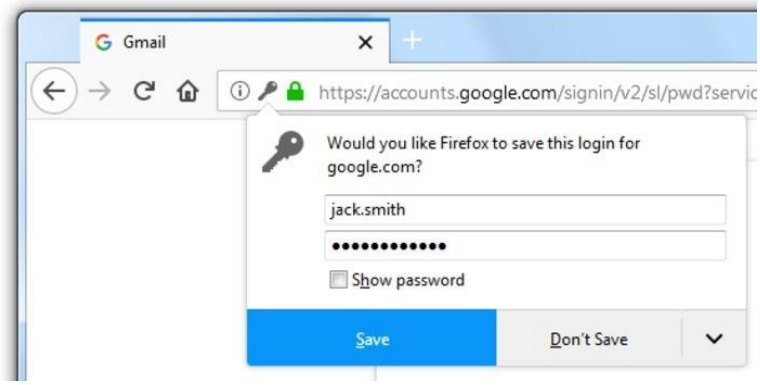
Browser Password Managers: Are They Good Enough? - Make Tech Easier

Whatever your browser of choice is, you'll often get an option that asks: "*Save password for this site?*" If you have several passwords or can't remember the last combination, browser-based password managers are terrific time-savers and make life more convenient. Most major browsers like Chrome, Firefox, and Opera all come with a built-in password manager. The question is, how reliable are they?

Are Browser Password Managers Safe?

As much as they're convenient and save time, browser password managers offer a false sense of security, especially in the event of a browser breach. Let's look at how some of the top web browsers fare.

Firefox



If you use Firefox and enter a password on a website, the browser will ask if you want it to remember the password. If you save the password, Firefox will save it on your device, and you can view saved passwords in the Options window. When you revisit the website, Firefox autofills the password you saved.

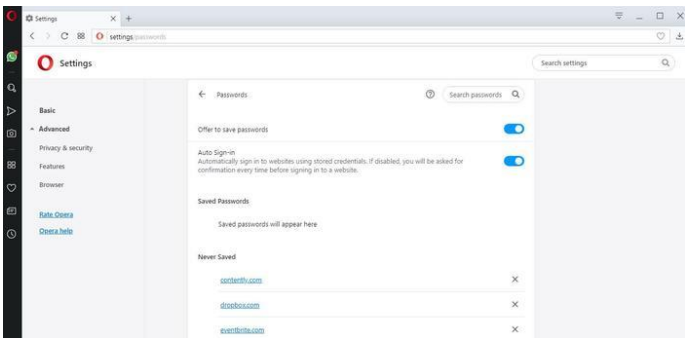
By default, Firefox saves passwords in an insecure form on your computer, but you can enable a master password in the options window.

Any passwords you save are encrypted with this master password which you have to enter before using the password manager. In this way no one can see your passwords even if they access your computer if you close Firefox.

Through Firefox Sync, you can sync passwords, and because they're encrypted before syncing, you can back them up online and sync them between devices.

Firefox's browser password manager is the safest owing to the master password feature. The downside is you cannot access Firefox's saved passwords on iOS or other mobile platforms.

Opera



This browser had an attack on its systems some time back, and the hackers must have gained access to some personal information of the browser's users, including passwords and account information.

