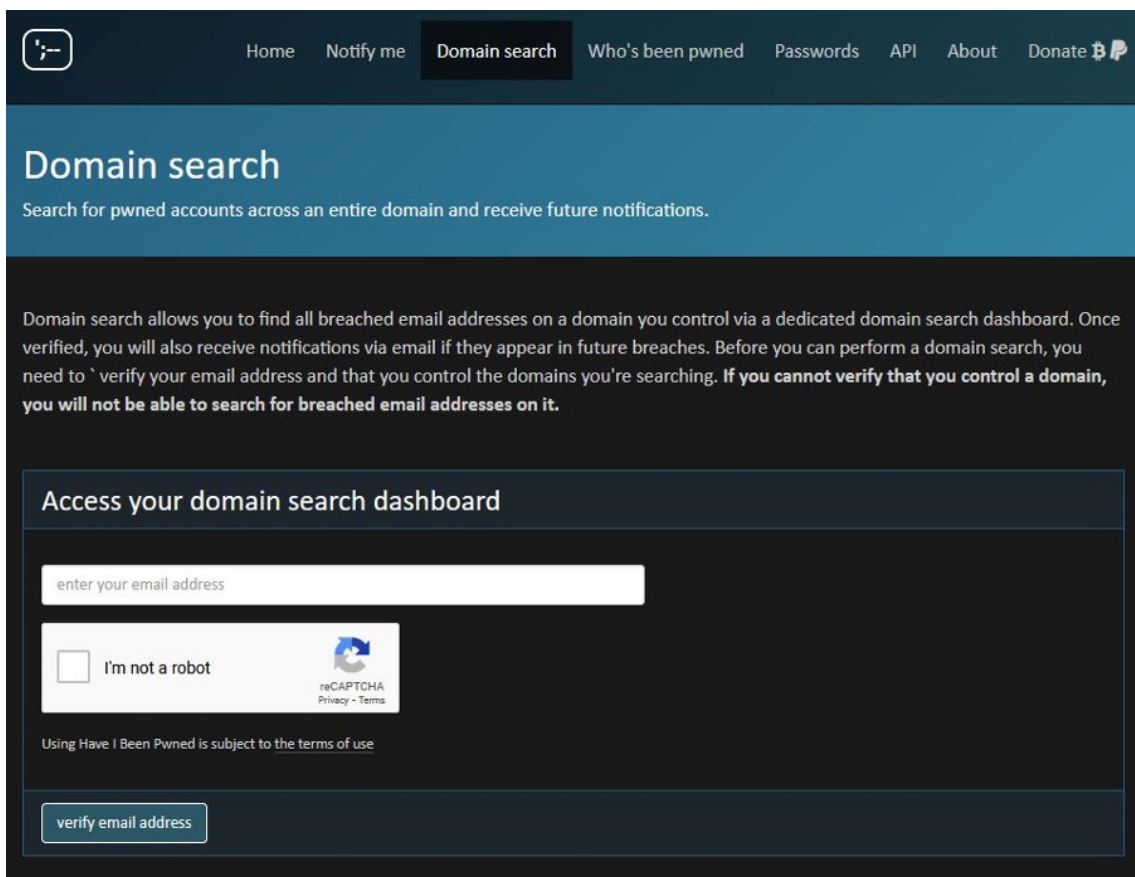


# Overenie úniku prihlasovacích údajov pre konkrétnu doménu

(v rámci známych databáz únikov v službe HaveIBeenPwned)

- 1) Prejdite na webstránku <https://haveibeenpwned.com/DomainSearch>
- 2) Zadaťte svoju e-mailovú adresu, ktorú chcete overiť. Vyplňte reCAPTCHA. V overovacom e-maile kliknite na overovací odkaz.

