Strengthening Email Security Solutions & Validation Programs with a Disposable Emails Database

Posted on July 28, 2020

Email validation has become a necessity for organizations that aim to protect themselves against cybersecurity threats. The process becomes all the more relevant as 65% of attackers use phishing as a primary infection vector. That's not a surprise, since attackers have long been weaponizing emails to serve as entry points for cyberattacks.

The ease with which threat actors can create disposable email addresses also contributes to the threat. In less than a minute, they can create a temporary email address with tons of providers, which they then use to send malware-laden and phishing messages to target victims. For this reason, a disposable email domain database can make email security vendors and email validation programs in general more robust and comprehensive. Let us elaborate on that.

2 Ways Email Solutions and Email Validation Program Can Benefit from the Integration of a Disposable Email Database

In a sense, temporary or disposable email services may serve as "privacy tools." By using these services, people can avoid receiving spam emails on their real addresses. But fraudsters and other cybercriminals have also begun using temporary email addresses to execute attacks while keeping their identity hidden. Disposable email addresses have thus become akin to virtual private networks (VPNs) and proxy servers, which initially served a good cause.

Since threat actors have found a way to weaponize them, it's usually best to filter disposable email addresses just as organizations block proxy users. By doing so, you weed out users who may have ill intentions or may not be interested in receiving follow-up brand communications. Sure, you may also sift out legitimate people who use disposable email addresses, but the danger of innocent employees falling for phishing emails far outweighs this.

1. Avoid Phishing by Blocking Disposable Email Addresses

In recent years, cybersecurity experts have seen a spike in attacks that use shared file services such as Office 365, OneDrive, and SharePoint. Employees would receive an email notification about their OneDrive account, for instance. Such emails could range from password expiry warnings to shared file notifications or voicemail alerts. Once the user clicks on the link embedded

in the email, the attackers can get hold of his/her login credentials. In some instances, users may download malware in the guise of an innocent-looking file, thereby infecting their network.

Threat actors typically use an email domain that closely resembles that of the shared files service provider. And this is consistent with what we found in our disposable email domain database. For instance, when we searched for the word "drive" (as in OneDrive) on the database, which contained more than 25,000 disposable email domains, we found 52 matching records.
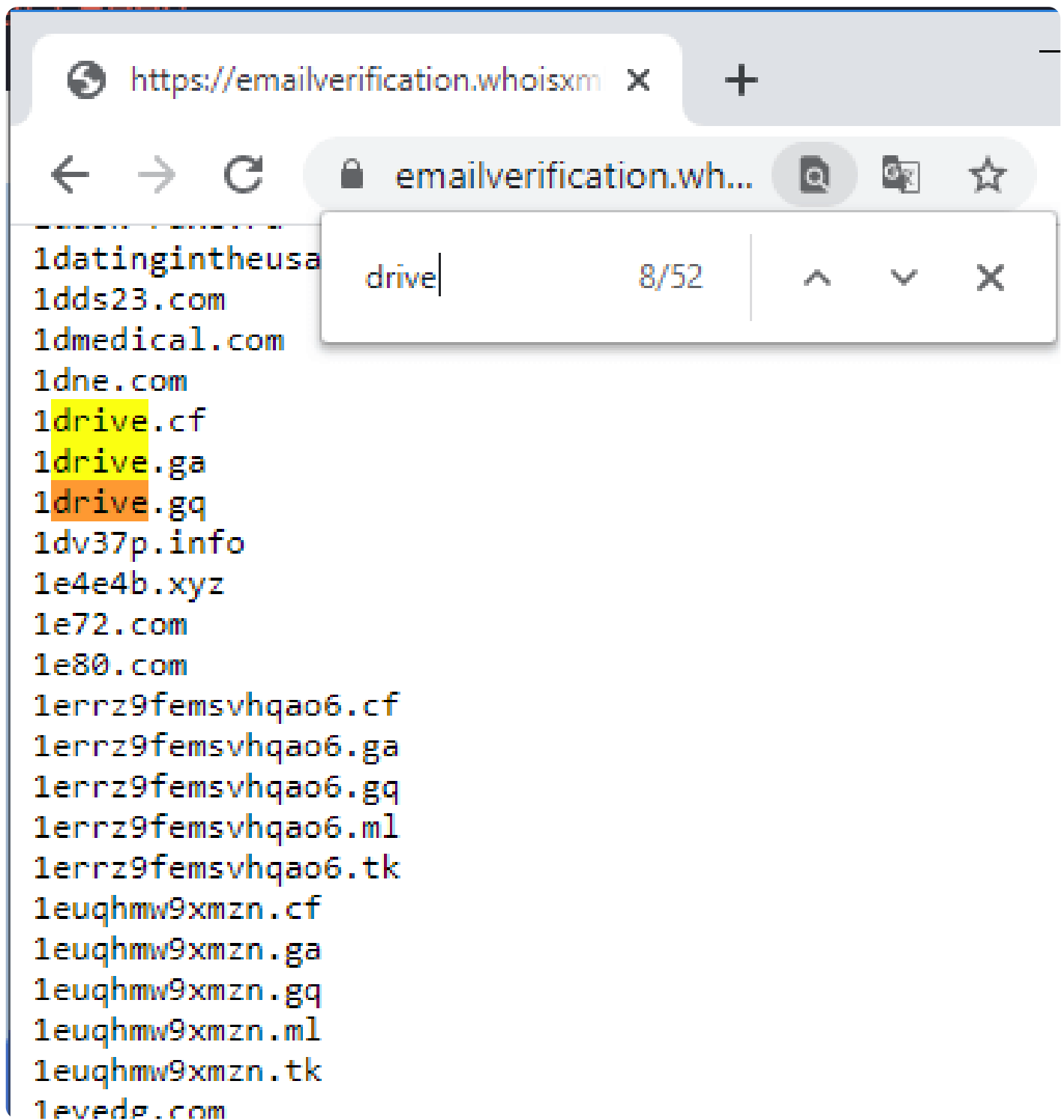
Of the 52 domains, nine could be masquerading as a shared files service domain:

