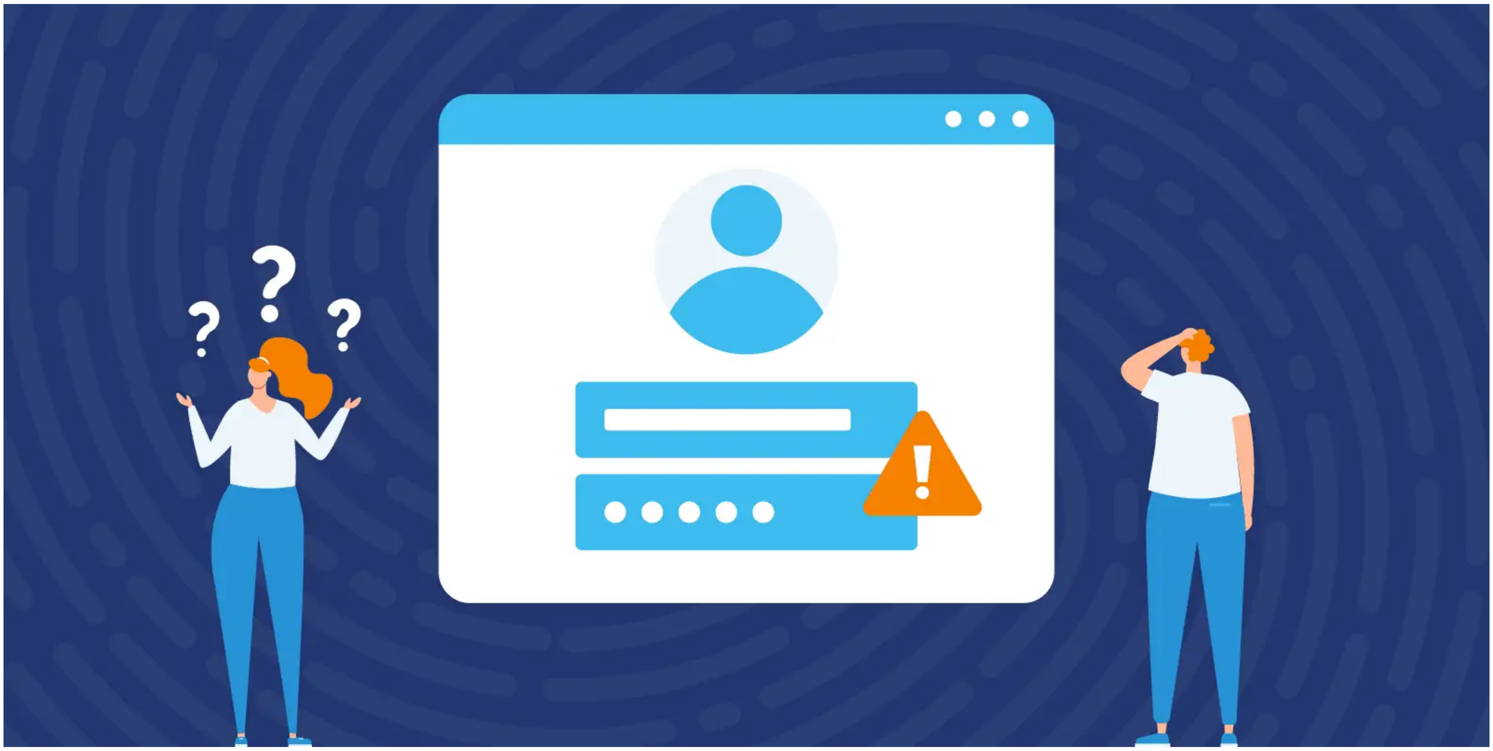
Is Your Browser’s Password Manager Safe?

By: Liz Wegerer

Update: 03-14-2022

Reading time: 11 minutes



Click here for a short summary about browser password managers

In today’s tech-driven world, most of us rely on the internet to manage our day-to-day lives. From checking in on social media to reading emails to paying bills, we log in online multiple times each day.

