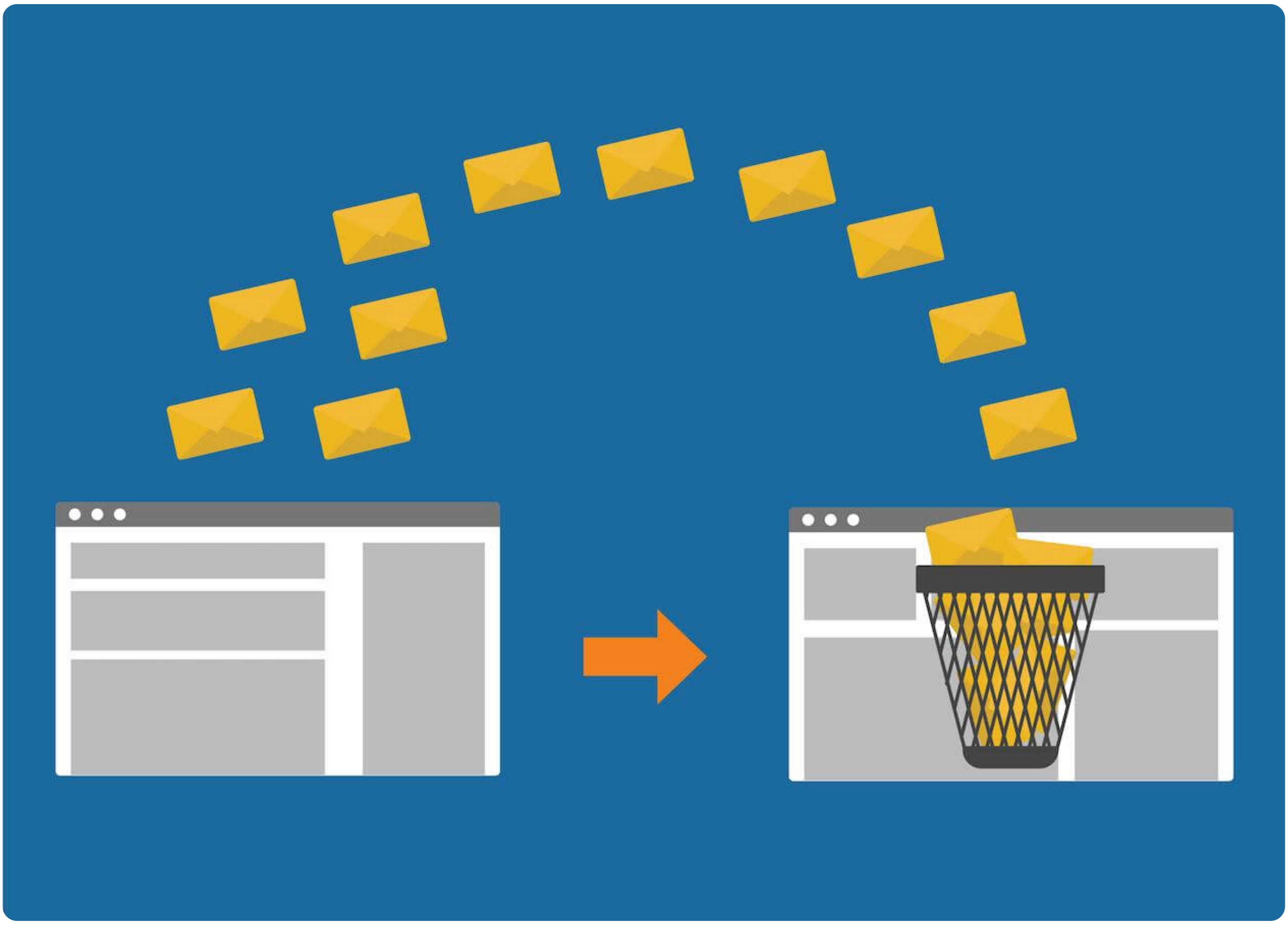
What Is a Disposable Email Address? A Complete Guide to DEAs

Posted on June 30, 2021



Privacy has become a top concern in the digital age, and online users often look for ways to keep their identities protected. One example of such a privacy-related initiative is the use of disposable email addresses (DEAs). This post takes a close look at this type of email address and discusses the following points:

- What is a disposable email address?
- Is using a disposable email address illegal?
- What are the types of disposable email addresses?
- What are disposable email addresses used for?
- What risks do disposable email addresses pose?
- How can you detect disposable email addresses?
- How to manage disposable email addresses

What Is a Disposable Email Address?

Disposable email address (DEA) is an email address that is meant for temporary use and can be discarded easily. After a specific amount of time or number of uses, DEAs are most likely disposed of or deleted. For this reason, DEAs are sometimes referred to as “throwaway email addresses” or “temporary email addresses.”