- 0nedrive[.]cf

- 0nedrive[.]ga

- 0nedrive[.]gq

- 0nedrive[.]ml

- 0nedrive[.]tk

- 1drive[.]cf

- 1drive[.]ga

- 1drive[.]gq

- onedrive[.]web[.]id

- g00gledrive[.]ga

- skydrive[.]tk

- xyz-drive[.]info

An email validation program that doesn't filter disposable email addresses may let all emails from these domains reach their intended recipients. That said, clients may end up receiving emails from 1drive[.]ga, a malicious domain, according to VirusTotal.

Of course, not all disposable email domains necessarily belong to bad actors, but not filtering them would also compromise clients and increase phishing risks.

2. Avoid Spam Emails

Google revealed that it now blocks 100 million spam emails daily on Gmail by using artificial intelligence. Put into perspective, however, this may not be much considering that 107 billion spam emails get sent every day.

A disposable email domain database can make email spam filters a lot more effective, as it immediately weeds out temporary email addresses mostly used by spammers.

Consider these spam messages with the subject line "Apple ID Locked." The email domains used are lslp6dpp-08448929[.]id and vqeadkdp-56899194[.]jp, which are already suspicious on their own.
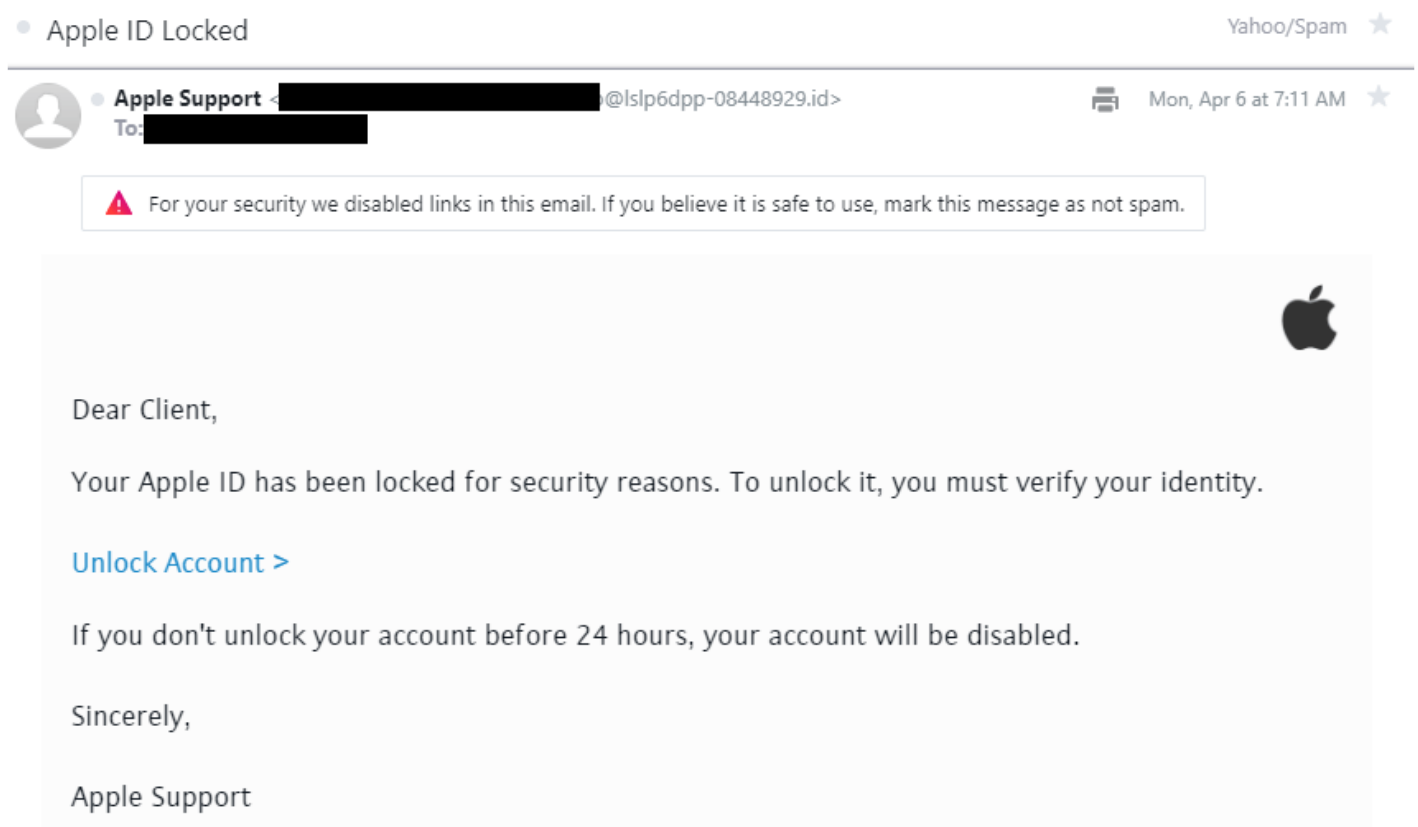
Both email domains are a combination of randomly generated alphanumeric characters, possibly generated by a disposable email service. Our disposable email domain database available for download contains hundreds of similar email domains. Below are some examples of them:

```
345v345t34t.cf      365.moe         3kk43.com                       ptcks1ribhvupd3ixg.cf
345v345t34t.ga      3651se.com      3knloiai.mil.pl                 ptcks1ribhvupd3ixg.ga
345v345t34t.gq      36552b.com      3kqvns1s1ft7kenhdv8.cf          ptcks1ribhvupd3ixg.gq