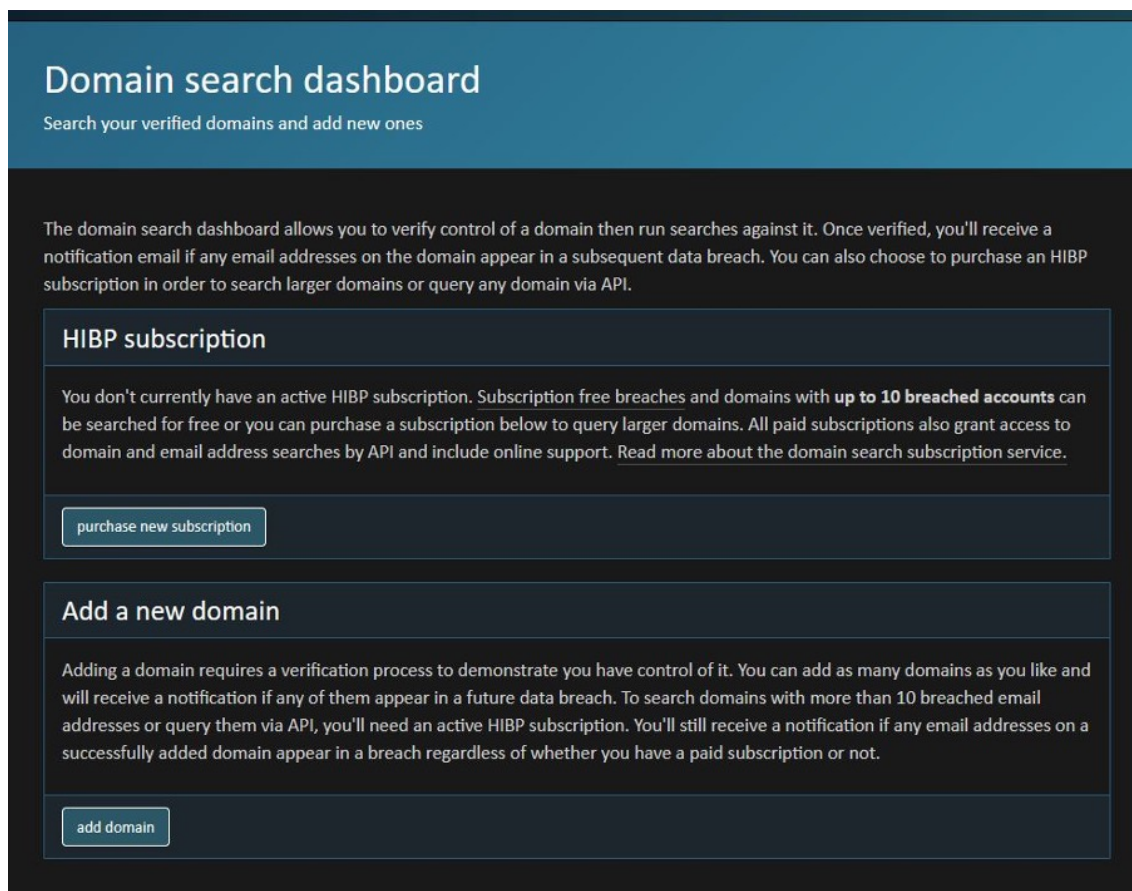


The screenshot shows the 'Domain search' page of the Have I Been Pwned website. The page has a dark blue header with navigation links: Home, Notify me, Domain search (active), Who's been pwned, Passwords, API, About, and Donate. Below the header, the 'Domain search' section is highlighted in a lighter blue. It contains the text: 'Search for pwned accounts across an entire domain and receive future notifications.' Below this, a paragraph explains the domain search process: 'Domain search allows you to find all breached email addresses on a domain you control via a dedicated domain search dashboard. Once verified, you will also receive notifications via email if they appear in future breaches. Before you can perform a domain search, you need to `verify your email address and that you control the domains you're searching. **If you cannot verify that you control a domain, you will not be able to search for breached email addresses on it.**' Below the text is a form titled 'Access your domain search dashboard'. The form contains a text input field labeled 'enter your email address', a reCAPTCHA widget with the text 'I'm not a robot', and a link to 'verify email address' at the bottom. A small note at the bottom of the form states: 'Using Have I Been Pwned is subject to the terms of use'.

