

Wildcard TLDs...

...AKA “Revisiting old advice...”

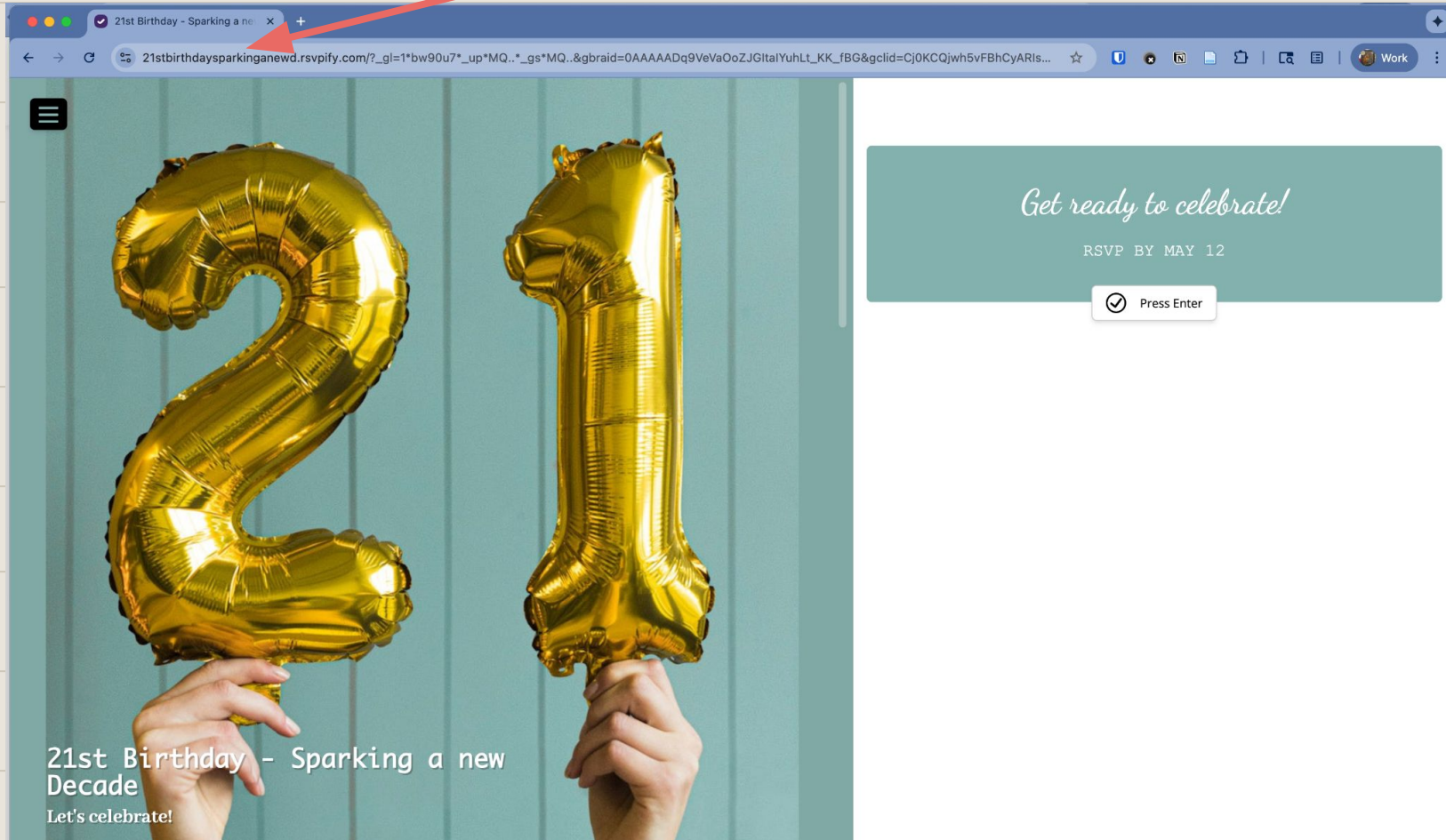
Wildcard Prohibition

- [ICANN “REGISTRY AGREEMENT”](#) (Jan 2014)

