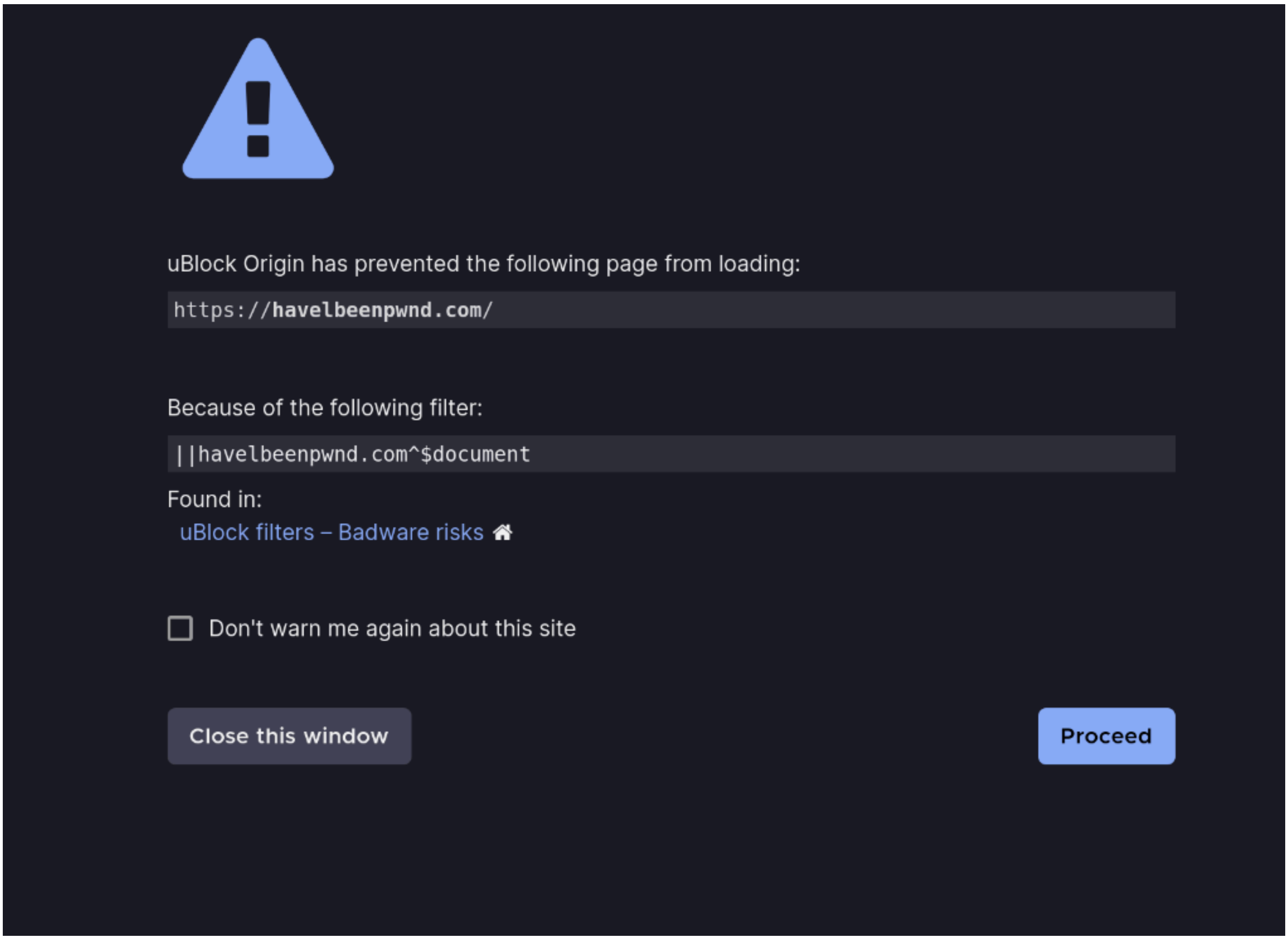
Have I Been Pwned - A Case of Typo Squatting

Have I Been Pwned - A Case of Typo Squatting

Have I Been Pwned is a wonderful tool made publicly available to everyone thanks to Troy Hunt for checking if certain credentials have been involved in a data breach. It can be a great way to be aware of where some risks you may have exist, and hadn't previously known about.