Types of Disposable Email Addresses

DEAs come in different forms. While they always follow the required syntax where the email prefix and domain are separated by the @ symbol, DEAs could have other purposes. Below are three common types of DEAs, according to how people use them.

- **Forwarding email address:** Some people give out a different email address but set it up so some or all messages are forwarded to their primary email accounts. This type of DEA is called a “forwarding email address.”

- **Alias email address:** This type of DEA is also hosted by the user’s primary email service provider. However, they are only used for secondary purposes and their inboxes are seldom opened by the owners.
- **Throwaway email address:** Throwaway email addresses are created using a temporary email service. They are primarily for one-time use only, are often created randomly using a variety of characters, and disappear after a certain amount of time.

6 Common Uses of Disposable Email Addresses

As previously mentioned, DEAs are among the technological applications or innovations brought about by the need for privacy protection. Thus, DEAs were initially designed to do just that—protect the privacy of their owners. However, some people have also taken advantage of the anonymity and privacy that DEAs provide.

Below are six common ways that people use DEAs. You may notice that they are a combination of positive and somewhat less positive or even malicious applications of the same technology.

- **Protect privacy and anonymity:** Email addresses are considered personally identifiable information (PII). Giving out your official email address can expose you to the risk of a data breach. To avoid such a risk, people resort to using DEAs.
- **Avoid marketing emails:** Most businesses believe that email is still king and that they can get more sales from email marketing. Others take it further, though, and bombard their target customers with too many marketing emails. To avoid this scenario, consumers have learned to give out DEAs instead.
- **Test email workflows:** Software and penetration testers use DEAs to test the email workflows of the projects they are working on. That helps them get a sense of the things they need to improve without bombarding their personal or work email accounts with test messages.

- **Abuse free trials:** Offering freemium features and free trials is a common business model of software-as-a-service (SaaS) companies. The goal is to impress freemium users enough to convert them into paying customers. However, some people abuse this strategy by signing up with multiple DEAs to get away with the limitations of a free account.

- **Send malicious messages:** The anonymity provided by DEAs can help protect people from getting too many marketing emails, but anonymity also gives some freedom to individuals with nefarious intentions. They may misuse throwaway emails to launch illegal and harmful campaigns, such as delivering malware through emails, for example. The malware would then be a vehicle for threat actors to gain access to victims' devices.

- **Deliver spam:** DEAs also provide spammers with the ability to send messages in bulk. And when a disposable email address is blocked due to spamming, they can obtain a new email account almost immediately and continue their campaign.

Is Using Disposable Email Addresses Illegal?

Using DEAs is not illegal, but how you use them would determine legality. Using them for privacy protection is obviously within your legal rights when no harm is intended. But if you employ them to extort money from people or carry out cyber attacks, you are violating the law.

What Are the Dangers That Disposable Email Addresses Pose?

For businesses, the most apparent effect of DEAs has to do with reduced email marketing campaign performance, particularly increased bounce rates. DEA inboxes could easily reach their storage limits or may not be able to receive messages at all. DEAs could also disappear after a specific amount of time, so any message sent to them would bounce.

There are other repercussions besides email marketing metrics. Failing to reach target customers or freemium users means that there's little to no chance of converting them into paying customers. Such a situation could be detrimental to businesses, especially those operating on a freemium business model.

Cyber attackers may also use DEAs since they are easy to get and hard to trace. Phishing or malware attacks, for example, could be carried out by using DEAs. The victims would only need to click a malicious link or download a file for the cyber attack to succeed. And since the victims don't have to reply to the email, the DEAs can be discarded right after the message is delivered.