People **serious about managing online risk often rely on password managers** as part of their security strategy. These convenient tools create computer-generated passwords that are complex, unique, and difficult for hackers to figure out. Password managers also keep your private information safe in a secure, encrypted location.

There are **two types of password managers**: third-party apps and the password manager built into your web browser. Password manager apps are plentiful on the market, and we’ve

But what about the password manager found in your favorite browser? Will it meet your needs? More importantly, is it safe? Read on to find out if the built-in password managers found in Chrome, Safari, Firefox, and Edge are right for you.

Are Browser Password Managers Safe?

For many years, security experts recommended never saving passwords in your browser. Historically, third-party password managers offered better encryption than their in-browser competitors. They also eliminated the risk of your passwords falling into the hands of someone who gains access to your computer, either physically or remotely.

Today, the use of two-factor authentication (2FA) makes in-browser password managers safer, and reduces the risk of unwanted computer access. With this feature turned on, anyone trying to access your account needs more than just your password to succeed. In terms of additional safety, the browsers in Safari, Chrome, Firefox, and Edge **all offer encryption**, and protect your saved passwords with the same security used to keep your email, cloud storage, and devices protected.

The truth is, **no password manager is failsafe**. Even third-party apps have been shown to have security flaws. Even so, password manager apps do incorporate stronger security measures that are needed to ensure the security of their additional functionality (like password sharing and cross-browser availability of data).

However, the companies behind today’s most popular browsers continue to invest heavily in strengthening their security protocols to create a safe and secure environment. Additional safety precautions a user can take, like password-protecting your computer, locking it whenever you are away, and turning on two-factor authentication, add to your overall safety.

An Overview of the Most Popular Browser Password Managers

Today, **every major browser offers a password manager** that uses encryption to keep your information secure. But there are some differences in functionality among the big four – Safari, Chrome, Firefox, and Edge.

BROWSER	OPERATING SYSTEMS	AUTHENTICATION	FEATURE
Safari	✖	✔	✖
Chrome	✔	✔	✔
Firefox	✔	✔	✔
Edge	✔	✔	✖

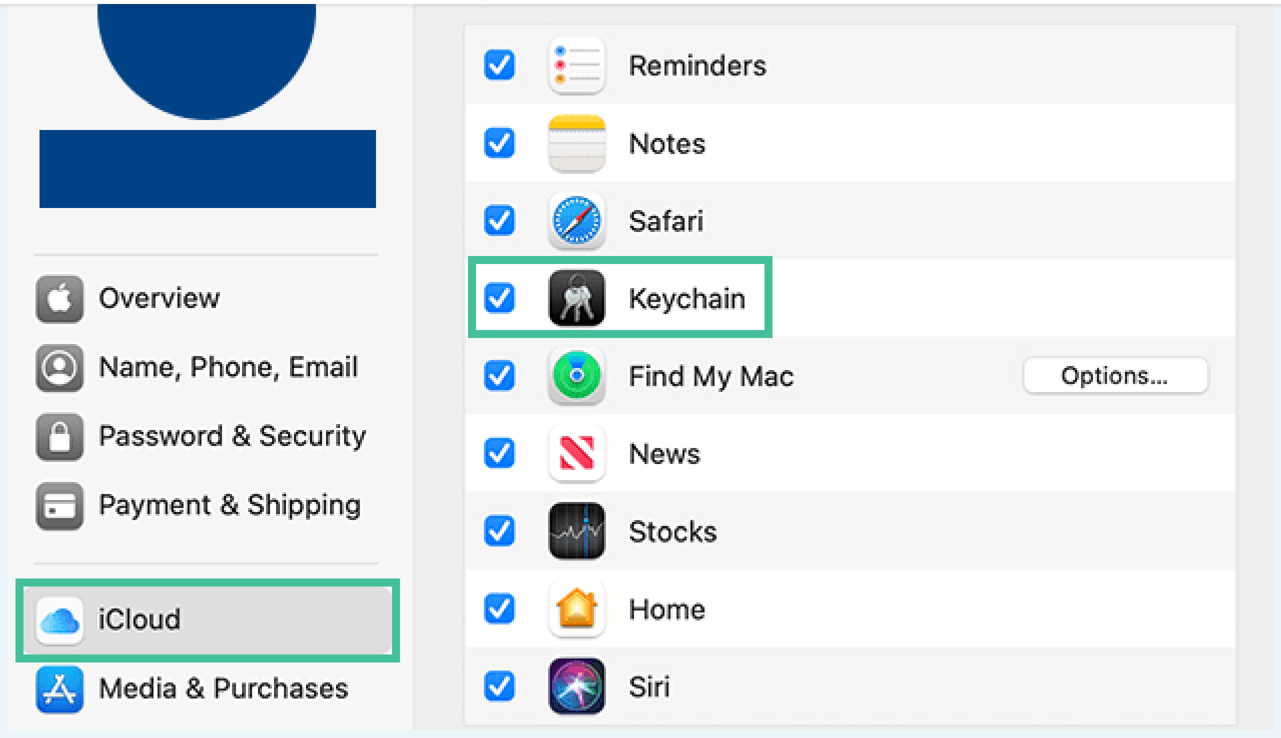
Safari Password Manager: Best for Apple Fans

