■ Reputation Check: https://www.google.com/url?q=http://89q.sk/6q1a2722&source=gmail&ust=17415375666960000

==

DOMAIN INTELLIGENCE REPORT

Timestamp : 2025-06-20 08:28:22

Analyzed Domain : https://www.google.com/url?q=http://89q.sk/6q1a2722&source=gmail&ust=1741537566696000&usg=AOvVaw09P1Uw6RhgypCt0EE7sQg9

Languages : English |

==

Summary Insight

The domain https://www.google.com/url?q=http://89q.sk/6q1a2722 lacks reputation and threat analysis data. Use IPQS for domain risk score and threat analysis. IPQS provides comprehensive cybersecurity checks.

Reviewed Intelligence Sources

----

1. https://support.google.com/mail/thread/10570288/how-to-improve-my-domain-reputation?hl=en
   Missing: threat analysis q= http:// 89q. sk/ 6q1a2722&source= gmail&ust= 1741537566696000&usg= AOvVaw09P1Uw6RhgypCt0EE7sQg9.

2. https://support.google.com/mail/thread/5648161/what-is-domain-reputation-and-ip-reputation-difference-how-one-of-the-reputation-impact-others?hl=en
   Missing: threat analysis q= 89q. sk/ 6q1a2722&source= gmail&ust= 1741537566696000&usg= AOvVaw09P1Uw6RhgypCt0EE7sQg9.

3. https://www.spamhaus.org/resource-hub/domain-reputation/a-beginners-guide-to-domain-reputation-what-is-it/
   Missing: analysis google. q= http:// 89q. 6q1a2722&source= gmail&ust= 1741537566696000&usg= AOvVaw09P1Uw6RhgypCt0EE7sQg9.

4. https://bolster.ai/blog/understanding-domain-reputation-attacks
   Missing: google. q= http:// 89q. 6q1a2722&source= gmail&ust= 1741537566696000&usg= AOvVaw09P1Uw6RhgypCt0EE7sQg9.

5. https://www.ipqualityscore.com/domain-reputation
   Please enter the mail server domain you wish to verify in the search box above to check the **domain risk score** and threat analysis. This free domain lookup tool will perform quick domain analysis to determine if any fraud, abuse, malware, phishing, and other types of unwanted actions have originated from this domain. IPQS analyzes domain threat data from across our network, based on scoring hundreds of millions of transactions per day and extensive live reporting feedback from our clients. [...] * [Cybersecurity](https://www.ipqualityscore.com/domain-reputation#) * [Malicious URL Scanner](https://www.ipqualityscore.com/threat-feeds/malicious-url-scanner) * [File Malware Scanner](https://www.ipqualityscore.com/file-malware-scanner) * [Data Breach Search](https://www.ipqualityscore.com/data-breach-search-engine) * [Leaked Emails](https://www.ipqualityscore.com/data-breach-lookup/leaked-email-checker) [...] * [Leaked Passwords](https://www.ipqualityscore.com/data-breach-lookup/password-leak-check) * [Leaked Usernames](https://www.ipqualityscore.com/data-breach-lookup/compromised-usernames) * [Domain Age Checker](https://www.ipqualityscore.com/domain-age-checker) * [Cyberthreat Intelligence](https://www.ipqualityscore.com/cyberthreat-intelligence-map) * [Threat Intelligence Feeds](https://www.ipqualityscore.com/threat-intelligence-feed-api)

End of Domain Report

==

■ Reputation Check: https://google.com/amp/trackmyorder-fedex.com

==

DOMAIN INTELLIGENCE REPORT
Timestamp : 2025-06-20 08:29:19
Analyzed Domain : https://google.com/amp/trackmyorder-fedex.com
Languages : English |

==

Summary Insight

The domain https://google.com/amp/trackmyorder-fedex.com is likely a phishing scam. FedEx advises against using unofficial tracking sites. Always use the official FedEx website for tracking.

Reviewed Intelligence Sources

----

1. https://www.reddit.com/r/Scams/comments/18bqhbh/fedex_scam_or_is_this_real/
   Missing: analysis domain

2. https://news.ycombinator.com/item?id=39479001
   FedEx may have the worst and least secure digital platform for a major company. Some examples I've noticed.

3. https://www.fedex.com/en-us/report-fraud.html
   Center](https://urldefense.com/v3/__https:/www.ic3.gov/__;!!BL9GA0TyTA!YNe7wD1QF7mQYNmKwloEAZ5glCESo_GDbOUs3R-r3Xw2FFnr5ry7ixijD967J8233EoD-vjScRwcI80XHJlvu62T9Q$), and/or your local law enforcement. [...] These scams involve directing you to malicious sites through a search engine. The site may offer low-cost products or services like credit cards or loans. If you enter your credit card information, it's collected by the phishing site. Smishing Similar to email and IM attacks, links are delivered to your mobile device via text messaging. Malware is launched when you click on a hyperlink that takes you to a malicious website. Social engineering [...] We use VeriSign Extended Validation (EV) certificates. Browsers that support EV certificates show that a site has undergone additional validation. Browsers without EV support will function on fedex.com, but you won't see the validation indicator. * * * * * * ![Image 63](https://cdn.bfldr.com/I22OPSFM/at/pw574k84ngszvtvvsm2ntt8x/Purple_Checkmark_Icon_-_Small.svg?auto=webp&fit=bounds&format=jpg&width=128&height=128&)