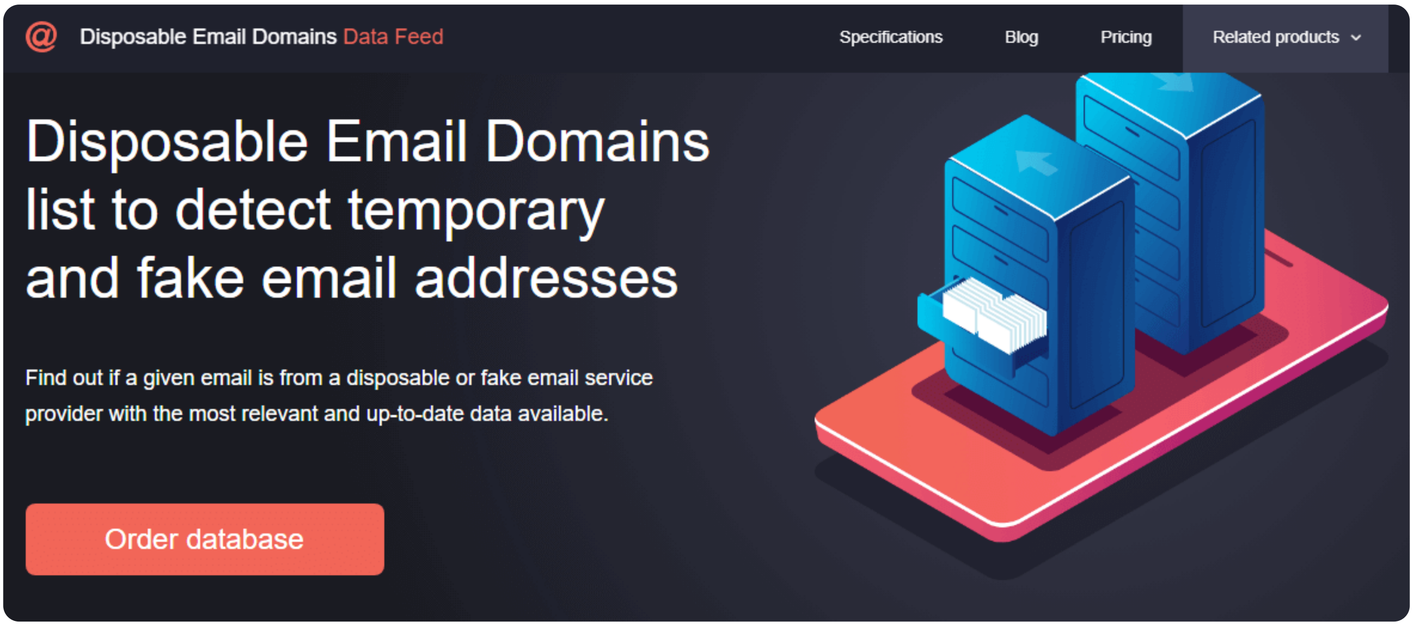
What's more, threat actors can obtain a new DEA for another attack quite easily. Some providers can immediately give you a temporary email address, which may become unusable after a few minutes or so. There's no need to fill in a form to open an email account or click several buttons to delete it.

How to Detect Disposable Email Addresses

Learning what a disposable email address is and how it is commonly used is essential to know if you need to block it from your network. If you find that it poses a danger and should be blocked, the first step would be to detect it.

You can do that with the help of Disposable Email Domains Data Feed, a database containing an extensive list of disposable email domains from more than 2,000 disposable service providers. Follow the steps below to detect disposable email domains.

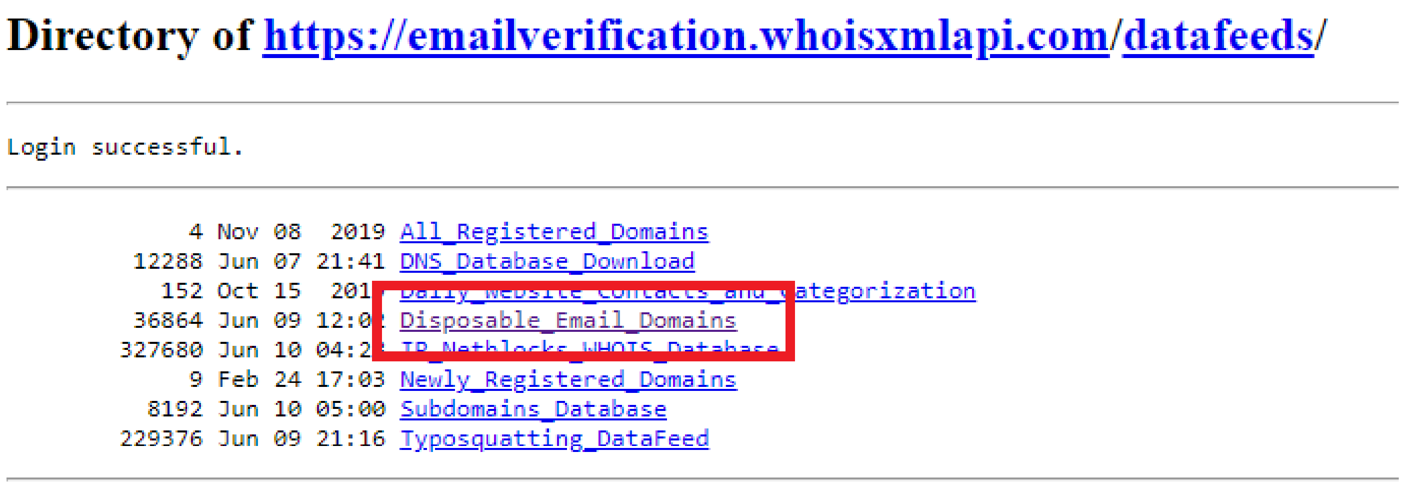
- Get started by leaving a request for the database here. If you already have access, please proceed to the next step.
- Click the "Order database" button.