If every device you own has a stylized fruit symbol on it, Apple's iCloud Keychain is a natural choice for your password manager. It comes pre-installed on every Mac, iPhone, and iPad. You'll need an iCloud account to use Safari's password manager. If you're already using an iPhone, iPad, or Mac (or all three), you likely have an iCloud account.

To use iCloud Keychain, you'll need to enable the feature on each Apple device. Keychain will sync your passwords automatically across every enabled device.

How to turn on iCloud Keychain on your Mac

1. Choose the **Apple** menu and go to **System Preferences**.
2. Click **Apple ID**, then **iCloud** in the sidebar.
3. Tick the **Keychain** box.



☑ Reminders
☑ Notes
☑ Safari
☑ Keychain
☑ Find My Mac
☑ News
☑ Stocks
☑ Home
☑ Siri

How to turn on iCloud Keychain on your iPhone and iPad

1. Tap **Settings**, then tap [**Your Name**], and choose **iCloud**.
2. Scroll down and tap **Keychain**.
3. Slide to turn on **iCloud Keychain***.

*You may be prompted for your Apple ID password to complete this step.

Once enabled, iCloud Keychain will operate in the background. It automatically generates a complex password whenever you create new login credentials on a website. You can also create and save your own passwords. Keychain autofills your saved password on every device where the Autofill feature is activated. Other iCloud Keychain features include notification of passwords involved in data breaches and alerts when it thinks the passwords you create are too weak.

How iCloud Keychain protects your data

Apple uses **end-to-end 256-bit AES encryption** to protect your data. It combines a unique key made from information specific to your device with a passcode you create. This encryption technology means no one else can read your data, not even Apple.

While this is a very safe approach to protecting your data, iCloud Keychain does have an obvious downside. If you don't have all your devices password protected, anyone with your phone, tablet, or computer has your passwords at their fingertips. It's important to always require password or biometric access to your phone, tablet, and computer. You'll also want to enable two-factor authentication for an additional layer of protection.

