Is the password manager on the browser secure enough?

Most major browsers like Chrome, Firefox and Opera come with integrated password manager. But the question is: Are they reliable?

Whichever browser you choose, you often get an optional question: 'Do you save the password for this site?' If you have many different passwords and can't remember all your passwords, using a browser-based password manager is a great time-saver and makes life more convenient. Most major browsers like Chrome, Firefox and Opera come with integrated password manager. But the question is: Are they reliable?

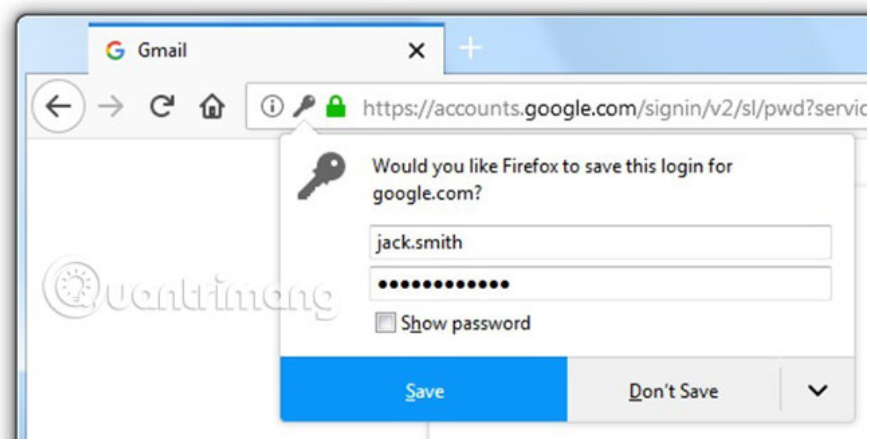
Should I use the password manager on the browser?

1. Is the password manager on the browser safe?
    1. Firefox
    2. Opera
    3. Chrome
    4. Safari
2. How to strengthen defenses and keep passwords safe?
    1. Dedicated password manager
    2. Two-factor authentication

Is the password manager on the browser safe?

While it is very convenient and saves time, the password manager on the browser gives users a sense of inaccuracy, especially in case the browser leaks information. Consider how some of the top web browsers handle user password archiving!

Firefox



If you use Firefox and enter a password on a web page, the browser will ask if you want to save the password. If you choose yes, Firefox will save the password on the device and you can view the saved password in the **Options** window **.** When you visit the website again, Firefox will automatically fill in the saved password.

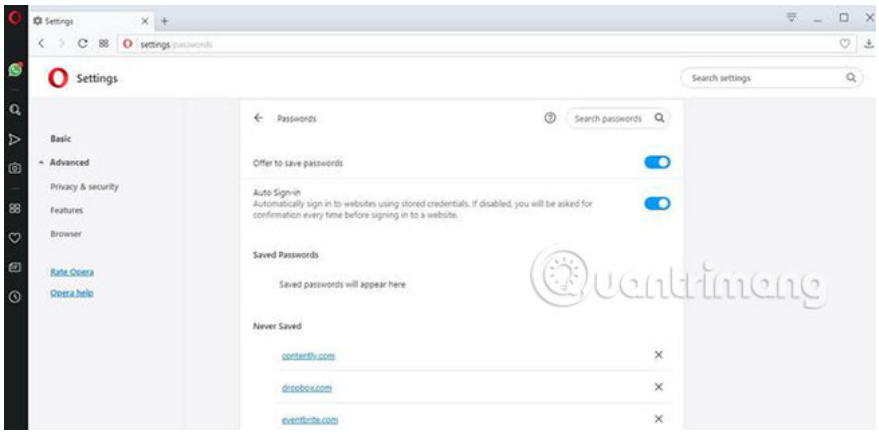
By default, Firefox saves passwords in an insecure format on your computer, but you can enable the master password in the **Options** window **.**

Any password you save is encrypted with this master password and you must enter it before using the password manager. In this way, no one can see your password, if you close Firefox (even if they have access to the computer).

Through **Firefox Sync,** you can synchronize passwords and because they are encrypted before syncing, you can backup them online, then sync between devices.

