted as classified business information. It is important for even members of the public to verify suspicious emails to protect themselves from attacks such as this.

Because of these risks, certain measures are taken in order to verify the nature, purpose, and origin of every email address entered. This is what email verification is all about, and its importance has only grown over the years with the prevalence

of the internet.

You should also engage in proper verification practices when sending emails. Emails you send out to potential customers and clients can just as easily be misidentified as suspicious or even malicious.

This most commonly happens when your sent emails bounce, i.e. return to the sender without being received by any recipients. And the most common time this happens is when businesses send emails to unverified email addresses.

Email campaign providers could close business accounts whose emails bounce too frequently. Thus, it is important to verify the email addresses that you try to contact, in addition to verifying any that try to contact yours.

Guide To Email Validation Terms

The first step of the process of email validation is understanding the terms and jargon associated with it. Here, we will provide a helpful and comprehensive guide to email validation terms that you may use to better understand the process. The guide is in the form of a glossary.

Abuse Emails

Abuse emails are email addresses belonging to people who are in the habit of labeling emails as Spam. Such people could label your emails as Spam, which can cause them to bounce. This term ultimately alerts you to recipients that are risky to try to contact.

Application Programming Interface (API)

This is a program that bonds two applications together. It extracts information from one application and delivers it to you, like an intermediary of sorts.

It works by calling another application, requests a specific date from it, and finally retrieves it. APIs are also commonly used to verify email subscribers in bulk.

Blacklist

This is a well-known and self-explanatory term in the email world. To be on a blacklist is to be barred from communication with the blacklister. It works by blocking the domain, IP address, or email address of a blacklisted person, business, or company.

Once someone has blacklisted you, you are barred by both their Internet Service Provider (ISP) and their Email Service Provider (ESP).

Attempting to send any emails from then on will result in them immediately bouncing back. Please be aware that a sloppy email list could result in you ending up on the blacklist, so take care to organize your information before sending it out.

(Side note: a sloppy email list is a list of potentially dormant, invalid, or fake email addresses alongside legitimate ones. It is therefore important to verify and sort out your email lists so that you don't send emails to these kinds of addresses and ultimately get them bounced or get blacklisted.)

Bounce Rate

The Bounce Rate is the percentage of the emails you send out that get bounced or cannot be delivered. This commonly occurs when you knowingly send out emails en masse with a sloppy email list (see above).

As stated above, it is best to clean out your email list of undesirable email addresses in order to maintain a low, if existent, bounce rate.

Catch-All Emails

Catch-All Emails are email address mailboxes that collect, or ‘catch’, all emails sent to their domain. This happens even to email addresses that don’t exist.

These kinds of mailboxes are typically used by businesses and government organizations that don’t want to miss any emails intended for them.

Deliverable

This is an email address that is capable of being delivered. It means that it is in a valid format and has an MX record.

Disposable

Disposables are temporary email 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.

Email Delivery

This is an important metric that shows how many of your emails have been delivered and is displayed in your inbox. This measurement directly impacts your business’s open and click-through rate, which in turn affects your business’s marketability.

Email Validation

This is the process of determining whether an email address exists and is in the correct format. Email validation is important for learning whether a certain mail record exists for a given domain and whether its address syntax is correct.

Email Verification

This is a process that checks whether an email address belongs to a real, active person. It is a more complex process aimed to determine whether a participant is both active and available for email reception.

Both of these two processes are part of one comprehensive system designed to clean out email lists and ensure that your company only reaches safe, verified, and validated email addresses.

Greylisting

Greylisting is an anti-spam method that allows email users to protect against unwanted spam 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 an email bouncing.

Greylisting typically works by rejecting an email from a sender and informing that the sender may try again in 1 to 15 minutes per email. If you suspect that an address has greylisted you, try to manually send an email and see if you get a similar message. If you have, then you have been greylisted by that user.

Conversely, you can employ an anti-greylisting technology distributed by some companies. This is handy if you are worried that your mailing list may contain users who have greylisted you but are not sure who they are and don’t have the time to find out.

Mail eXchanger (MX) Record

This is an important Domain Name System (DNS) record. It works by redirecting email to a designated mail host, which indicates the location to which the email should be delivered.

Role-Based Emails

These are emails that belong to a position or group of people within an organization, designated by specific formats such as sales@, team@, or contact@. Your business email (or emails) is likely to use such a format.

Spam Traps

Spam traps are email addresses that were abandoned and subsequently repurposed into traps for spammers. This is commonly done by ESPs and blacklist providers. Existing solely to catch spammers, Spam Traps aren't owned by real people despite being valid email addresses.

Toxic Domain

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

SMTP Bounce Codes

SMTP stands for Simple Mail Transfer Protocol. These are codes that you receive from different mail servers when a sent email bounces and informs you why.

They are very helpful in understanding why an email got bounced and may be required by an email validation service representative to prevent further bounces.

Whitelist

The opposite of a Blacklist. To whitelist someone is to demonstrate that you trust them and allow emails from them. To be on someone's whitelist means that your domain, IP, and email addresses follow email marketing best practices, and 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.