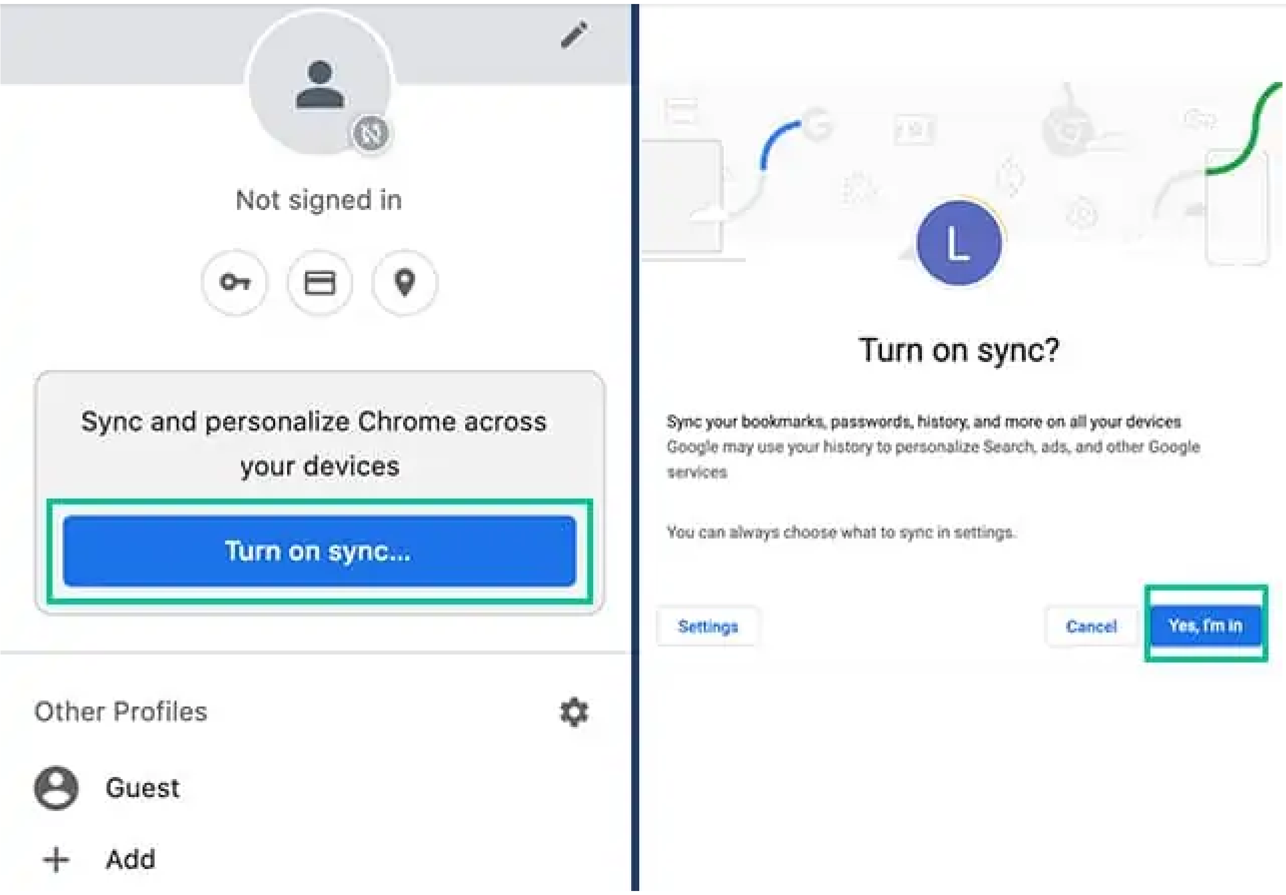
Google Chrome Password Manager: Great across operating systems

Not loyal to one operating system? Google's password manager works wherever you use the Chrome browser. Chrome doesn't care if you're on an Android, Windows, or iOS device. Google offers Chrome apps for all operating systems.

The password manager found in Chrome is tied to a user's Google account. You **must be signed in to your Google account** to use this feature. When you are, your passwords are saved in your Google account and synced on all devices where you're using Chrome. To enable this, turn on the Chrome sync feature on each device.

How to turn on Chrome Sync on your computer

1. Open Chrome.
2. Click **Profile** in the top right of your screen.
3. Click **Turn on sync**.
4. Log in to your Google Account.
5. Click **Yes, I'm In** to turn on sync.



Sync and personalize Chrome across your devices

Turn on sync?

Sync your bookmarks, passwords, history, and more on all your devices

Google may use your history to personalize Search, ads, and other Google services

You can always choose what to sync in settings.