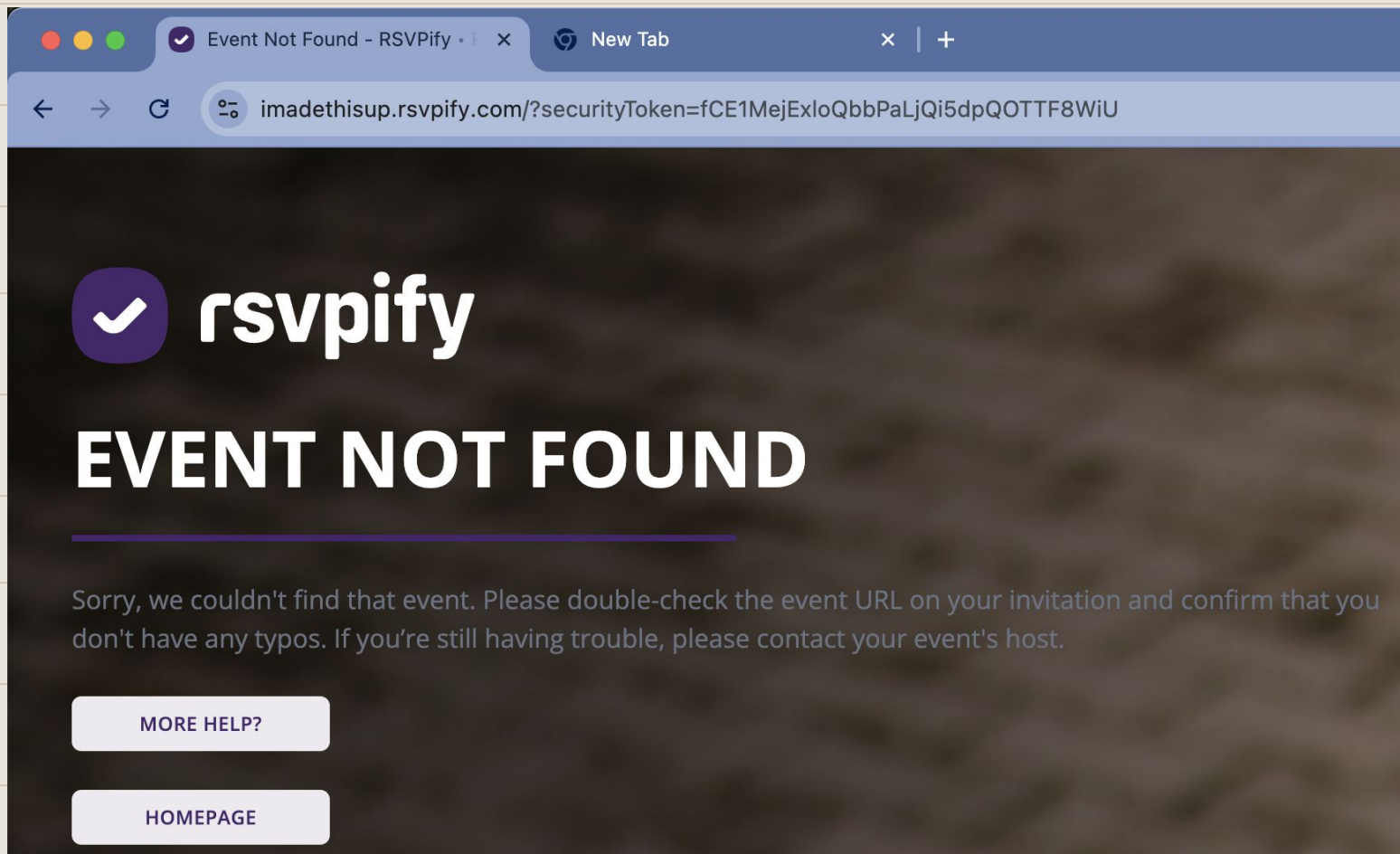
2.2. Wildcard Prohibition.

For domain names which are either not registered, or the registrant has not supplied valid records such as NS records for listing in the DNS zone file, or their status does not allow them to be published in the DNS, the use of **DNS wildcard Resource Records** as described in RFCs 1034 and 4592 **or any other method or technology for synthesizing DNS Resources Records** or using redirection within the DNS by the Registry is **prohibited**.