345v345t34t.ml      36552e.com      3kqvns1s1ft7kenhdv8.ga          ptcks1ribhvupd3ixg.ml
345v345t34t.tk      36552k.com      3kqvns1s1ft7kenhdv8.gq          ptcks1ribhvupd3ixg.tk
346345473.xyz       36552o.com      3kqvns1s1ft7kenhdv8.ml          ptjdthlu.pl
3464445.com         36552u.com      3kqvns1s1ft7kenhdv8.tk          ptll5r.us
3484445.com         36552x.com      3krtqc2fr7e.cf                  ptolbv.info
348es7arsy2.cf      36552z.com      3krtqc2fr7e.ga                  ptpigeaz0uorsrygsz.cf
348es7arsy2.ga      365600.info     3krtqc2fr7e.gq                  ptpigeaz0uorsrygsz.ga
348es7arsy2.gq      365600.net      3krtqc2fr7e.ml                  ptpigeaz0uorsrygsz.gq
348es7arsy2.ml      365600.xyz      3krtqc2fr7e.tk                  ptpigeaz0uorsrygsz.ml
348es7arsy2.tk      365jjs.com      3kurge.us                       ptpigeaz0uorsrygsz.tk

pxtv02fbb830f53fcd46.xyz      qb10em.info                   sj206.com
pxtv052d46b7e333b664.xyz      qb23c60behoymdve6xf.cf        sj20bt.net
pxtv0e80b6e5b469e8dc.xyz      qb23c60behoymdve6xf.ga        sjadhasdhj3423.info
pxtv15c3f2c6e0ce2b37.xyz      qb23c60behoymdve6xf.gq        sjck.icu
pxtv1c4cb8a428306c18.xyz      qb23c60behoymdve6xf.ml        sjl0ec.us
pxtv2a957f7925521397.xyz      qb23c60behoymdve6xf.tk        sjnq9o.us
pxtv2ba2369697313665.xyz      qbaydx2cpv8.cf                sjokbl.shop
pxtv2bcdd23327c95645.xyz      qbaydx2cpv8.ga                sjpvvp.org
pxtv2d9adfcce7badf9a.xyz      qbaydx2cpv8.gq                sjqmiihs.shop
pxtv2da8c6b4f6c5f609.xyz      qbaydx2cpv8.ml                sjrajufhwlb.cf
pxtv47938c1abc5b0fb2.xyz      qbaydx2cpv8.tk                sjrajufhwlb.ga
pxtv4975b124e768c0c5.xyz      qbesar.net                    sjrajufhwlb.gq
pxtv56c76c80b948b92a.xyz      qbex.pl                       sjrajufhwlb.ml
                                                            sjrajufhwlb.tk
```