How to turn on Chrome Sync on your Android device

1. Open the Chrome app on your Android phone or tablet.
2. Tap **More**, then **Settings**, then **Turn on sync**.
3. Select the account you want to use.
4. Tap **Yes, I'm In** to turn on Sync.

How to Turn On Chrome Sync on iPhone and iPad

1. Open the Chrome app on your device.
2. **Sign in** to your Google Account.
3. Tap **More …**, then **Settings**.
4. Choose your **Account Name**.
5. Tap **Sync**.

How Chrome Password Manager protects your data

Google uses **AES 256-bit SSL/TLS encryption** for passwords. Google's **passphrase** feature offers an additional layer of security. Passphrase creates a unique primary password that nobody knows, except you. Even Google cannot access your unique passphrase. With Chrome's built-in **Password Checkup** feature, you can see if your login credentials have been involved in a data breach. This feature is turned on by default.

Safety considerations

Although Google takes steps to protect your data with encryption and a passphrase, there are still safety concerns. Anyone who can access your device also has your passwords. It's important to password-protect all your devices. Enabling two-factor authentication boosts security even more.

Perhaps one of the bigger concerns for users is **data sharing**. When you use Chrome password manager, you send all your information to Google, a company in the business of capturing and using data for profit. While there are no known cases of Google compromising account holders' private information in this way, it is something to think about. You can read more about general browser safety here and here.

Firefox Password Manager: Best for privacy and limited data sharing

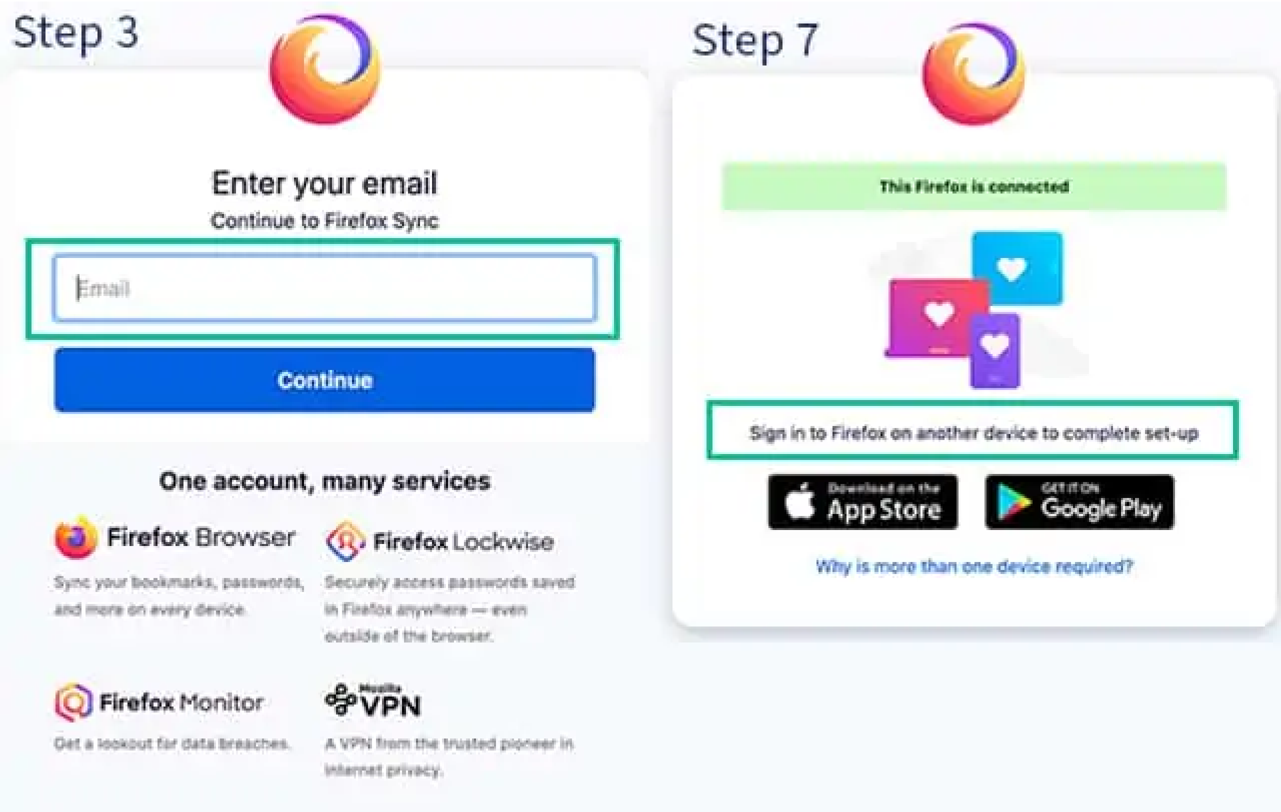
People serious about their online privacy often turn to Mozilla Firefox as their primary browser. Mozilla, the parent company of Firefox, is a non-profit entity with a main focus of online security.

