**Email validation**

**Email validation** is the process of identifying incorrect email addresses from an email list.

An email validation API should automatically check your mailing list for mistyped email addresses, unauthorized domains or disposable email IDs to ensure deliverability.

**What’s a disposable email address?**

A disposable email address (or a fake ID) is a temporary email ID that expires after a certain time period.

People create and use disposable emails to avoid spammers and phishers when visiting blogs and websites that require them to fill in marketing forms or subscriptions to continue browsing.

Emails sent to these addresses go unnoticed or don’t get delivered at all — affecting your deliverability and sender reputation.

**How Does Email Verification Work?**

Each email address is systematically analysed using a variety of factors to verify it.

Here’s a quick look at these stages:

**1. Syntax Check**

All email addresses follow a particular**syntax** standardized by the IETF (Internet Engineering Task Force) and RFC (Request for Comments).

An email verifier identifies email addresses that don’t correspond with these standards and removes them from the mailing list.

It usually checks:

* The**email prefix** (sequence of letters, numbers, and symbols before the “@” sign).
* **Email domain** (email service provider’s name) that comes after the “@” sign. For example, gmail.com.
* After domain it should contain **.com, .org, .in**.

An example of an incorrect email address syntax is [**xyz#123..@exampel.co**](mailto:xyz#123..@exampel.co)**.**

**2. Address Name Detection**

This step detects and flags email names that are role-based or suspicious, as they affect deliverability due to blacklisting: info@, admin@, adam@eve.com, etc., are examples of such email names.

**3. DEA Detection**

DEA detection identifies and removes **disposable email addresses** (DEA), which are usually temporarily used by people for signups and subscriptions to avoid spam emails.

Disposable Email Address (DEA) detection involves identifying email addresses that are likely to be temporary and not associated with a real user. Here are some ways to achieve DEA detection:

Use third-party APIs: There are several APIs available that can help you identify DEA email addresses. These APIs typically maintain a database of known disposable email providers and can return a flag or score indicating whether an email address is likely to be a DEA.

Check for domains associated with DEA providers: Another way to detect DEA is to check if the email domain is associated with a known DEA provider. There are several public lists of DEA providers that you can use for this purpose.

Use regular expressions: DEA providers often use a specific pattern in the domain name of their email addresses. For example, some DEA providers use subdomains like "temp" or "disposable". You can use regular expressions to identify these patterns and flag email addresses that match.

Analyse usage patterns: Disposable email addresses are often used in specific ways, such as for one-time sign-ups or to receive a single email. You can look for patterns in the usage of email addresses to identify ones that are likely to be disposable.

Use machine learning: Machine learning models can be trained to detect DEA based on patterns in the data. For example, you can use historical data to identify features that are strongly correlated with DEA and train a model to predict whether new email addresses are likely to be DEA.

Overall, DEA detection is a complex task that requires a combination of techniques. Using a combination of the above methods can help increase the accuracy of DEA detection in your application

**4. Spam Trap Detection**

Spam traps are fraud management tools disguised as email addresses. They are created by major ISPs (Internet Service Providers) to identify spammers and block them.

If you send email marketing campaigns to these addresses, they will be marked as spam — which affects your sender reputation.

To prevent this from happening to you, email verifiers help remove spam traps from your email list.

**5. DNSBL and URI DNSBL Check**

An email checker runs your email through a **DNSBL** (DNS-based black list) and **URI** (Uniform Resource Identifier).

DNSBL is a list of IP addresses used for spamming, while URI DNSBL is a list of domain names found only in spam email bodies.

**6. MX Record Lookup**

Checks and verifies the **MX records** of an email address to identify invalid domains.

MX (mail exchange) records are resource records within the DNS (Domain Name System) that clarify which mail servers accept emails from a domain and which don’t.

When the verifier identifies an invalid domain, it removes that particular email address from your email list.

**7. Active Mailbox Check**

An email verifier also sends ping requests to an email address’ server to verify whether it’s active. Once the request is received and responded to, it recognizes the mailbox as authentic and active.