Firefox browser password manager is the safest way to remember passwords, thanks to the master password. The downside is that you cannot access Firefox's saved passwords on iOS or other mobile platforms.

Opera



This browser faces an attack on the previous system and hackers already have access to some personal information of browser users, including passwords and account information.

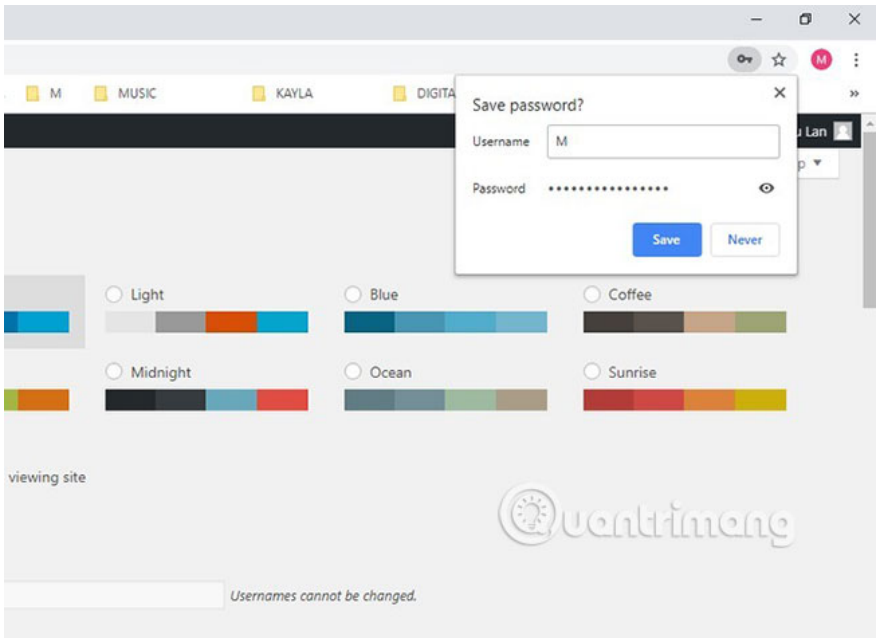
This happens with the **Opera Sync** feature **, which** helps users synchronize passwords on many different devices. For example, if users have saved their Twitter passwords in Safari, Chrome or Opera on the desktop, they will also find the password on the mobile device, as long as they are logged in.

Finally, Opera has to reset all synchronized account passwords and to prevent any uncertainty, users are also required to reset the password for both the browser and the third-party website.

This problem is a serious reminder of how risky browser password managers are and if it happens to Opera, it's likely to happen to other browsers as well.

Worse is the security level of the password manager on the browser is unclear, although always commit that your password has been encrypted.

Chrome



This browser always tries its best to keep the user's password secure. But security is always prioritized in second place. Users often appreciate the more convenient, but unfortunately convenient does not mean safety.

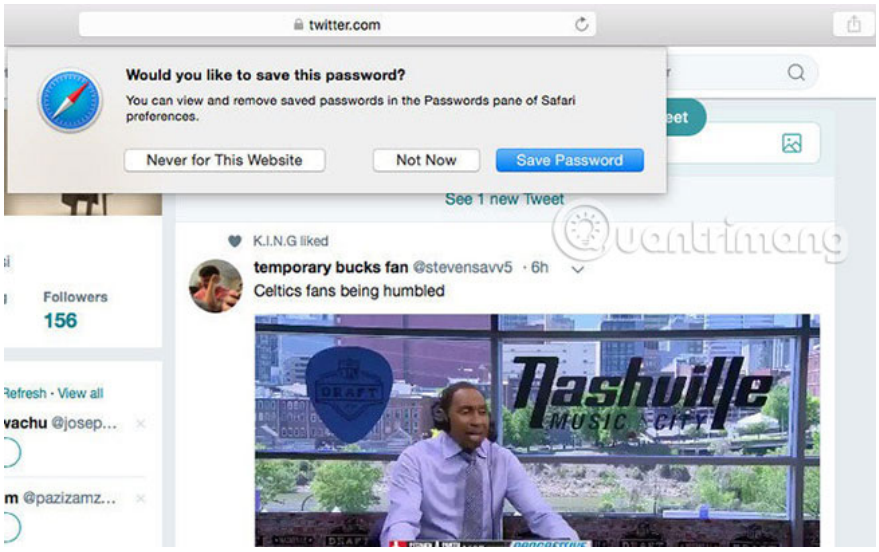
However, it should be noted that Google is trying to improve its password manager. Recently, Google introduced a central location, from which you can manage the password that Chrome is storing, as part of the **Smart Lock** feature set **.** This **password.google.com** platform is protected by two-factor authentication, so that only users with the right account can access the site.