4. https://www.fedex.com/en-us/tracking.html
   We use cookies and similar analytical technologies on our site. Functional cookies and certain privacy-friendly analytical cookies are always enabled to create an outstanding website experience. **By clicking "Accept All Cookies" or by continuing to use this site, you consent to other analytical cookies and tracking cookies which allow FedEx to provide a more personalized experience.** See our [cookie notice](https://www.fedex.com/content/dam/fedex-com/legal/FedEx_Cookie_Notice.pdf) to learn [...] [Ad Choices](https://www.fedex.com/en-us/trust-center/privacy.html#section7 "Ad Choices")   * * * * * *   Your Browser is Not Currently Supported We have updated our list of supported web browsers. Note that Internet Explorer is no longer supported. We recommend using one of the following browsers to access this site. * * * MICROSOFT WINDOWS BROWSERS *   Edge 41+ *   Google Chrome 41+ *   Mozilla Firefox 38+ APPLE

```
    BROWSERS  *   Google Chrome 41+ *   Mozilla Firefox 38+ *   Safari 7++ [...]
    [](https://www.linkedin.com/company/fedex)
    [](https://www.youtube.com/user/fedex/custom?sub_confirmation=1)
    [](https://www.pinterest.com/FedEx/)  * * *  * * *   FedEx 1995-2025  * * *  * * *  [Site
    Map](https://www.fedex.com/en-us/sitemap.html "Site Map") |   [Terms of
    Use](https://www.fedex.com/en-us/terms-of-use.html "Terms of Use") |   [Privacy &
    Security](https://www.fedex.com/en-us/trust-center.html "Privacy & Security") |

 End of Domain Report
====================================================================================================================
```

■ Reputation Check: https://usps.com-ylfrtgt.top/us

```
====================================================================================================================
DOMAIN INTELLIGENCE REPORT
 Timestamp        : 2025-06-20 08:29:44
 Analyzed Domain   : https://usps.com-ylfrtgt.top/us
 Languages        : English |
====================================================================================================================

 Summary Insight
----------------------------------------------------------------------------------------------------
The domain https://usps.com-ylfrtgt.top/us is likely a phishing site. It mimics USPS and attracts
significant traffic, indicating a high threat level. It's associated with known malicious
activities.

 Reviewed Intelligence Sources
----------------------------------------------------------------------------------------------------
1.  https://www.reddit.com/r/Scams/comments/1h7fy1x/pretty_sure_this_is_a_scam/
    Missing: analysis ylfrtgt.

2.  https://www.resecurity.com/blog/article/smishing-triad-targeted-usps-and-us-citizens-for-data-
theft
    Missing: reputation ylfrtgt.

3.  https://www.akamai.com/blog/security-research/phishing-usps-malicious-domains-traffic-equal-to-
legitimate-traffic
    Missing: reputation ylfrtgt.

4.  https://www.infosecurity-magazine.com/news/study-reveals-usps-phishing-levels/
    Through filtering criteria, domains containing the string "USPS" were isolated, resulting
    in a dataset reflecting malicious intent. Notably, the study took great care to avoid
    false positives, ensuring accuracy in the analysis. [...] Furthermore, analysis of top-
    level domains (TLDs) revealed common choices among threat actors, with ".com" and ".top"
    domains dominating the landscape. Interestingly, while the ".com" TLD provided global
    legitimacy, ".top" emerged as a popular alternative known for its association with
    malicious activities among security researchers. [...] A recent analysis has shed light on
    the extent of phishing and smishing attacks targeting the United States Postal Service
    (USPS), particularly during the holiday season.  The study, conducted by Akamai Security
    researchers using anonymized global DNS query logs, revealed a startling trend.
    Illegitimate domains mimicking USPS websites attracted nearly equal, and sometimes higher,
    traffic compared to legitimate domains, especially during peak shopping periods like
    Thanksgiving and Christmas.
```

5. https://www.domaintools.com/resources/blog/merry-phishmas-beware-us-postal-service-phishing-during-the-holidays/
With the holiday season approaching, DomainTools urges the public to exercise increased caution and remain vigilant against the threat of US Postal Service-themed (USPS) package redelivery phishing attacks. DomainTools is monitoring several USPS phishing campaigns, including activity that aligns with known tactics, techniques, and procedures of the China-based "[Chenlun](https://krebsonsecurity.com/2023/10/phishers-spoof-usps-12-other-natl-postal-services/)" phishing actor and their affiliates [...] "Chenlun" also has a history of targeting postal services in other countries. Notably, *Correos de Chile* is a frequent target. The file structure, configuration files, and objective these phishing kits bear an uncanny similarity with those impersonating the USPS. Moreover, historical analysis of this threat actor's targeting suggests Spanish-language postal services were targets *before* the USPS. The same applies for countless other countries. ![A computer screen with white text [...] In short, phishing actors targeting decisions are based on potential financial upside and risk tolerance. Considering these factors, USPS phishing activity will likely continue to increase until threat actor ability to send phishing lures is significantly degraded or the business decision calculus behind such phishing campaigns presents insufficient upside. This likelihood is supported further by past phishing activity by "Chenlun" and others that first sought to impersonate the postal services

End of Domain Report

==

■ Reputation Check: https://purolator.etcnrr.vip/ca

==

DOMAIN INTELLIGENCE REPORT
Timestamp : 2025-06-20 08:30:08
Analyzed Domain : https://purolator.etcnrr.vip/ca
Languages : English |

==

Summary Insight

The domain https://purolator.etcnrr.vip/ca is likely fraudulent. It mimics a legitimate site but uses a suspicious subdomain. Avoid using it.

Reviewed Intelligence Sources

----

1. https://www.reddit.com/r/purolator/comments/1kcq7h6/is_this_a_scam/
Fraudsters make subdomains to make it LOOK like it's a legit link, but that last part right before the dot com is the actual site you're going

End of Domain Report

==