BROWSER AUTOFILL SAFETY

Browser autofill items are typically **stored locally on your device**. Here's how it works for different browsers:

- **Google Chrome**: Autofill data is stored in a file called "Web Data" in the browser's profile folder, which is encrypted and accessible only by the browser.
- **Mozilla Firefox**: Autofill data is stored in a file called "formhistory.sqlite" in the browser's profile folder, also encrypted.
- **Microsoft Edge**: Autofill data is stored locally in a folder on your Windows computer, accessible through the LocalAppData folder.
- **Syncing**: Some browsers, like Google Chrome and Safari, allow you to sync autofill data across devices using cloud storage, which means the data is stored on the company's servers. This ensures that your autofill data is secure and can be accessed when needed.

Examples of Browsers Supporting Passkey Autofill:

- **Chrome:** Supports passkey autofill on various platforms, including Android, macOS, and Windows.
- **Safari:** Supports passkey autofill on iOS, iPadOS, and macOS.
- **Edge:** Supports passkey autofill on Windows and mobile devices.

Benefits of Passkey Autofill:

- **Security:** Passkeys are more secure than passwords because they are tied to a specific device and require a strong authentication method.
- **User Experience:** Passkey autofill provides a seamless and convenient login experience, eliminating the need for users to remember passwords.
- **Reduced Risk:** Passkeys reduce the risk of password leaks and phishing attacks.

https://thetechylife.com/where-are-autofill-addresses-stored/

Additional privacy for your saved passwords - Microsoft Support.