Disposable Email Domains list to detect temporary and fake email addresses

Find out if a given email is from a disposable or fake email service provider with the most relevant and up-to-date data available.

- You will be taken to a page where all the databases you subscribe to are listed. Click “Disposable Email Domains.”

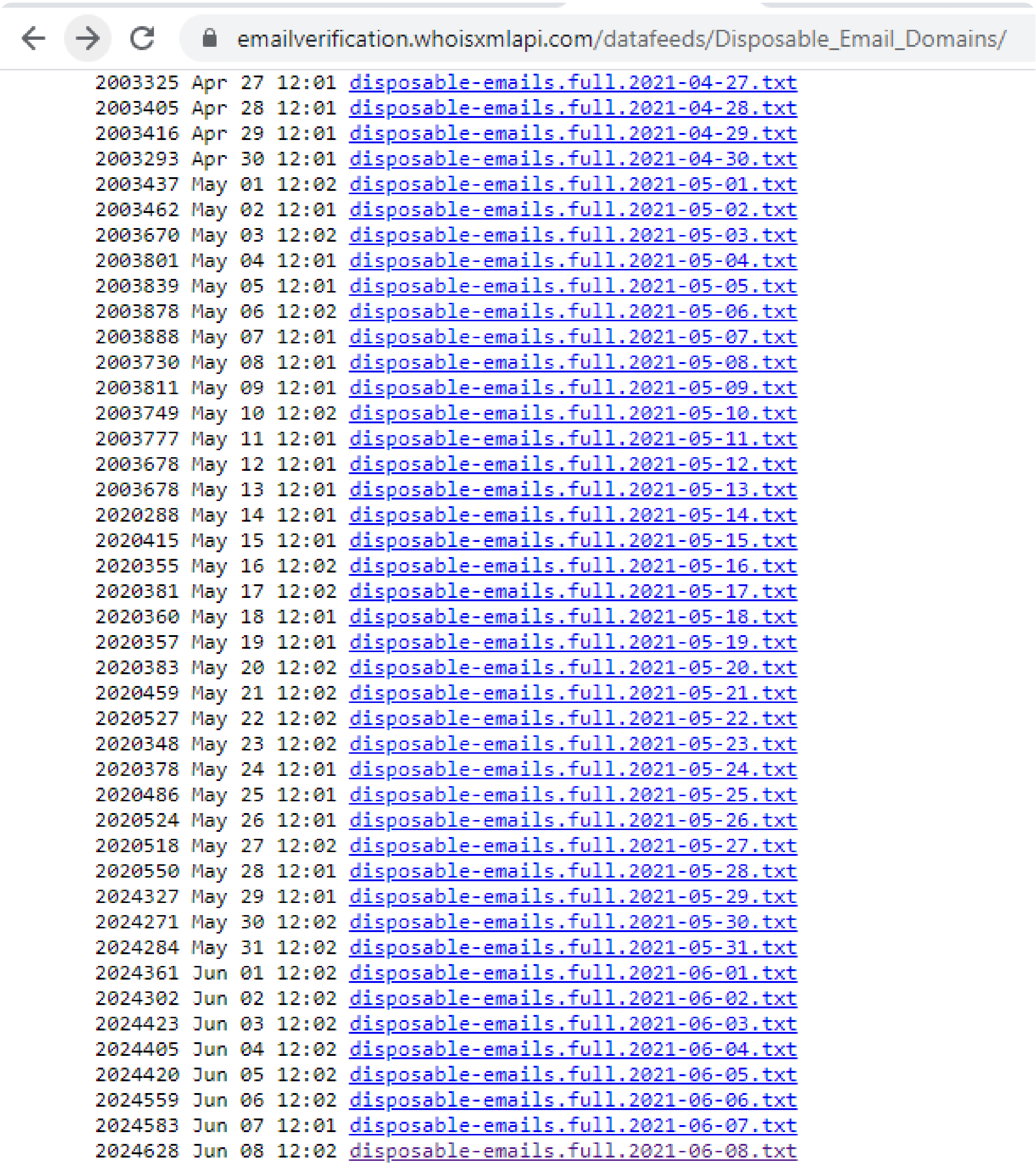


Directory of https://emailverification.whoisxmlapi.com/datafeeds/

```
Login successful.
```

```
        4 Nov 08  2019 All_Registered_Domains
    12288 Jun 07 21:41 DNS_Database_Download
      152 Oct 15  201  Daily_Website_Contacts_and_Categorization
    36864 Jun 09 12:0  Disposable_Email_Domains
   327680 Jun 10 04:2  IP_Netblocks_WHOIS_Database
        9 Feb 24 17:03 Newly_Registered_Domains
     8192 Jun 10 05:00 Subdomains_Database
   229376 Jun 09 21:16 Typosquatting_DataFeed
```

