6 Compelling Reasons Why You Should Check Email Address Owners and Other Email Security Tips

An email address is, perhaps, one of the most overlooked network-accessible resources. Many highly publicized attacks are attributed to a phishing email link that an unsuspecting employee regrettably clicked on. Also, business email compromise (BEC) accounted for 50% of total losses among organizations or $1.2 billion in 2018. Yet despite all the constant warnings and devastating examples, these attacks keep on happening. Why is this so?

The occurrence could be bewildering indeed for cybersecurity professionals who deploy the most advanced endpoint protection and intrusion detection systems (IDSs) there is. Unfortunately, all efforts to ward off attackers can prove irrelevant unless you educate employees on good email hygiene or implement the right email security policies.

This post aims to do precisely the following: provide employees with some guidelines on how to recognize potentially dangerous email addresses. It also illustrates the many ways in which an email verification API can mitigate the problem.

Why Validate Email Senders and Recipients

Employee negligence and insider threats are a leading cause of email-related data leakage among organizations. Misaddressed emails, in particular, is a common reason behind a data leak. This emphasizes the need for companies to deploy tools that **check email address owners**. The following issues can be avoided merely by verifying the source of emails, either manually or with the help of an email verification API:

- **Data loss prevention (DLP):** A data loss occurs when an employee sends an email containing confidential information to a recipient outside a corporate network. It can also happen when an employee clicks on a malicious link that effectively downloads malware onto his/her system. Such an application can communicate with a command-and-control (C&C) server that collects stolen information.Network administrators can prevent the exfiltration of sensitive data by **checking email addresses** and denying access to owners that don't satisfy their DLP rules. An email verification API can be integrated into a DLP solution so it would verify if a sender's email address should be granted access to a user's inbox or not based on a series of verification tests that are elaborated on later in this post.
- **Spam blocking:** While most email filtering tools do a great job preventing unsolicited emails from reaching users' inboxes, a few may occasionally slip through the cracks. Spam takes up email storage space and can carry severe risks for non-tech-savvy users. The majority of them have malicious attachments that users might accidentally open.Integrating an email verification API into an existing email filter gives it the ability to **check if the email addresses' owners** meet the criteria specified for making it to the intended recipients' inboxes.

- **Phishing prevention:** Cleverly crafted phishing emails appear as if they come from real persons and institutions. These messages can specifically target company leaders or employees with access to corporate financial accounts to dupe them into transferring money or transmitting proprietary information to the messages' senders, such as in a spearphishing or BEC attack.You can configure an email verification API to block messages coming from email addresses with nonexistent mailboxes to mitigate phishing attempts. The tool checks if an email address has a Simple Mail Transfer Protocol (SMTP) connection.
- **Malware infection prevention:** Always screen emails from external or third-party networks for harmful content. Make sure these don't come from disposable addresses that many cybercriminals use.You can configure an email verification API to red-flag messages coming from disposable email addresses for further inspection before granting them access to the network to prevent potential malware infections.
- **Helping to avoid hacker reconnaissance:** Cybercriminals always research email users and corporate networks to look for security lapses. At times, with temporary email addresses, they contact employees from target companies to confirm that their email addresses are active (through delivery receipts).An email validation tool can help stave off these attempts by scrutinizing senders' email addresses to make sure they are not disposable. Many cybercriminals use disposable email addresses to stay off the authorities' radar.
- **Email hijacking protection:** This occurs when an email address in a reply thread has been hacked, say, one of your colleague's. Hijacked email responses can efficiently bypass email filtering technologies because they use legitimate addresses. As such, they are often used to deliver a malicious payload, such as the Emotet banking trojan, to people that are part of the existing email thread.Email hijacking won't occur in the first place if you validate every email sent and received by employees with email verification software. Email Verification API can check the incoming mail's mail exchanger (MX) record to see if it matches your company's. If it doesn't then it can be flagged for further inspection or automatic blocking.