Firefox offers a built-in password manager and syncing across devices. It works on different operating systems. You'll need to sign up for a Firefox account and enable **Firefox Sync** to save and share passwords across devices. But unlike setting up accounts in Google, Microsoft, or Apple, your Firefox account won't be tied to other services, like email or cloud storage.

How to create a Firefox account and turn on Firefox Sync on your computer

1. Open the Firefox browser.

4. If you are creating a new Firefox Account, you will be prompted to create a password and enter your age (required).
5. Choose what to sync.
6. Click **Create Account**.
7. You will be prompted to add a second device. Follow the prompts on that device to complete your Firefox Account and Sync setup.



Enter your email

Continue to Firefox Sync

One account, many services

Firefox Browser

Sync your bookmarks, passwords, and more on every device.

Firefox Lockwise

Securely access passwords saved in Firefox anywhere — even outside of the browser.

Firefox Monitor

Get a lookout for data breaches.

Mozilla VPN

A VPN from the trusted pioneer in internet privacy.

This Firefox is connected

Sign in to Firefox on another device to complete set-up

Why is more than one device required?

As with other in-browser password managers, Firefox will generate strong passwords for you. You can also create and save your own. **Firefox Lockwise** auto-fills your passwords across devices. It operates behind the scenes on your computer, and has a separate app for your phone or tablet.

How Firefox Password Manager protects your data

Firefox uses **256-bit AES encryption** to protect passwords. Enabling the Primary Password feature of Firefox adds an additional layer of safety to the passwords you save. **Firefox Monitor** alerts you if your passwords were involved in a data breach.