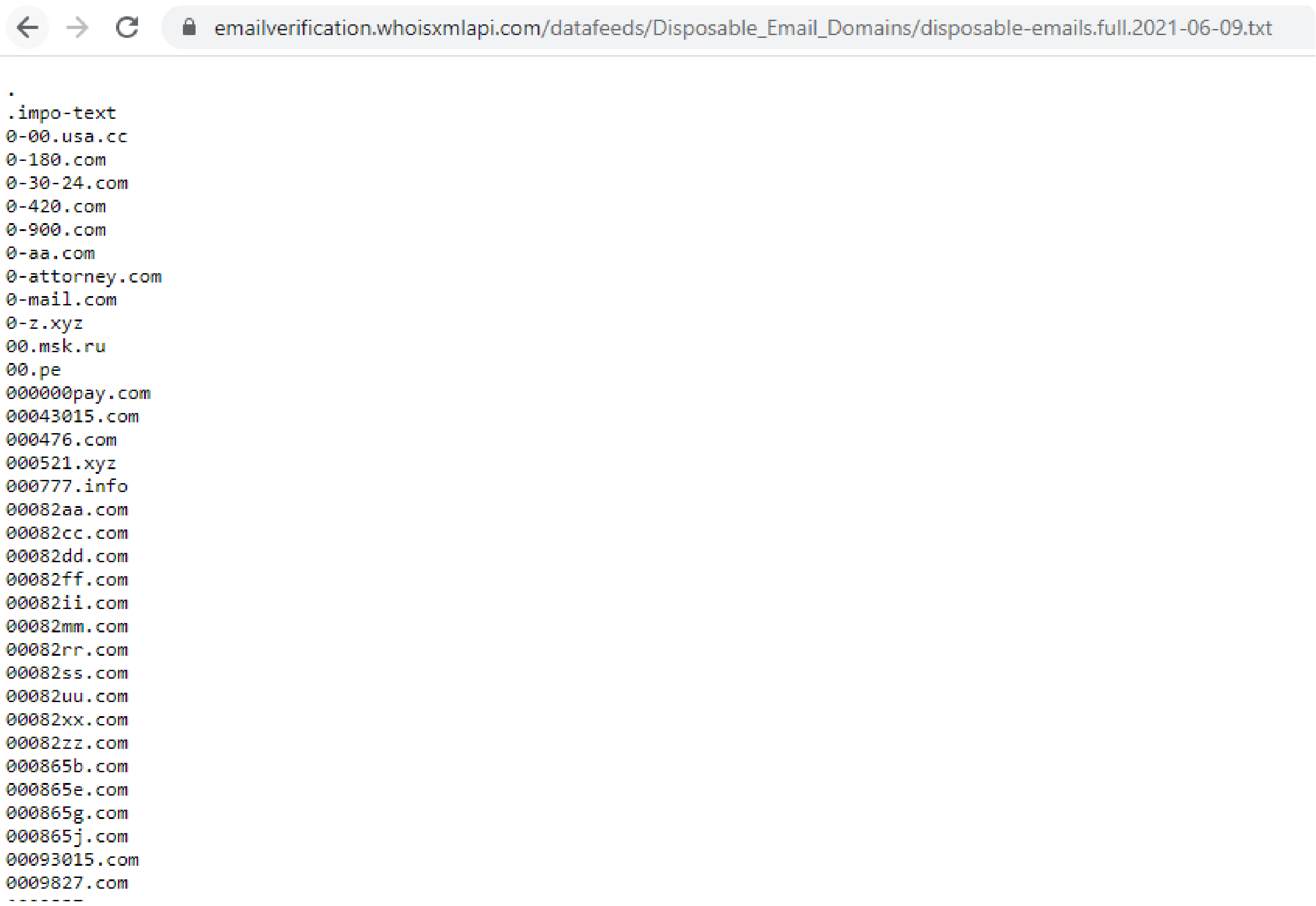
- The next page displays the daily disposable email domain data feeds. Select the date you want to download. If you want the latest data feed, scroll all the way down.



