Key Features Your Email Validator or Verifier API Should Have

Posted on April 7, 2020

Email remains the most preferred platform for business communication. In marketing, the most efficient way to reach a company's target audience regardless of their age is through email. The current email open rate stands at 22.86% compared to social media's engagement reach of 3.71% only.

Therefore, it is not surprising that a lot of today's cybersecurity threats still arrive on networks via emails. In fact, 90% of threats use email as an attack vector. Malware-carrying messages that use effective social engineering ploys still manage to trick unsuspecting users into downloading malicious attachments or clicking embedded harmful links.

And while advanced security solutions protect networks against these dangers, not all companies can afford to buy expensive offerings to defend their assets. But those that want to take steps to stay safe from email-based threats can rely on a product such as Email Verification API. Of course, other security solutions that can detect and block spam are also critical in defending your network. However, you can also integrate a multifunctional and reliable **email validator API** into these as an additional layer of security.

You may be wondering how an **email verifier API**, which marketers typically use, helps with cybersecurity. This post will tell you all about it.

How Can an Email Validator API Be Relevant for Cybersecurity?

Cleaning up your mailing list and improving your bounce rate lessens your chances of landing on a spam blacklist.

It is true; these are typically part of marketing teams' tasks. But if your company lands on a spam blacklist, your security team will also have to help get your domain delisted. And so, avoiding inclusion in any blacklist may be the best approach.

As part of security efforts, encourage marketers to use an **email verifier API** to confirm if the addresses in their mailing lists are active and correct. You can even go the extra mile and integrate Email Verification API into your email software so that it can verify email addresses in real time.

Note that when anyone sends an email to an incorrect address, it comes back, which negatively affects your company's bounce rate. Of course, having a high bounce rate can be indicative of spamming, thus harming your organization's domain reputation, and consequently, your ability to reach existing and potential customers. In fact, if 1% of your emails get tagged as junk mail, your delivery rate also decreases.

As such, a reliable **email validator API** not only helps marketers clean up your company's list of subscribers but also ensures you of high deliverability and low spam rates. In the context of cybersecurity, that translates into domain integrity, which is a must for any company that does business online.

A good cybersecurity posture is all about maintaining your domain's integrity.

Like your bounce rate, maintaining a high domain reputation score is a must for any successful business. Your domain reputation not only affects the success or failure of your email marketing efforts, but it can also make or break your company image.

If Internet service providers (ISP) or email service providers (ESP) get wind of reports that a lot of the emails you send end up in users' spam folders, you are likely to be added to their blacklist. That could prevent your website and pages from appearing in search results and lead to lost opportunities to connect with potential customers and, ultimately, result in revenue loss. It also affects your credibility, brand and reputation that you worked so hard to build. That said, you must exhaust all ways to keep your domain reputation score high.

Maintaining a high domain reputation score also assures you that your intended recipients for email marketing materials will get them. Ultimately, an **email verifier API** saves you time and effort from performing arduous tasks such as manually sifting through email lists and removing

invalid addresses.

A reliable **email validator API** can also help you keep a healthy domain reputation by making sure you refrain from sending messages to spam traps. Spam traps detect organizations that add email addresses to their mailing lists without their users' consent. The tool diminishes your chances of falling for such traps as it would detect addresses that have been deleted by their users and, therefore, no longer exist.

A cyber-secure organization avoids dealings with fraudsters.

Cybercriminals frequently use disposable email addresses for their attacks and fraudulent schemes. That lessens their chances of being identified and nabbed by the authorities.

In light of this, an **email verifier API** helps avoid dealings with nefarious actors. In fact, it can detect external parties using disposable email addresses when reaching out or signing up for your services.

In turn, this can prevent a situation in which an attacker seeking to remain anonymous with a temp address intends to deliver a piece of malware to your network in the guise of an invoice dispute, for example. The attack vector here could be a ransomware variant in the form of a PDF file as an email attachment. Once anyone in your company downloads the file, the malware would run and infect the user's system. If the ransomware replicates and spreads to other connected devices and systems in the network, that could mean a halt in your operations and loss of revenue, not to mention a huge dent on your reputation.

What Does Email Verification API Offer?

Not all **email validator APIs** are created equal. When choosing the right tool, make sure that it will work not just for your marketing efforts but also for your overall cybersecurity posture. It should have features that include:

- **Issuing real-time alerts when users have typos or misspellings in their email addresses:** When integrated into sign-up forms and pages, a good email verifier can check the validity of a user's email address as it gets keyed into form fields. It alerts users to possible typos as they fill in registration forms. For the form owner, that serves as a warning of potential fake addresses.

- **Checking for nonsensical words in email addresses:** Email Verification API is configured to check for nonsensical words or unnecessary terms included in senders' email addresses as an additional layer of security against cyber attacks. Messages coming from email addresses that do not conform can thus be blocked from recipients' inboxes, reducing their chances of becoming cybercrime victims.

- **Checking an email address's format and syntax:** The API checks every email address for the correct format based on the standards laid out by the Internet Engineering Task Force (IETF) as part of using a syntactical email validation engine. If a cybercriminal sender doesn't follow these standards, the API could help invalidate the email account, and the message would not reach the intended recipient's inbox. It can also alert the IT team to look into fake email addresses for further investigation.

- **Disallowing the use of disposable email addresses:** Some users do not necessarily provide their real email addresses when registering on sites. They may just want to get freebies or avoid getting follow-up emails from businesses. Although this seems harmless, it can still dampen your reputation score. Email Verification API can prevent this by disallowing users to contact you or sign up with disposable email addresses, particularly those provided by Mailinator, 10MinuteMail, GuerrillaMail, and other similar services.

- **Authenticating mail servers:** Using email-sending emulation, the API checks if an email address can send and receive messages via a Simple Mail Transfer Protocol (SMTP) connection. That is a surefire way of validating any email address's validity. In cybersecurity, an email address that can't send or receive emails via SMTP usually has to do with a nonexistent or parked domain. Although parked domains are not necessarily malicious, there are cases when cybercriminals park them in preparation for use in an attack.

- **Checking if an email address domain exists:** It verifies if the domain of any email address has a corresponding mail exchanger (MX) record. Most attackers use bogus email accounts for campaigns, and this feature can help cybersecurity researchers tell malicious from non-malicious messages. All emails coming from domains with nonexistent MX records can automatically be blocked or flagged for further investigation.

- **Checking for catch-all accounts:** It is common practice for big companies to have catch-all accounts. That way, they will never miss any message sent to any of their employees. But, it is also common cybercriminal practice to use catch-all email addresses to hide the malicious nature of their messages. Email addresses such as info@companyname[.]com or contact@companyname[.]co often figure in all kinds of cyberattacks. Email Verification API can be integrated into other software to screen all messages that come from catch-all accounts. Cybersecurity specialists can then screen these against a publicly accessible blocklist to check if any of them are malicious. The email addresses of senders of malicious messages can then be added to your blocklist so they cannot pose risks to your network any longer.

As we have demonstrated, **email validator APIs** go beyond boosting your marketing efforts. It can also help your company filter out “bad” email addresses that cybercriminals may be using to infiltrate your network. Email Verification API can be used together with other security solutions to combat fraud and other threats like spamming and phishing effectively.

It also helps cybersecurity teams dig into potentially malicious email addresses to mitigate future attacks proactively. With its help, you can reap better returns on investment (ROIs) from your marketing campaigns while maintaining a good cybersecurity posture.