# Overenie úniku prihlasovacích údajov pre konkrétnu doménu

(v rámci známych databáz únikov v službe HavelBeenPwned)

3) Vyberte možnosť „add domain“.



The screenshot shows the 'Domain search dashboard' interface. It has a blue header with the title and a subtitle 'Search your verified domains and add new ones'. Below the header, there is a paragraph explaining the dashboard's functionality. The main content area is divided into two sections: 'HIBP subscription' and 'Add a new domain'. The 'HIBP subscription' section includes a paragraph about the subscription service and a 'purchase new subscription' button. The 'Add a new domain' section includes a paragraph about the verification process and an 'add domain' button.

## Domain search dashboard

Search your verified domains and add new ones

The domain search dashboard allows you to verify control of a domain then run searches against it. Once verified, you'll receive a notification email if any email addresses on the domain appear in a subsequent data breach. You can also choose to purchase an HIBP subscription in order to search larger domains or query any domain via API.

### HIBP subscription

You don't currently have an active HIBP subscription. Subscription free breaches and domains with **up to 10 breached accounts** can be searched for free or you can purchase a subscription below to query larger domains. All paid subscriptions also grant access to domain and email address searches by API and include online support. [Read more about the domain search subscription service.](#)

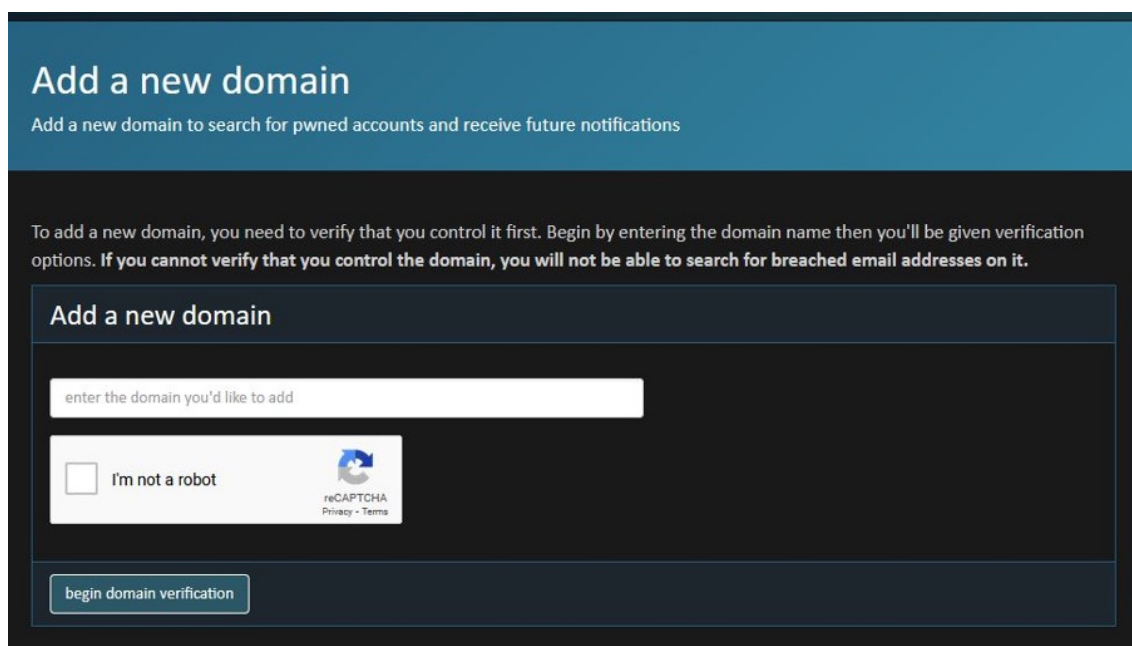
[purchase new subscription](#)

### Add a new domain

Adding a domain requires a verification process to demonstrate you have control of it. You can add as many domains as you like and will receive a notification if any of them appear in a future data breach. To search domains with more than 10 breached email addresses or query them via API, you'll need an active HIBP subscription. You'll still receive a notification if any email addresses on a successfully added domain appear in a breach regardless of whether you have a paid subscription or not.