emailverification.whoisxmlapi.com/datafeeds/Disposable_Email_Domains/

```
2003325 Apr 27 12:01 disposable-emails.full.2021-04-27.txt
2003405 Apr 28 12:01 disposable-emails.full.2021-04-28.txt
2003416 Apr 29 12:01 disposable-emails.full.2021-04-29.txt
2003293 Apr 30 12:01 disposable-emails.full.2021-04-30.txt
2003437 May 01 12:02 disposable-emails.full.2021-05-01.txt
2003462 May 02 12:01 disposable-emails.full.2021-05-02.txt
2003670 May 03 12:02 disposable-emails.full.2021-05-03.txt
2003801 May 04 12:01 disposable-emails.full.2021-05-04.txt
2003839 May 05 12:01 disposable-emails.full.2021-05-05.txt
2003878 May 06 12:02 disposable-emails.full.2021-05-06.txt
2003888 May 07 12:01 disposable-emails.full.2021-05-07.txt
2003730 May 08 12:01 disposable-emails.full.2021-05-08.txt
2003811 May 09 12:01 disposable-emails.full.2021-05-09.txt
2003749 May 10 12:02 disposable-emails.full.2021-05-10.txt
2003777 May 11 12:01 disposable-emails.full.2021-05-11.txt
2003678 May 12 12:01 disposable-emails.full.2021-05-12.txt
2003678 May 13 12:01 disposable-emails.full.2021-05-13.txt
2020288 May 14 12:01 disposable-emails.full.2021-05-14.txt
2020415 May 15 12:01 disposable-emails.full.2021-05-15.txt
2020355 May 16 12:02 disposable-emails.full.2021-05-16.txt
2020381 May 17 12:02 disposable-emails.full.2021-05-17.txt
2020360 May 18 12:01 disposable-emails.full.2021-05-18.txt
2020357 May 19 12:01 disposable-emails.full.2021-05-19.txt
2020383 May 20 12:02 disposable-emails.full.2021-05-20.txt
2020459 May 21 12:02 disposable-emails.full.2021-05-21.txt
2020527 May 22 12:02 disposable-emails.full.2021-05-22.txt
2020348 May 23 12:02 disposable-emails.full.2021-05-23.txt
2020378 May 24 12:01 disposable-emails.full.2021-05-24.txt
2020486 May 25 12:01 disposable-emails.full.2021-05-25.txt
2020524 May 26 12:01 disposable-emails.full.2021-05-26.txt
2020518 May 27 12:02 disposable-emails.full.2021-05-27.txt
2020550 May 28 12:01 disposable-emails.full.2021-05-28.txt
2024327 May 29 12:01 disposable-emails.full.2021-05-29.txt
2024271 May 30 12:02 disposable-emails.full.2021-05-30.txt
2024284 May 31 12:02 disposable-emails.full.2021-05-31.txt
2024361 Jun 01 12:02 disposable-emails.full.2021-06-01.txt
2024302 Jun 02 12:02 disposable-emails.full.2021-06-02.txt
2024423 Jun 03 12:02 disposable-emails.full.2021-06-03.txt
2024405 Jun 04 12:02 disposable-emails.full.2021-06-04.txt
2024420 Jun 05 12:02 disposable-emails.full.2021-06-05.txt
2024559 Jun 06 12:02 disposable-emails.full.2021-06-06.txt
2024583 Jun 07 12:01 disposable-emails.full.2021-06-07.txt
2024628 Jun 08 12:02 disposable-emails.full.2021-06-08.txt
```