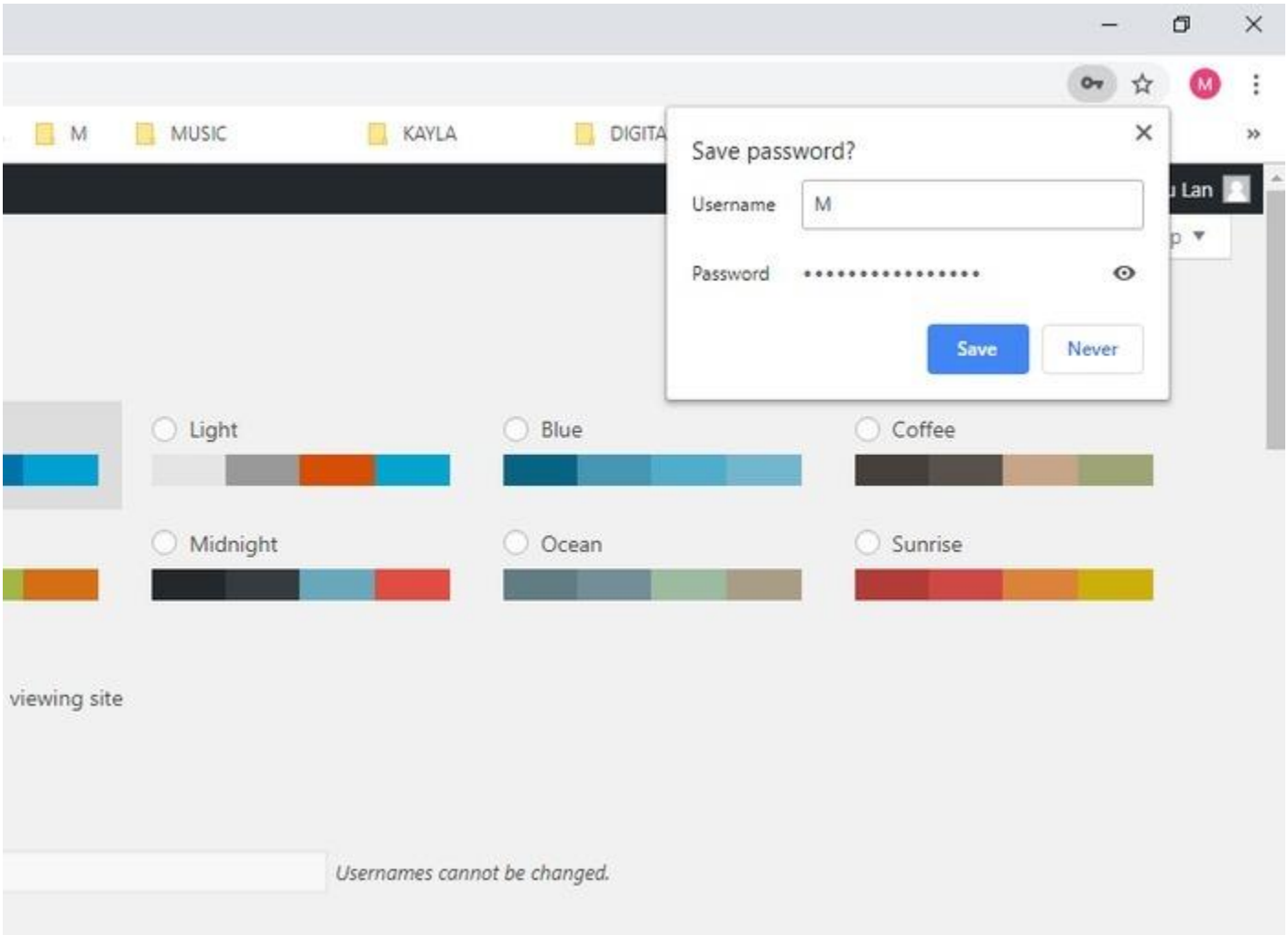
This happened with the Opera sync, which helps users coordinate their passwords across different devices. For example, if a user saved his Twitter password in Safari, Chrome, or Opera on desktop, they'd find it waiting for them on their mobile devices as long as they are logged in.

Eventually, Opera had to reset all Opera sync account passwords, and as a precaution, requested its users to reset their passwords both for the browser and third-party sites.

This incident is a stark reminder of how risky browser password managers are, and if it happened to Opera, it is likely to happen with other browsers.

Even worse is that it isn't quite clear how secure they really are, even though they say your passwords are always encrypted.

Chrome



Browsers can do as much as they can to keep your passwords safe, but security will probably be a second priority, as the feature is meant for convenience, not necessarily making life safer.

But this doesn't mean they're not taking any steps to improve their password managers.