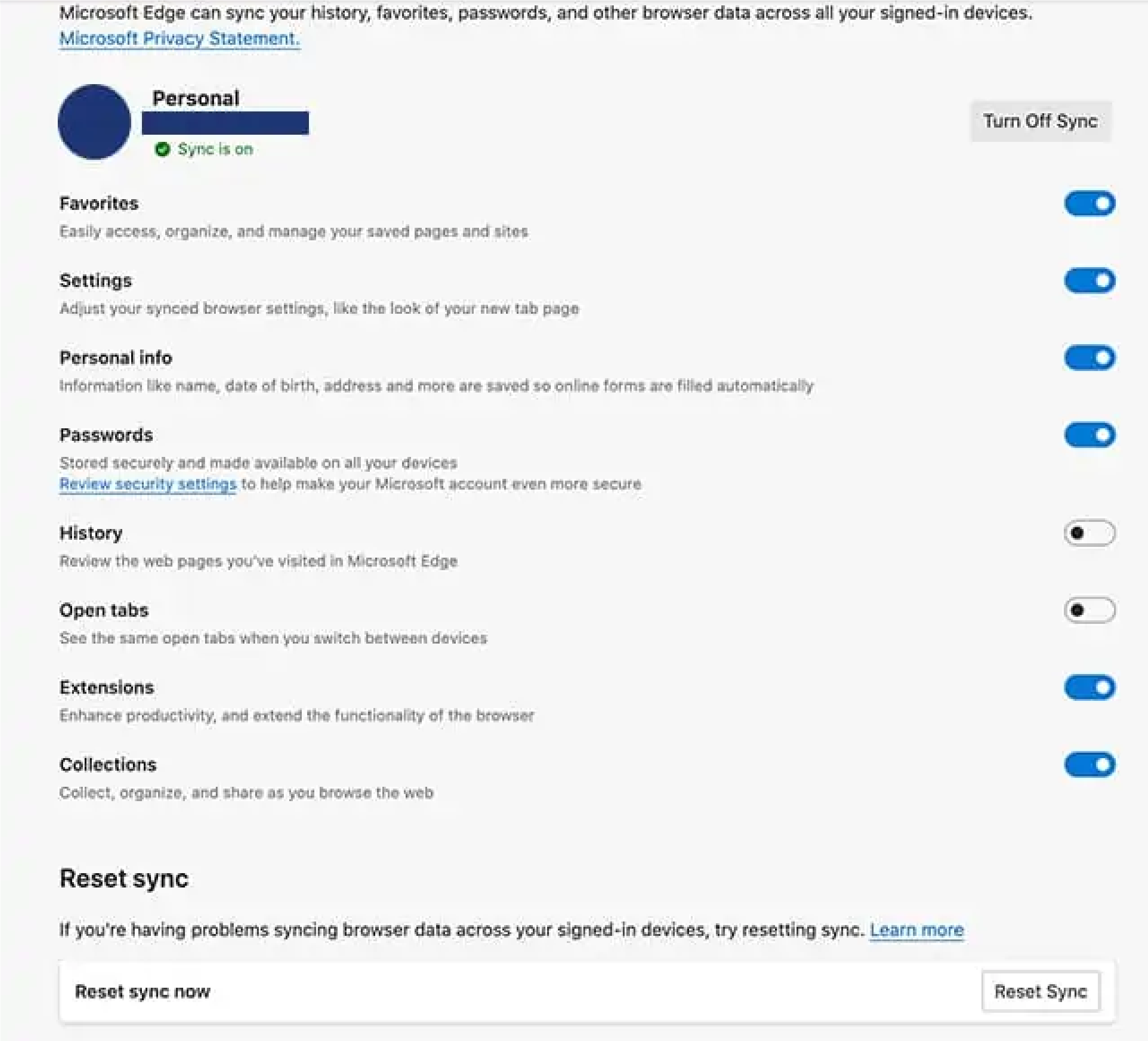
Just as with the other browser-based password managers, your information is only as safe as your device is protected. Incorporating password protection on your phone, tablet, and computer adds a layer of protection. Firefox also offers two-factor authentication, which should be enabled.

Edge Password Manager: Ideal for Microsoft Account users

If you already have a Microsoft account, it's convenient to use the password manager in Edge. When you activate sync, your passwords are available in the Edge browser on every device where you're logged in to your Microsoft account. If you don't already have a Microsoft account, you'll need to create one.

How to turn on Edge Sync on your computer

1. Select your **profile image** in the Edge taskbar.
   Note: If you see Manage Profile Settings, you are already logged in. If not, you'll receive a prompt to log in to your account (proceed to step 3).
2. Select **Manage Profile Settings** > **Sync** > **Turn on Sync**.
3. Click **Sign In** and enter your credentials, then click **Continue**.
4. Choose **Sync** when prompted.



Microsoft Edge can sync your history, favorites, passwords, and other browser data across all your signed-in devices. Microsoft Privacy Statement.

Personal
[redacted]
Sync is on

Favorites ☑
Easily access, organize, and manage your saved pages and sites

Settings ☑
Adjust your synced browser settings, like the look of your new tab page

Personal info ☑
Information like name, date of birth, address and more are saved so online forms are filled automatically

Passwords ☑
Stored securely and made available on all your devices
Review security settings to help make your Microsoft account even more secure

History ☐
Review the web pages you've visited in Microsoft Edge

Open tabs ☐
See the same open tabs when you switch between devices

Extensions ☑
Enhance productivity, and extend the functionality of the browser

Collections ☑
Collect, organize, and share as you browse the web

Reset sync

If you're having problems syncing browser data across your signed-in devices, try resetting sync. Learn more

Reset sync now

How to Turn On Edge Sync on Your Mobile Device

1. **Download** the Microsoft Edge app for iOS and Android.
2. **Sign in** to your Microsoft account.
3. Tap **Sync**.