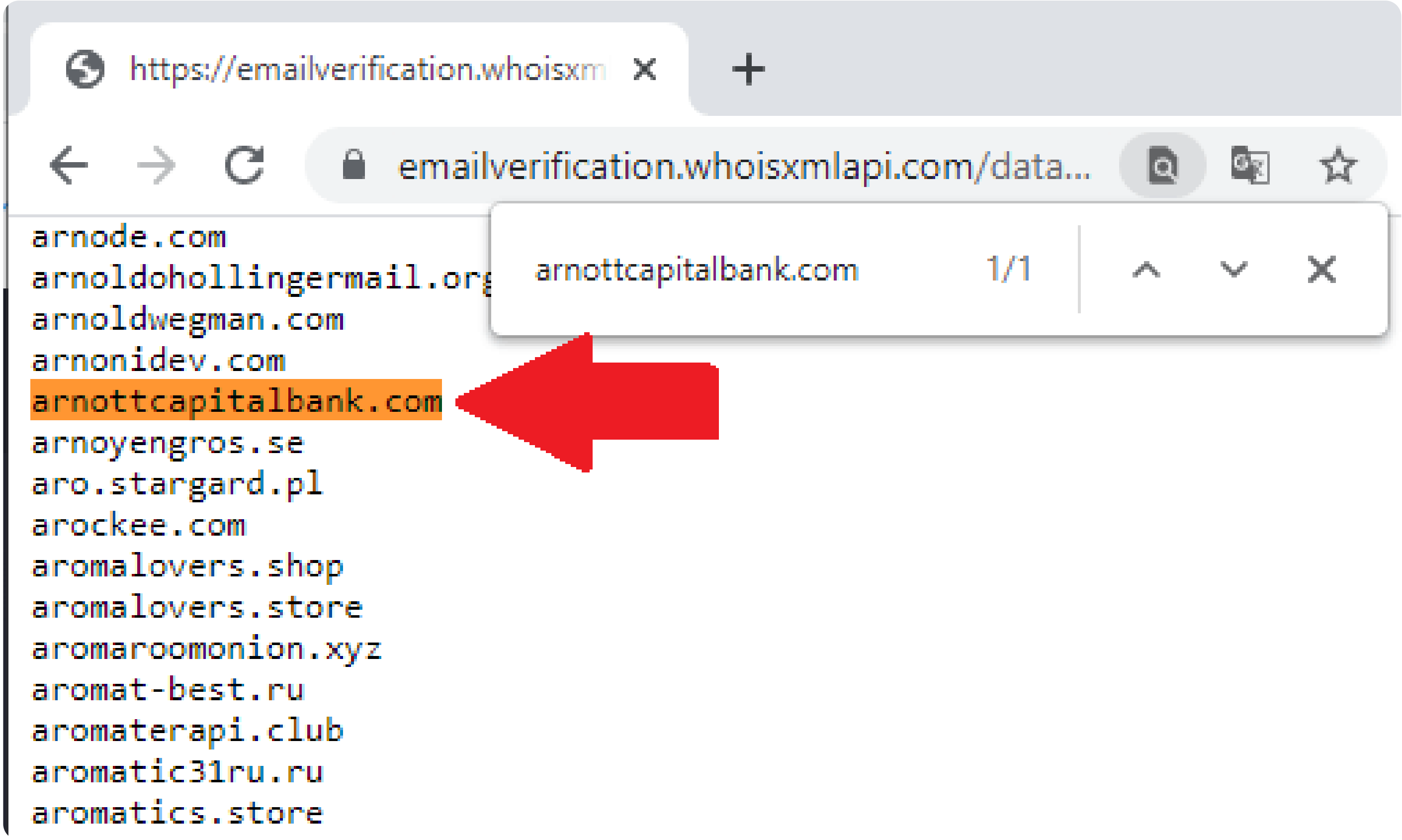
- Click a specific link to open the .txt file.



emailverification.whoisxmlapi.com/datafeeds/Disposable_Email_Domains/disposable-emails.full.2021-06-09.txt

```
.
.impo-text
0-00.usa.cc
0-180.com
0-30-24.com
0-420.com
0-900.com
0-aa.com
0-attorney.com
0-mail.com
0-z.xyz
00.msk.ru
00.pe
000000pay.com
00043015.com
000476.com
000521.xyz
000777.info
00082aa.com
00082cc.com
00082dd.com
00082ff.com
00082ii.com
00082mm.com
00082rr.com
00082ss.com
00082uu.com
00082xx.com
00082zz.com
000865b.com
000865e.com
000865g.com
000865j.com
00093015.com
0009827.com
```

- Search for the email domain you want to verify. If it’s on the file, all email addresses using the domain are disposable.


https://emailverification.whoisxm
emailverification.whoisxmlapi.com/data...
arnottcapitalbank.com
1/1

```
arnode.com
arnoldohollingermail.org
arnoldwegman.com
arnonidev.com
arnottcapitalbank.com
arnoyengros.se
aro.stargard.pl
arockee.com
aromalovers.shop
aromalovers.store
aromaroomonion.xyz
aromat-best.ru
aromaterapi.club
aromatic31ru.ru
aromatics.store
```

- You may copy and paste the data onto a spreadsheet and perform the analysis there. There are more automated ways of using the Disposable Email Domains Data Feed to detect disposable emails, depending on the systems you may have. For instance, you can import the data into marketing or cybersecurity tools.

- You may also use our Disposable Email Checker or our Email Verification API. Aside from automatically detecting DEAs, the API can help you detect invalid and nonexistent email addresses.