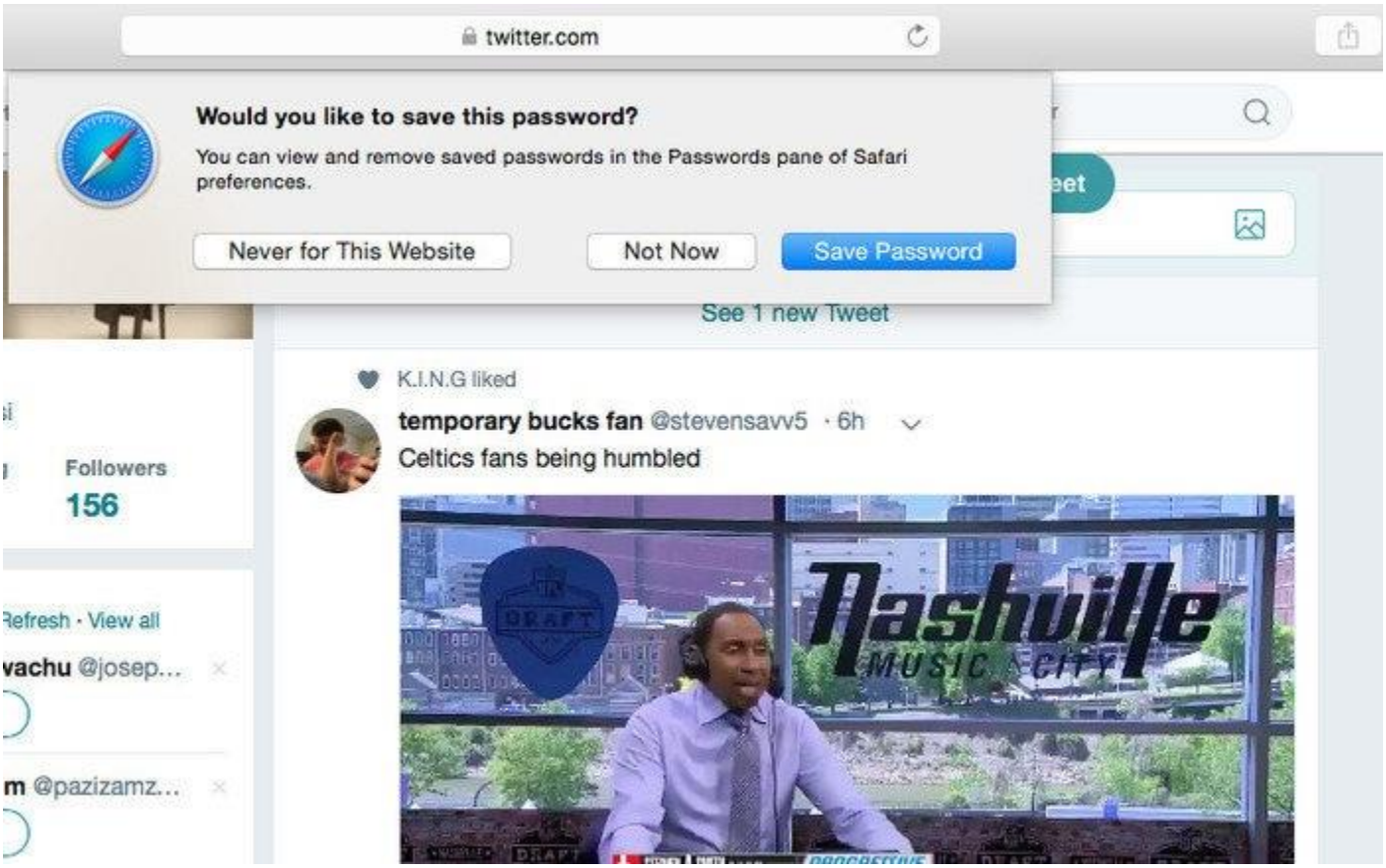
Recently, Google introduced a central place from where you can manage the passwords that Chrome keeps, as part of its Smart Lock suite. The platform, passwords.google.com, is protected by two-factor authentication so that only the genuine account user can gain access to the site.

Another feature is their improved password manager in Chrome that offers to generate random passwords automatically when you sign up to websites the first time.

The password is stored securely in a Google account that is synced across Chrome mobile and desktop versions. This prevents regular Chrome users from constantly picking similar passwords for every site. It also prevents the painful experiences users go through when a site is compromised or breached.

However, even with these new changes, you may still want to use a separate, dedicated password manager.

Safari



Safari also has a built-in password manager, which autofills website passwords for a new login or when you log into new sites.

It can also save your contact and credit card information, and if you have iCloud Keychain access, it syncs this information in an encrypted file across your devices. One of the challenges with Safari's built-in password manager is you can only access it through Apple devices. If someone steals your device or you lose it, you may not access your passwords until you replace it. However, the browser creates and stores strong passwords for you to ensure they're unique and robust.

Once Safari stores passwords, it autofills them across your Apple devices. In the Preferences setting, you can see passwords you've used more than once and update them easily.

The downside is it lacks two-factor authentication and isn't nearly as robust as third-party password managers.

How to Stay Safe and Bolster Your Defenses

Dedicated Password Manager

Browser-based password managers also don't require strong passwords; otherwise they'd add more value than they currently do. A good password manager – like Dashlane, LastPass and others – can help you create and keep stronger, and better passwords.

If you had to choose between convenience and security, this is a fair trade-off. It makes password managers better than what your browser offers.

Two-factor authentication

Most services you may use, including Google, banking platforms and social networks offer an extra layer of protection. This can be in the form of a code that you get via SMS to your phone. You can also use YubiKey or Google Authenticator.

Other ways you can stay safe include:

- Update your device software to get crucial security patches.
- Don't install software from anywhere other than the official device manufacturer or OS provider like Apple, Microsoft, or Google-managed app storesl
- Do not store valuable secrets in password managers.
- Use different strong passwords with each signup on a site; avoid reusing passwords.
- Register only on sites with valid SSL certificates.
- Update browsers regularly with each security update rolled out.
- Research each browser extension you use before installing it.
- Do not use auto-fill features.
- Install a strong antivirus or anti-malware software on all devices and schedule regular scans.
- Don't log into websites using public WiFi connections.

Final Thoughts

All these browsers have password managers built into them. However, they may be okay for convenience and to save time, but they're not good enough in terms of securely managing all your passwords.

Have you been a victim of password manager breaches? Or do you use browser password managers? Share your experience in a comment below.