How to Recognize Unsafe Email Addresses

Hackers and cybercriminals work very hard to make their emails appear legitimate. Below are some tell-tale signs that an email address has to do with a malicious campaign:

- **Punycode:** Countries with non-Latin alphabets or diacritics commonly use internationalized domain names (IDNs). These contain characters that don't have American Standard Code for Information Interchange (ASCII) equivalents. An example would be "München," which is represented by the Punycode "xn--mnchen-3ya." The domain was converted to Punycode as the German letter "ü" doesn't have an English equivalent.Nefarious actors abuse punycode for phishing campaigns or IDN homograph attacks. Look out for unwanted emails hosted on such domains.
- **Oddly constructed email addresses:** Real email addresses are straightforward and professional-sounding. They don't contain unnecessary words. They don't feature multiple random numbers either. Apart from these, legitimate addresses typically use old generic top-level domains (gTLDs).
- **Sub-, second-, or third-level domains:** Legitimate email addresses rarely use these domain types. As such, be wary of email addresses such as user@accounting[.]thiscompany[.]adifferentdomain[.]co[.]at.
- **Catch-all or disposable email addresses:** Often, generic-sounding email addresses such as info@company[.]com refer to catch-all inboxes. Attackers often use addresses that resemble those of catch-all accounts in hopes of taking recipients aback and making them open a malware-laden email.

As for email content, users can watch out for the following red flags:

- **Does it contain grammatical errors?** The sentence structure is usually a little off in spam or phishing emails.
- **Were you addressed correctly?** Look into how companies address their

email recipients. PayPal, for instance, addresses users by their full name. If you weren't addressed appropriately, then think twice before responding to an email or downloading its attachment.

- **What was the email about?** Refrain from replying or giving in to the demands of email senders outside your network, especially if they ask for login privileges or you to transfer money urgently. Get in touch with the person you suspect is being impersonated directly to confirm such requests.

How Email Verification API Prevents Data Breaches

Email Verification API is a great tool to automate email address validation, filtering, and segmentation. It specifically checks email addresses for the following:

- **Syntax:** The tool looks for typos and format errors in email addresses. It ensures that the format of the address is in congruence with the Internet Engineering Task Force (IETF) standards.
- **MX record:** The tool can determine whether a mail server exists for an email address and where it points to. Retrieving this resource record allows cybersecurity professionals to conduct reverse MX server lookups to identify domains associated with a particular email address and how they figure in attacks.
- **Domain Name System (DNS) record:** The API determines whether a domain associated with an email address actually exists.
- **SMTP connection:** The API looks for an existing inbox for the email address. It can also tell whether a mailbox provider used by an email address temporarily cannot receive messages.
- **Catch-all address:** Email Verification API is capable of identifying whether an email address serves as a catch-all account.
- **Disposable address:** The API determines whether an email address is used as a temporary means of (mis)communication.

To demonstrate how the tool works, let's use it on a sample email address associated with a fake financial claim message. Here's a screenshot of the results in JSON format (the tool also provides users with the option to download results in CSV and XML formats):


```
{
   "emailAddress": "info@claim.com",
   "formatCheck": "true",
   "smtpCheck": "true",
   "dnsCheck": "true",
   "freeCheck": "false",
   "disposableCheck": "false",
   "catchAllCheck": "true",
   "mxRecords": [
      "mx76.mb1p.com.",
      "mx76.m2bp.com."
   ],
   "audit": {
      "auditCreatedDate": "2020-01-15 06:10:52.000 UTC",
      "auditUpdatedDate": "2020-01-15 06:10:52.000 UTC"
   }
}
```


The tool yielded some interesting results. At a glance, it appears that the address used might be from a hijacked corporate domain. It looks like the catch-all domain of a company that uses the domain claim[.]com, which has MX records. These MX records can help users uncover who's behind the spoofed or hijacked email address.

We used Reverse MX API to find associated domains. The tool revealed a long list of new domains bought around the same time in 2019. As for claim[.]com, we analyzed its website and confirmed that its host possesses multiple vulnerabilities and configuration issues.

Other Applications of Email Verification API

Email Verification API also comes in handy for the following marketing purposes, such as:

- **Preventing free trial abuse:** Some users sign up from multiple accounts on sites to take advantage of freemium services. The application can quickly identify email addresses from users that abuse access to content.
- **Verifying user registrations and accounts:** Ensure that users can verify the email addresses they used for newsletter subscriptions and account sign-ups with Email Verification API. The tool prevents users from registering a non-existent email address and prompts them to correct typos and misspellings during registration.
- **Getting better email campaign results:** Reduce bounce rates and boost your sender reputation. Weed out inactive subscribers and fake accounts by using the API.

While there’s no one way to plug all email security loopholes, tools such as Email Verification API can significantly help by **checking email address owners** and more. It is a potent tool for combating cyber attacks caused by lax Internet security habits and compromised credentials.

Get in touch with our team to find out how Email Verification API can protect your business. The first 1,000 API calls are free for new accounts.