[add domain](#)

4) Vyplňte názov domény, pre ktorú chcete skontrolovať úniky. Vyplňte reCAPTCHA a kliknite na „begin domain verification“.



The screenshot shows the 'Add a new domain' form. It has a blue header with the title and a subtitle 'Add a new domain to search for pwned accounts and receive future notifications'. Below the header, there is a paragraph explaining the verification process. The main content area is divided into two sections: 'Add a new domain' and a form. The 'Add a new domain' section includes a text input field for the domain name, a checkbox for 'I'm not a robot' with a reCAPTCHA logo, and a 'begin domain verification' button.


## Add a new domain

Add a new domain to search for pwned accounts and receive future notifications

To add a new domain, you need to verify that you control it first. Begin by entering the domain name then you'll be given verification options. **If you cannot verify that you control the domain, you will not be able to search for breached email addresses on it.**

### Add a new domain

enter the domain you'd like to add

☐ I'm not a robot  reCAPTCHA  
Privacy • Terms

[begin domain verification](#)

# Overenie úniku prihlasovacích údajov pre konkrétnu doménu

(v rámci známych databáz únikov v službe HavelBeenPwned)

- 5) Zvoľte spôsob overenia, že ste majiteľom danej domény.
- Najjednoduchším spôsobom je prvá možnosť, kedy vám služba pošle overovací kód na jedno z vybraných preddefinovaných emailových kont.
  - Môžete nahrať meta tag do koreňového priečinka domény.
  - Môžete nahrať súbor do koreňového priečinka domény.
  - Môžete vytvoriť záznam TXT pre vašu doménu.

### Verify your authorisation for domain csirt.sk

You can verify your authorisation for the domain by either responding to one of the standard email addresses below, adding a TXT entry to the domain, adding a meta tag to the HTML at the root of the domain or uploading a .txt file to the site. Leave this page open until the process is complete otherwise you'll need to start again from scratch.

#### Verify by email

Verifying by email is the fastest way to confirm ownership of the domain. You can verify by using one of several pre-defined addresses for the domain.

☐ security@csirt.sk

☐ hostmaster@csirt.sk

☐ postmaster@csirt.sk

☐ webmaster@csirt.sk

send verification email

#### Verify by meta tag

Place the following meta tag in the head of the page at the root of the domain:

<meta name="have-i-been-pwned-verification" value="94726c2c4e58d11f9b78156865086142">

This meta tag should be publicly accessible at <http://csirt.sk>

verify meta tag

#### Verify by file upload

Upload a file to the root of the domain with the following name and contents:

File name:

have-i-been-pwned-verification.txt

File content:

94726c2c4e58d11f9b78156865086142

This file should be publicly accessible at <http://csirt.sk/have-i-been-pwned-verification.txt>

verify file upload

#### Verify by domain TXT record

You can create a TXT record on the domain if it's not a subdomain. The record should have the following value:

have-i-been-pwned-verification=94726c2c4e58d11f9b78156865086142

verify txt record

# Overenie úniku prihlasovacích údajov pre konkrétnu doménu

(v rámci známych databáz únikov v službe HavelBeenPwned)

6) Po overení systém vygeneruje zoznam účtov, ktoré boli pre danú doménu nájdené v databázach únikov dostupných v službe HavelBeenPwned. Tieto dáta si môžete stiahnuť vo formáte HTML, XLSX, alebo JSON kliknutím na príslušnú ikonu.