How to Manage Disposable Email Addresses

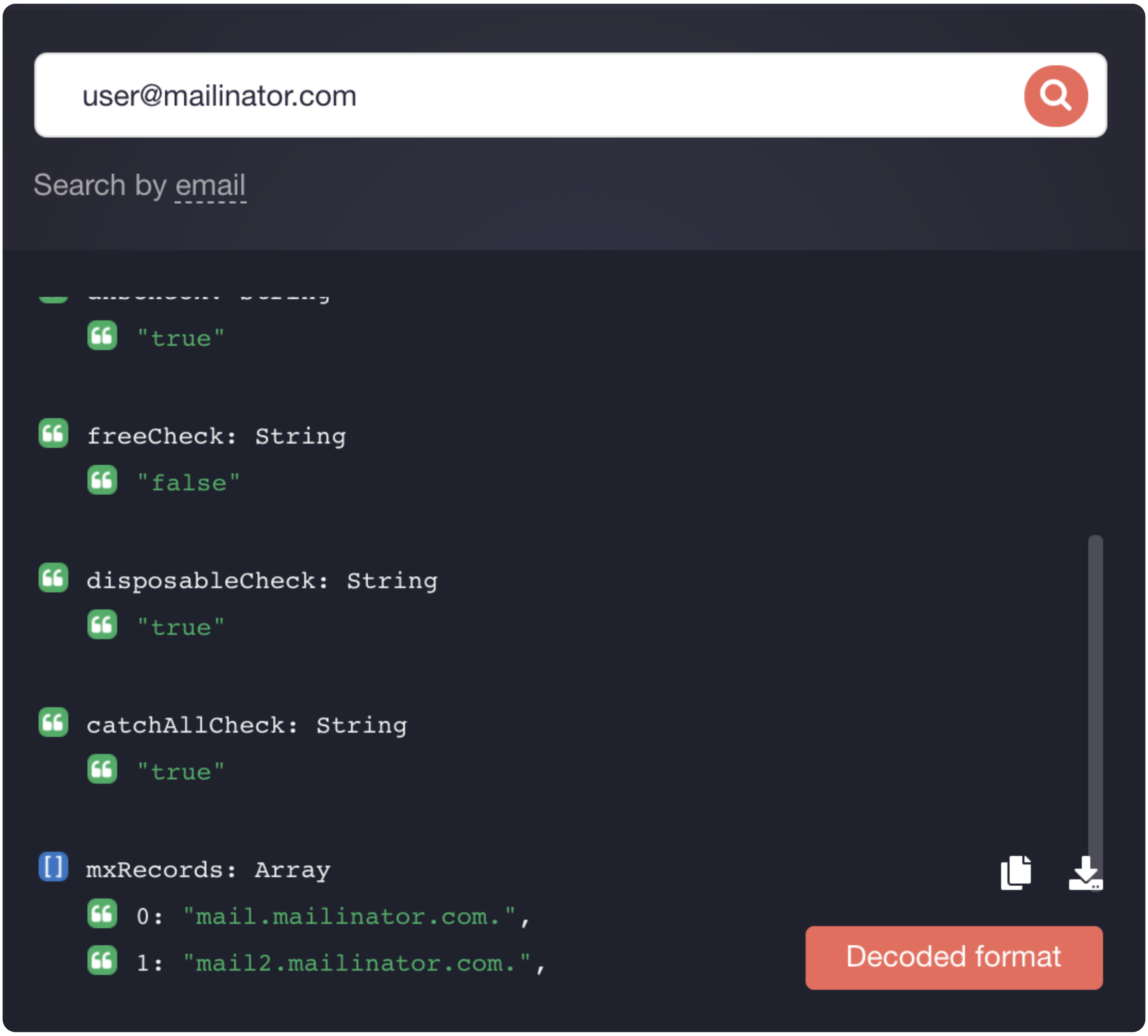
For most businesses, especially those that rely heavily on email marketing, it is crucial to keep

DEAs out of distribution lists. As mentioned earlier, allowing them to be part of such lists could result in higher bounce rates and rating lower deliverability that could potentially result in the company domain's blocking.

The first step in managing DEAs is to identify them in your database. You can use DEA data feeds or email verification tools for that. Once you've pinpointed all of them, you need to delete them from your distribution list. These two steps must be done regularly as part of an organization's email marketing cleanup process. As such, the final step in managing DEAs is monitoring your distribution list to ensure that DEAs are kept out of it as much as possible.

Companies that want to automate DEA management can integrate email verification into their signup pages. The tool they choose to use can be configured to prevent users from registering for subscriptions and free trials, among others, using DEAs.

Email Verification API, when integrated into a signup page, for instance, would instantly detect the email address user@mailinator[.]com as a DEA.



user@mailinator.com

Search by email

```
    "true"

freeCheck: String
    "false"

disposableCheck: String
    "true"

catchAllCheck: String
    "true"

[] mxRecords: Array
    0: "mail.mailinator.com.",
    1: "mail2.mailinator.com.",
```

The signup page, if configured to disallow the use of DEAs, would thus prevent the user from becoming a subscriber and his/her disposable email address will not make it to your distribution list.

Another way is to regularly download (daily, if possible) disposable email domain data feeds and include the data they contain to a blocklist that is specially crafted to prevent DEAs from becoming part of your distribution list.

Including disposable email domain data to your email marketing blocklist would prevent you from sending messages to users who may never turn into customers. That should lower your bounce rate and improve your deliverability rating, ultimately helping to keep your company domain off the spam blacklists that email service providers (ESPs) and Internet service providers (ISPs) maintain.

While not all DEA users are malicious, it’s important to conceive that some of them could be threat actors evading identification. And if you’re running a business, keeping them from getting into your distribution lists is critical, as even if they don’t belong to nefarious users, they can still do more harm than good for your marketing campaigns.