

O que é Vazamento de Dados?

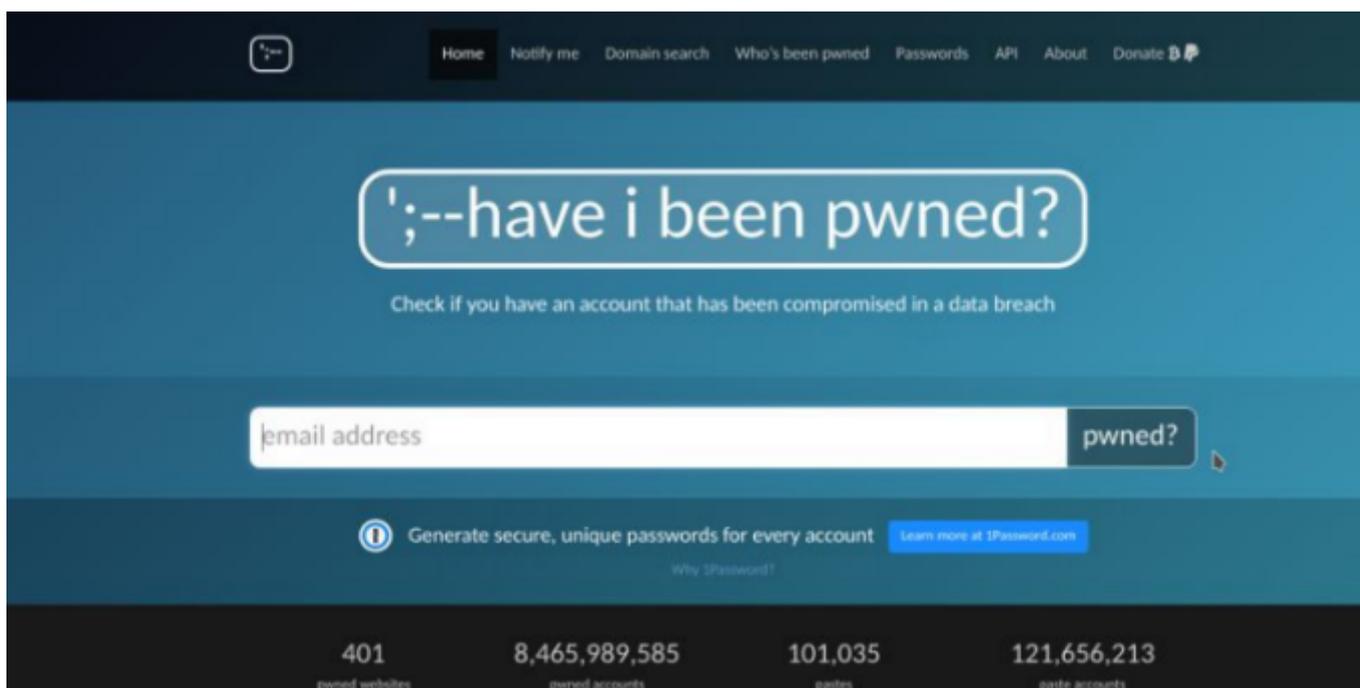
Como a verificar se foi vítima de algum vazamento?

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.



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.

The screenshot shows a dark red background with white and yellow text and icons. At the top left, there is a blue information icon followed by the text '3 Steps to better security'. To the right, there is a blue button that says 'Start using 1Password.com'. Below this, there are three yellow boxes, each containing an illustration and text. The first box shows a person holding a blue circle with the password 'CUV6U4!GU' and the text 'Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.' The second box shows a person at a desk with a laptop and a blue circle, with the text 'Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.' The third box shows a person at a desk with a laptop and a blue envelope icon, with the text 'Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.' Below these steps, there is a small 'Why 1Password?' link and a 'Donate' button with social media icons. The bottom section is titled 'Breaches you were pwned in' and contains a paragraph explaining what a breach is. Below this, there is a large, colorful 'D' icon and a section titled 'Dubsmash' with text describing a data breach in December 2018. At the bottom, there is a line of text: 'Compromised data: Email addresses, Geographic locations, Names, Passwords, Phone numbers, Spoken'.

3 Steps to better security [Start using 1Password.com](#)

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.

[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.

D **Dubsmash:** In December 2018, the video messaging service Dubsmash 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.im".

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

Revision #5

Created 25 February 2023 12:27:06 by Josivaldo Lisboa de Oliveira

Updated 11 September 2023 13:08:59 by Josivaldo Lisboa de Oliveira