Integrating a disposable email domain database into an email validation tool would, therefore, help weed out similar spam emails.

How to Access the Disposable Email Domain Database

You can request access to the disposable email domain database here. If you don't have an account yet, don't hesitate to contact us. Once logged in, you will see a complete list of databases,

arranged by date.

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

(/Disposable_Email_Domains)

```
Login successful.
```

```
-rw-r--r--   1 ftp_admin 1005        636903 Nov 21 20:57 disposable-emails.full.2019-11-21.txt
-rw-r--r--   1 ftp_admin 1005        637509 Nov 22 12:00 disposable-emails.full.2019-11-22.txt
-rw-r--r--   1 ftp_admin 1005        637509 Nov 23 12:00 disposable-emails.full.2019-11-23.txt
-rw-r--r--   1 ftp_admin 1005        637509 Nov 24 12:00 disposable-emails.full.2019-11-24.txt
-rw-r--r--   1 ftp_admin 1005        637509 Nov 25 12:00 disposable-emails.full.2019-11-25.txt
-rw-r--r--   1 ftp_admin 1005        637509 Nov 26 12:00 disposable-emails.full.2019-11-26.txt
-rw-r--r--   1 ftp_admin 1005        637509 Nov 27 12:00 disposable-emails.full.2019-11-27.txt
-rw-r--r--   1 ftp_admin 1005        645258 Nov 28 12:00 disposable-emails.full.2019-11-28.txt
-rw-r--r--   1 ftp_admin 1005        648102 Nov 29 12:00 disposable-emails.full.2019-11-29.txt
-rw-r--r--   1 ftp_admin 1005        648400 Nov 30 12:00 disposable-emails.full.2019-11-30.txt
-rw-r--r--   1 ftp_admin 1005        648400 Dec 01 12:00 disposable-emails.full.2019-12-01.txt
-rw-r--r--   1 ftp_admin 1005        648400 Dec 02 12:00 disposable-emails.full.2019-12-02.txt
-rw-r--r--   1 ftp_admin 1005        648400 Dec 03 12:00 disposable-emails.full.2019-12-03.txt
-rw-r--r--   1 ftp_admin 1005        649802 Dec 04 12:00 disposable-emails.full.2019-12-04.txt
-rw-r--r--   1 ftp_admin 1005        650188 Dec 05 12:00 disposable-emails.full.2019-12-05.txt
-rw-r--r--   1 ftp_admin 1005        650166 Dec 06 12:00 disposable-emails.full.2019-12-06.txt
-rw-r--r--   1 ftp_admin 1005        653616 Dec 07 12:00 disposable-emails.full.2019-12-07.txt
-rw-r--r--   1 ftp_admin 1005        654094 Dec 08 12:00 disposable-emails.full.2019-12-08.txt
-rw-r--r--   1 ftp_admin 1005        654021 Dec 09 12:00 disposable-emails.full.2019-12-09.txt
-rw-r--r--   1 ftp_admin 1005        659403 Dec 10 12:00 disposable-emails.full.2019-12-10.txt
-rw-r--r--   1 ftp_admin 1005        659402 Dec 11 12:00 disposable-emails.full.2019-12-11.txt
-rw-r--r--   1 ftp_admin 1005        659406 Dec 12 12:00 disposable-emails.full.2019-12-12.txt
-rw-r--r--   1 ftp_admin 1005        659981 Dec 13 12:00 disposable-emails.full.2019-12-13.txt
-rw-r--r--   1 ftp_admin 1005        663518 Dec 14 12:00 disposable-emails.full.2019-12-14.txt
-rw-r--r--   1 ftp_admin 1005        663146 Dec 15 12:00 disposable-emails.full.2019-12-15.txt
-rw-r--r--   1 ftp_admin 1005        663292 Dec 16 12:00 disposable-emails.full.2019-12-16.txt
-rw-r--r--   1 ftp_admin 1005        663439 Dec 17 12:00 disposable-emails.full.2019-12-17.txt
-rw-r--r--   1 ftp_admin 1005        663529 Dec 18 12:00 disposable-emails.full.2019-12-18.txt
-rw-r--r--   1 ftp_admin 1005        663290 Dec 19 12:00 disposable-emails.full.2019-12-19.txt
-rw-r--r--   1 ftp_admin 1005        671794 Dec 20 12:00 disposable-emails.full.2019-12-20.txt
-rw-r--r--   1 ftp_admin 1005        672627 Dec 21 12:00 disposable-emails.full.2019-12-21.txt
-rw-r--r--   1 ftp_admin 1005        672851 Dec 22 12:00 disposable-emails.full.2019-12-22.txt
-rw-r--r--   1 ftp_admin 1005        672593 Dec 23 12:00 disposable-emails.full.2019-12-23.txt
-rw-r--r--   1 ftp_admin 1005        672691 Dec 24 12:00 disposable-emails.full.2019-12-24.txt
-rw-r--r--   1 ftp_admin 1005        673229 Dec 25 12:00 disposable-emails.full.2019-12-25.txt
-rw-r--r--   1 ftp_admin 1005        681714 Dec 26 12:00 disposable-emails.full.2019-12-26.txt
-rw-r--r--   1 ftp_admin 1005        681711 Dec 27 12:00 disposable-emails.full.2019-12-27.txt
-rw-r--r--   1 ftp_admin 1005        681711 Dec 28 12:00 disposable-emails.full.2019-12-28.txt
```

You can find the most recent database that contains all disposable email domains at the bottom of the index.

Disposable email addresses may have some legitimate uses, but since they can be used as attack vectors, security protocol usually ensures that these are blocked outright or are at least investigated before being granted access to an organization's network. Therefore, an email validation application or program that aims to protect users from phishing and spam should also integrate a disposable email domain database.

Would you like to learn more about using a disposable email database and our other email validation products? Contact us for more information.