Another advantage is that an improved password manager in Chrome provides automatic password generation, when you register for the first time.

Passwords that are securely stored in your Google account are synced on Chrome versions for mobile devices and desktops. This prevents Chrome users from continually selecting the same password for every site, as well as preventing the heavy consequences that users will experience, when a website is compromised or leaks data.

However, even with these new changes, you should still use a separate password manager.

Safari

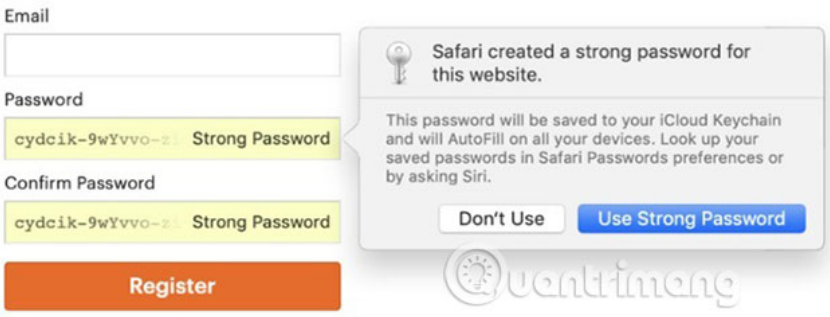


Safari also has an integrated password manager, which automatically fills in website passwords when you log in to new websites.

This integrated password manager can also store contact and credit card information and if you have access to **iCloud Keychain,** it will sync this information in an encrypted file on the device you own. .

One of the challenges with Safari's integrated password manager is that you can only access it through Apple devices. If someone steals or you lose your device, you cannot access your password until you have a new device replaced.

However, the browser creates and stores strong passwords for you to ensure they are unique and reliable.



When Safari stores passwords, it automatically fills them on Apple devices. In the **Preferences** settings **,** you can see the password you have used many times and update them easily.

The downside is that Safari lacks the two-factor authentication and is not as robust as the third-party password managers.

How to strengthen defenses and keep passwords safe?

Dedicated password manager

Browser-based password managers do not require strong passwords. Otherwise, their reliability will be much greater than the current level. A good password manager - like Dashlane, LastPass, etc. - can help you create and keep passwords better.

If you have to choose between convenience and security, this is a worthy trade-off. Dedicated password manager does better than what your browser offers.

Two-factor authentication

Most of the services you can use, including Google, online banking and social networks provide an extra layer of protection. This protection may be in the form of code that you receive via SMS on the phone. You can also use **YubiKey** or **Google Authenticator.**

Other ways you can keep your password safe include:

1. Update device software to get important security patches.
2. Do not install the software from any other place, in addition to the official website of the device manufacturer or operating system vendor such as Apple, Microsoft or the app store managed by Google.
3. Do not store valuable secrets in the password manager.
4. Use many different strong passwords each time you register on a new website. Avoid reusing old passwords.
5. Only register on sites with valid SSL certificates.
6. Update your browser regularly, every time a new security update is released.
7. Study each browser extension you use before installing.
8. Do not use Autofill auto-fill features.
9. Install powerful anti-virus or anti-malware software on all devices and schedule regular scans.
10. Do not log in to the site with a public WiFi connection.

All of the above browsers have a password manager built into it. They can be convenient and save time, but not enough to keep all your passwords safe.

Have you been a victim of password management violations? Are you using a browser password manager? Share your experience with everyone in the comment section below!