Wildcards in the wild... 21stbirthdaysparkinganewd.rsvispfy.com



Wildcards in the wild...



How do they do that?!!!

```
$ dig imadethisup.rsvpify.com
; <<>> DiG 9.10.6 <<>> imadethisup.rsvpify.com
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; ANSWER SECTION:
imadethisup.rsvpify.com. 300      IN      A      104.18.30.45
imadethisup.rsvpify.com. 300      IN      A      104.18.31.45

;; Query time: 30 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
```

Two “types” of wildcards:

- Wildcard records themselves
 - `*.rsvpify.com. IN A 104.18.30.45 ; Catches any subdomain for rsvpify.com`
- Synthesized answers
 - The nameserver generates answers on the fly...

So many wildcards in the wild...

a-mo.net

adjust.com

adnxs.com

ampproject.org

ap4r.com

appsflyersdk.com

azurefd.net

b-cdn.net

bing.com

datadoghq.com

duolingo.com

everesttech.net

fbsbx.com

firetv captiveportal.com

gcdn.co

githubusercontent.com

googleapis.com

googleusercontent.com

ifconfig.me

intentiq.com

kargo.com

kaspersky.com

live.com

mail.ru

mikrotik.com

msn.com

omnitagjs.com

onedrive.com

onelink.me

onesignal.com

pki.goog

qualtrics.com

reddit.com

run.app

sentinelone.net

sentry.io

shopify.com

slack.com

speedtest.net

svc.ms

taobao.com

telegram.org

ui.com

userapi.com

visualstudio.com

vivoglobal.com

vk.com

withgoogle.com

xhamster.com

xnxx-cdn.com

xvideos-cdn.com

yandex.com

yandex.ru



So, presumably
wildcards are
fine?!

Why are wildcards prohibited in TLDs?!

- In 2003, a large registry installed a wildcard in their TLD
- This was designed to provide helpful search answers if an unregistered domain was queried
 - Example: rome.travel → search result page with flights and hotels in Rome

Push back

- Phishing
 - www.bankofameric.com
- Loss of privacy
 - www.alkoholicsanonymouse.com
- Email
 - RCPT TO: bob@example.com → long delays, or bounce → privacy
 - SPAM detection - does MAIL FROM: <something>@example.com exist?!
- Protocol confusion
 - How do e.g SNMP or SIP or XMPP or... handle wildcard results?
- Caches
 - 12:01 - example.com → NXDomain. 12:02 - example.com → 192.0.2.1

Many documents...

- [SAC006 - Redirection in the COM and NET Domains](#) (Jul 2004)
- [SAC015 - Why Top Level Domains Should Not Use Wildcard Resource Records](#) (Nov 2006)
- [SAC041 - Recommendation to prohibit use of redirection and synthesized responses by new TLDs](#) (June 2009)
- [ICANN RSTEP Report on Internet Security and Stability Implications of the Tralliance Corporation search.travel Wildcard Proposal](#) (Nov 2006)
- [ICANN "REGISTRY AGREEMENT"](#) (Jan 2014)
- [RFC4592 - "The Role of Wildcards in the Domain Name System"](#) (July 2007)

Wildcard Prohibition

- ICANN “REGISTRY AGREEMENT” (Jan 2014)

2.2. Wildcard Prohibition.

For domain names which are either not registered, or the registrant has not supplied valid records such as NS records for listing in the DNS zone file, or their status does not allow them to be published in the DNS, the use of **DNS wildcard Resource Records** as described in RFCs 1034 and 4592 **or any other method or technology for synthesizing DNS Resources Records** or using redirection within the DNS by the Registry is **prohibited**.

Why is this OK for RSVPify,
but not for a TLD?!

TLD has multiple
registrants in the zone...

...except for Brand TLDs

K. So what's your point...

- <https://www.youtube.com/c/veritasium/videos> -> <https://veritasium.youtube>
- https://www.google.com/maps/place/221B+Baker+St,+London+NW1+6XE,+UK/@51.5234508,-0.1582897,711m/data=!3m2!1e3!4b1!4m6!3m5!1s0x48761acf33628211:0x445d7677a88322e1!8m2!3d51.5234508!4d-0.1582897!16s%2Fg%2F11bw4hsx_m!5m1!1e1?entry=ttu -> <https://sherlock.maps>
- **This makes Brand TLDs actually useful and valuable**



We are asking the SSAC to
revisit the earlier SSAC
advice.

