

# Verificação de vazamento de dados.

Manual de Orientação quanto a verificação de vazamento de dados pessoais como : email telefone e senha

- [O que é Vazamento de Dados?](#)

# O que é Vazamento de Dados?

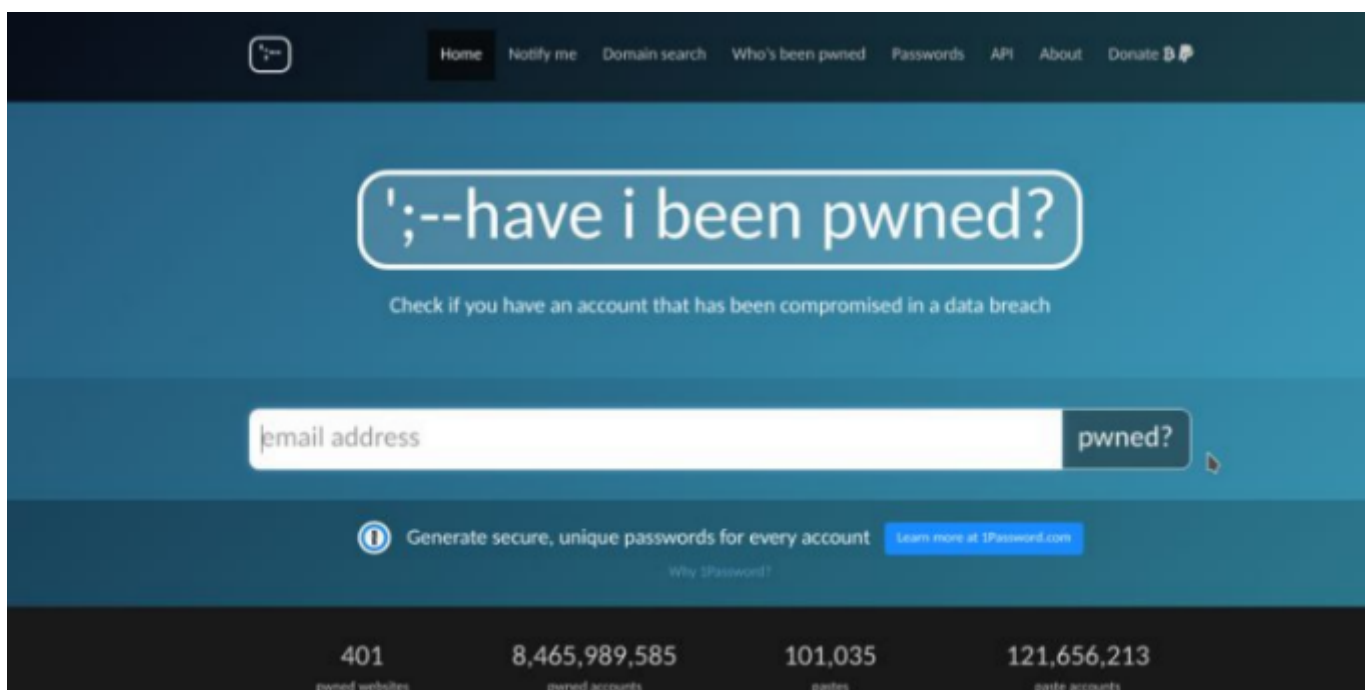
Como a verificar se foi vítima de algum vazamento?

Existem ferramentas online que permitem checar se um email foi identificado em algum vazamento de dados. Sites como <https://haveibeenpwned.com> e <https://monitor.firefox.com> são referências nesse tipo de verificação.

O tutorial a seguir vai ser usando o primeiro site, porém o segundo funciona da mesma forma e é tão intuitivo quanto o primeiro. Ao final, existe uma configuração adicional que pode ser feita no Google Chrome para complementar.

Acessar o site


<https://haveibeenpwned.com> e verificar se algumas das suas contas de emails foram comprometidas e se dados seus foram expostos.




The screenshot shows the homepage of the 'have i been pwned?' website. The header is dark blue with a navigation menu containing links: Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main content area has a light blue background. At the top, there's a large white rounded rectangle containing the text 'have i been pwned?'. Below this, a smaller text says 'Check if you have an account that has been compromised in a data breach'. In the center, there's a search bar with the placeholder text 'email address' and a button labeled 'pwned?'. Below the search bar, there's a section with an information icon and the text 'Generate secure, unique passwords for every account', followed by a link 'Learn more at 1Password.com'. At the bottom, there's a dark blue footer with four statistics: '401 pwned websites', '8,465,989,585 pwned accounts', '101,035 pwned', and '121,656,213 pwned accounts'.

| Statistic      | Value         |
|----------------|---------------|
| pwned websites | 401           |
| pwned accounts | 8,465,989,585 |
| pwned          | 101,035       |
| pwned accounts | 121,656,213   |


Nos sites que as informações foram comprometidas é necessário que as senhas sejam alteradas. Se você usa o mesmo nome de usuário e a mesma senha para outras contas, redefina a senhas delas também.



**Step 1** Protect yourself using 1Password to generate and save strong passwords for each website.








**Step 2** Enable 2 factor authentication and store the codes inside your 1Password account.



**Step 3** Subscribe to notifications for any other breaches. Then just change that unique password.


[Start using 1Password.com](#)

Why 1Password?

     [Donate](#)

### Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.



**Dubsplash:** In December 2018, the video messaging service Dubsplash suffered a data breach. The incident exposed 162 million unique email addresses alongside usernames and PBKDF2 password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.in".

**Compromised data:** Email addresses, Geographic locations, Names, Passwords, Phone numbers, Spoken