

Have I Been Pwned?

In this lesson, you'll find out if your password and/or username were compromised.

We'll cover the following





- Re-using credentials: a real-world story

Remember when you were a teenager, and signed up for your first online service ever? Do you remember the password you used? You probably don't, but the internet might.

Chances are that, throughout your life, you've used an online service that has been subject to attacks, with malicious users being able to obtain confidential information like your password. I'm going to make it personal here: my email address has been seen in at least ten public security breaches, including incidents involving trustworthy companies like LinkedIn and Dropbox.

How do I know?

I use a very useful service called haveibeenpwned.com (HIBP), created by Troy Hunt, an Australian web security expert. The site collects information about public data breaches and allows you to see whether your personal information was in any of these breaches. There's no shame in being involved in one of these data breaches, as it's not really your fault. This is, for example, the result of looking up the email address of Larry Page, one of Google's co-founders:

 [Home](#) [Notify me](#) [Domain search](#) [Who's been pwned](#) [Passwords](#) [API](#) [About](#) [Donate](#) 


';--have i been pwned?

Check if you have an account that has been compromised in a data breach


pwned?

Oh no — pwned!


Pwned on [24 breached sites](#) and found [1 paste](#) ([subscribe to search sensitive breaches](#))

 **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?](#)

Larry's email address has been masked, but it's pretty public information

By knowing when and where an incident happened, you can take a few actions to improve your personal security posture, such as activating two-factor authentication (2FA) and being notified of a breach as soon as HIBP is.

One of the interesting side-effects of HIBP is the ability to use it to improve your business' security. The site offers an API that you can use to verify whether users within your organization were involved in a data breach. This is important as, too often, users consider security an afterthought, and opt out of mechanisms like 2-factor authentication. This quickly becomes disastrous when you think about password re-use, a practice that is way too common. A user signs up to multiple services using the same exact password and when one of those services is breached, the accounts on all the other ones may be breached as well.

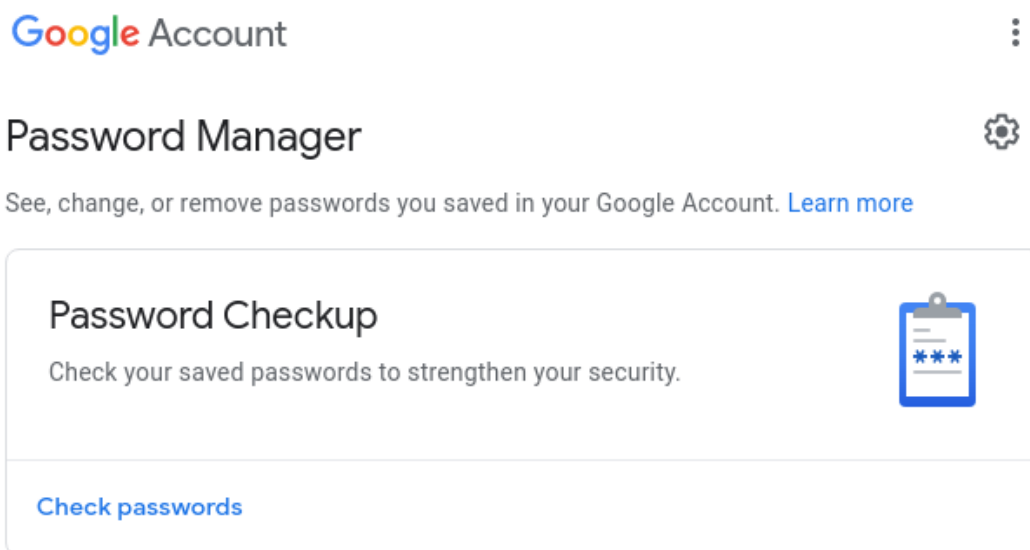
Re-using credentials: a real-world story

I've been directly hit by a password re-use attack during my career, and it wasn't a fun experience.

While I was heading technology at a company, our security team received a message from a researcher claiming he could login into many of our user accounts, sending across plaintext passwords to prove the fact. Baffled, we quickly realized we either were compromised, or someone else had been. When the attacker revealed *how* he got those credentials, we quickly realized they were available to the public through some hardcore googling.

After obtaining a full list of emails included in the breach, we then had to join it with the list of our customers, ending with forcefully resetting the password of the ones found both in the breach and our own database.

In an effort to improve overall privacy and security, Google took steps to offer a service similar to HIBP and rolled their Password Checkup service in late 2019, available at passwords.google.com.






Given the fact that Chrome allows you to safely store passwords, it offers a few additional insights around your credentials. It's not only able to alert you on which passwords are at risk of having been compromised, but it will also let you know when you reuse the same ones on different sites, or when passwords are too weak and at risk of being easily guessed by attackers.

← Password Checkup



We analyzed your saved passwords and found the following issues

| | | |
|---|--|---|
|  | 7 compromised passwords Change these passwords now | ▼ |
|  | 138 reused passwords Create unique passwords | ▼ |
|  | 138 accounts using a weak password Create strong passwords | ▼ |



See personalized security recommendations for your Google Account in the Security Checkup. [Get started](#)

Google Password Checkup gives an analysis of your 'password health'

As you've probably read elsewhere, the best method to protect your online credentials is to use a password manager that can generate long and complicated passwords without you having to come up with creative strings and remember them every time you need to login on a website. If you don't use a password manager, I'd strongly suggest using one such as [1Password](#), [LastPass](#) or even your browser's built-in password manager.

Choose your username



Your username is how other community members will see you. This name will be used to credit you for things you share on Reddit. What should we call you?

CHOOSE A USERNAME


jane_doe_1234567



PASSWORD

Use suggested password u8cVkRXxj fwj pwq

Chrome will save this password in your Google Account. You won't have to remember it.

Here are some username suggestions 

[Altruistic-Escape](#)

[AccomplishedArcher1](#)

[Longjumping-Tip](#)

[Virtual-Independent](#)

[Complex-Contribution](#)

Back

SIGN UP

Chrome's own password manager will suggest a strong password for you to use when creating an account on a website

In the next lesson, we'll see how to work with a stateless architecture.