Restrictions...

- 1. TLD must only be a single registrant - Spec 13 Brand TLDs**
- 2. Must point at a “service”, not “website”**
 - This is to prevent cookie theft/supercookies, phishing pages and similar**
 - Litmus test: Wildcard cannot point at user provided HTML/JS**
- 3. No MX records**
- 4. Must do DNSSEC & HSTS preload**

Making Brand TLDs useful...

Source:
<https://dns.coffee/tlds/graveyard>

Dead TLDs 150				
TLD	Created	Removed	Age	Domains
dunlop	Jun 11, 2016	Oct 21, 2025	9 years, 4 months, 10 days	2
bentley	Jul 10, 2015	Apr 23, 2025	9 years, 9 months, 13 days	28
guardian	May 14, 2016	Mar 05, 2024	7 years, 9 months, 20 days	48
comcast	Jul 08, 2016	Feb 06, 2024	7 years, 6 months, 29 days	2
xfinity	Jul 08, 2016	Feb 06, 2024	7 years, 6 months, 29 days	2
bananarepublic	Aug 05, 2016	Jan 22, 2024	7 years, 5 months, 17 days	2
oldnavy	Aug 05, 2016	Jan 22, 2024	7 years, 5 months, 17 days	2
volkswagen	Jan 10, 2016	Nov 20, 2023	7 years, 10 months, 10 days	5
kinder	Oct 10, 2015	Nov 02, 2023	8 years, 23 days	8
rocher	Nov 07, 2015	Nov 02, 2023	7 years, 11 months, 26 days	3
cbs	Aug 05, 2016	Oct 25, 2023	7 years, 2 months, 20 days	11
showtime	Aug 05, 2016	Oct 25, 2023	7 years, 2 months, 20 days	2
cityeats	Nov 11, 2015	Oct 18, 2023	7 years, 11 months, 7 days	2
frontdoor	Jun 24, 2016	Oct 18, 2023	7 years, 3 months, 24 days	48
northwesternmutual	Apr 07, 2016	Aug 08, 2023	7 years, 4 months, 1 day	5

A decorative graphic in the top right corner consisting of a white triangle pointing towards the top right, with a black triangle pointing towards the top left, creating a corner effect.

**THANK
YOU!**

Backup...

- [CAB Forum Baseline Requirements Section 3.2.2.6 Wildcard Domain Validation:](#)
 - A CA is not prohibited from issuing a Wildcard Certificate to the Registrant of an entire gTLD, provided that control of the entire namespace is demonstrated in an appropriate way."
- ["ICANN Registry Services Technical Evaluation Panel Report on Internet Security and Stability Implications of the Tralliance Corporation search.travel Wildcard Proposal"](#)
 - These documents all raise very valid concerns around the use of wildcards at the TLD level - but these concerns are all related to the fact that there are multiple users (registrants) within the TLD, and so the wildcard would co-exist with other registrations. Our proposed usage is restricted to Google-operated closed TLDs, where Google would be the only "registrant", and the wildcard would capture all queries. This is basically identical to <anything>.[rsvpify.com](https://www.rsvpify.com) going to a page with information about an event.
- <https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm> **Specification 6 paragraphs 1.1 and 2.1**
 - This states: " Wildcard Prohibition. For domain names which are either not registered, or the registrant has not supplied valid records such as NS records for listing in the DNS zone file, or their status does not allow them to be published in the DNS, the use of DNS wildcard Resource Records as described in RFCs 1034 and 4592 or any other method or technology for synthesizing DNS Resources Records or using redirection within the DNS by the Registry is prohibited. When queried for such domain names the authoritative name servers must return a "Name Error" response (also known as NXDOMAIN), RCODE 3 as described in RFC 1035 and related RFCs. This provision applies for all DNS zone files at all levels in the DNS tree for which the Registry Operator (or an affiliate engaged in providing Registration Services) maintains data, arranges for such maintenance, or derives revenue from such maintenance."