Ublock Origin saved me (again)



uBlock Origin has prevented the following page from loading:

```
https://havelbeenpwnd.com/
```

Because of the following filter:

```
||havelbeenpwnd.com^$document
```

Found in:
uBlock filters – Badware risks

□ Don't warn me again about this site

That's an L instead of an i

Danger: DO NOT CLICK

There are spaces intentionally put here to prevent you doing so.

https:// havelbeenpwnd . com/

Explanation:

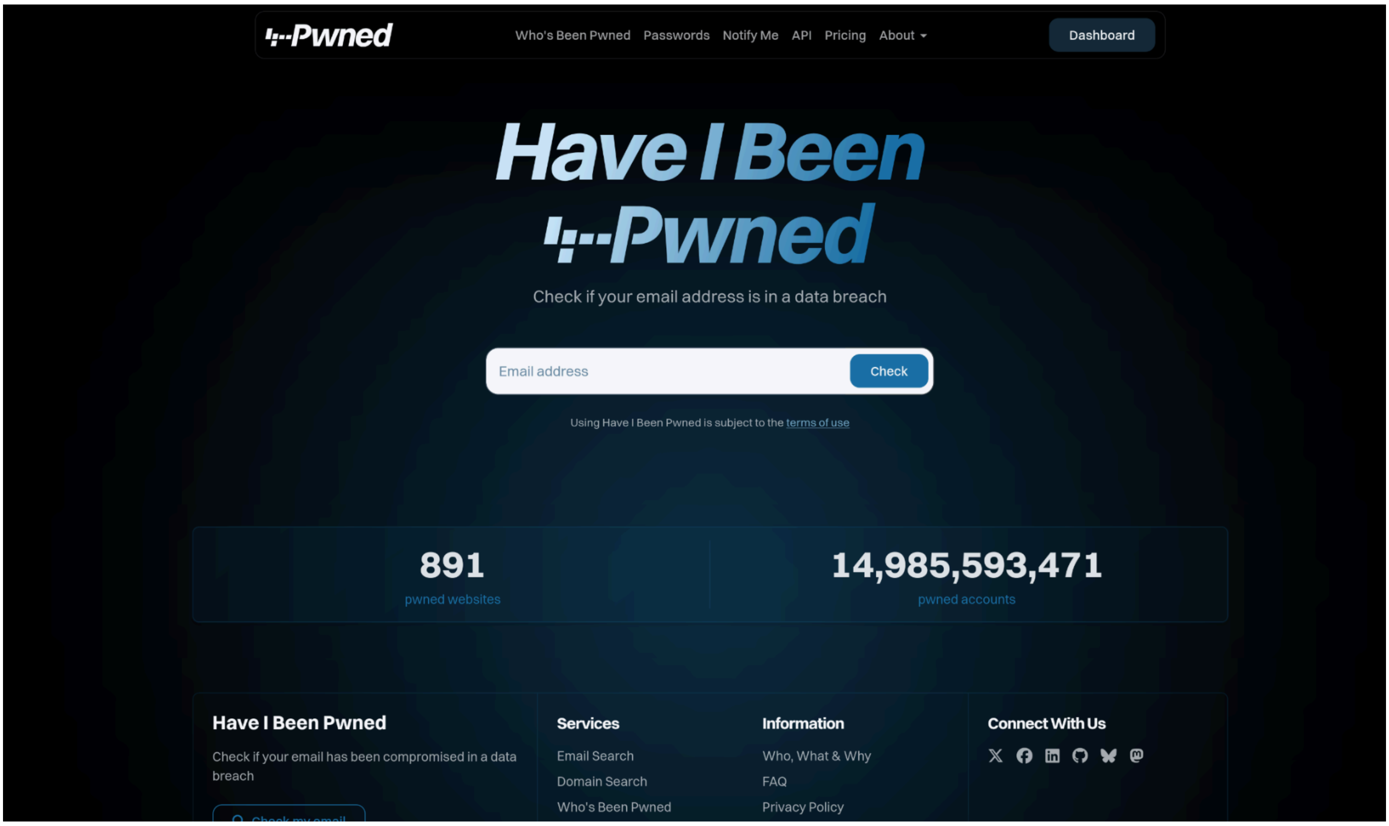
Typo squatting is when you intentionally try to mimic or imitate the domain or subdomain of another.

In this case, we see "Have L Been Pwned" rather than the actual site, which is "Have I been Pwned" this is another case of fonts that have potential for ambiguity, and I'd really like to see them done away with entirely because of this. Something simple and impossible to confuse with tricks like this, such as Times New Roman.

It is for this reason I highly recommend all organizations implement both ad blockers and DNS Security filtering such as Cisco's Umbrella service, or for your homelab, Pi-hole or Adguard Home DNS. For ad blockers, I recommend Ublock Origin Lite for the enterprise setting. Ublock Origin is also FOSS, so your orginization may audit its source code at any time if needed for regulatory or compliance reasons.

Why Lite over regular Ublock Origin? Gareth Heyes at PortSwigger explained it perfectly here with: uBlock, I exfiltrate: exploiting ad blockers with CSS

Correct site:



Check if your email address is in a data breach

Using Have I Been Pwned is subject to the terms of use

891
pwned websites

14,985,593,471
pwned accounts

Have I Been Pwned

Check if your email has been compromised in a data breach