When you are creating new website login credentials, Edge will auto-generate a complex password. You can also create and save your own. Edge password manager works across multiple browsers and devices. To enable auto-fill on Chrome, you'll need the **Microsoft Autofill extension**. For Android and iOS devices, you can autofill with the **Microsoft Authenticator app**.

Microsoft Edge uses **AES-256 encryption** to protect your confidential information. Microsoft also recently rolled out the [Microsoft's Password Monitor](). This new feature informs you if one of your passwords is identified in a security breach. It also prompts you to change the compromised password. While other browser password managers also offer this feature, Microsoft is unique by using **homomorphic encryption**, a newer cryptographic technology.

Safety concerns

As with Chrome, Firefox, and Safari, the Edge password manager is safe as long as your device doesn't fall into the wrong hands. Always turn on password protection on all your devices. Although Edge **does not offer an extra option to set a master password** within the password manager itself (a feature both Chrome and Firefox offer), you can further secure your Microsoft account with two-factor authentication. You should turn this feature on.

Should You Use an In-Browser Password Manager?

Like all technology, in-browser password managers aren't a magical solution to every security issue. They offer benefits, but also have limitations. When deciding whether to use an in-browser password manager, it comes down to **the functionality you need**.

PROS	CONS
Free	Can't securely share passwords
Easy to use	No cross-browser ability to access saved passwords
No downloads required	No option to change how auto-generated passwords are created

For users who don't need to share login credentials with anyone, an in-browser password manager is a viable option. The same goes for users who stick to a single browser whenever they're surfing the web. In-browser password managers are also already installed with your browser, eliminating the need for you to download anything.

encryption that is needed to support their additional functionality.

Other Ways to Increase Your Online Safety

Whether you choose the password manager in your favorite browser or a third-party app, staying safe online is a priority. Password managers are one of many tools to help you do that.

Besides securing your passwords, there are **other ways to protect yourself** and your confidential data. Install and run an **antivirus program**. There are several free and paid options we recommend. Antivirus software runs behind the scenes, and quickly detects and resolves problems before they escalate.

Another way to stay safe is to maintain your privacy while browsing the web is with a **virtual private network** (VPN). VPNs do three things very well. They make you anonymous on the internet, help to keep hackers and cybercriminals away from your devices, and allow you to access potentially blocked websites.

Don’t forget to **password-protect** all your devices, and **use two-factor authentication** on your accounts whenever it is available. This multi-pronged approach is the best way to stay safe in today’s online world.

In-Browser Password Managers: Frequently Asked Questions

Still have questions about using an in-browser password manager? Check out our most frequently asked questions for more information. Not seeing what you need? Drop a comment below. We’re always happy to help you out.

Are browser password managers safe to use? +

Which browser has the best password manager? +

Liz Wegerer Author

Tech journalist

Liz is a professional writer with a special interest in online privacy and cybersecurity. As a US expat who travels and works in diverse locations around the world, keeping up with the latest internet safety best practices remains her priority.

Share this article

More articles from the "Password Managers" section

Abine Blur Review (2023): Password Manager Safety at a Cost

January 3, 2023

Keeper Review (2023): A Secure Password Manager With Extras

January 3, 2023

RememBear Review (2023): A User-Friendly Password Manager

January 3, 2023

Leave a comment

Name *

E-mail address *

Post comment

Table of contents

More About Password Managers

Abine Blur Review (2023): Password Manager Safety at a Cost

Is Your Browser's Password Manager Safe?

Keeper Review (2023): A Secure Password Manager With Extras

RememBear Review (2023): A User-Friendly Password Manager

The Best Password Managers of 2023: Our Top 5 Picks