

Reasons not to use password manager browser extensions, even though they are very convenient

While password manager browser extensions provide a convenient way to securely save passwords and autofill them, we cannot ignore the potential risks and limitations.

While I'm not completely opposed to browser extensions that help manage passwords, there are some good reasons to avoid them and use desktop or smartphone apps instead.

1. Extensions are browser dependent

The biggest downside to using a password manager browser extension is browser dependency. If you switch browsers, you'll need to install and set them up from scratch. If you switch to a browser that doesn't support these extensions, you'll still have to rely on desktop applications.

If you use multiple browsers and one doesn't support extensions, you'll need to constantly switch between them to copy and paste passwords. Additionally, if you encounter browser sync issues, it may take additional time to resolve before you can use the extension again. Major browser updates can also cause extensions to malfunction, leaving you stranded.

In contrast, password management applications only need to be installed and set up once, so you won't have to worry about the above issues.

2. They increase the risk of fraud



The most compelling reason to avoid using password manager extensions is their increased vulnerability to Phishing attacks. Clicking on malicious links in emails, fraudulent search ads, or links embedded in articles can

compromise your browser. If that happens, scammers can track your activity and steal your passwords.

Sophisticated phishing attacks can also trick such extensions into autofilling passwords on malicious sites, leaking them to scammers.

In contrast, antivirus software built into the operating system will effectively detect malicious hacking attempts and will notify you if the device is compromised. Additionally, manual copy-and-paste passwords let you double-check URLs before entering them, minimizing risk. Likewise, accidentally clicking on a malicious link is less of a risk to your credentials.

Warning : Do not store the secret key you received when setting up a password manager application on your computer; This could allow anyone with access to your computer to gain access to your password.

3. Extensions can affect browser performance

Every new extension you add to your browser increases the amount of work that needs to be done. Because password manager extensions run in the background to monitor and autofill passwords, they constantly consume memory and CPU resources. If you already have many required extensions and are running resource-intensive processes, this can reduce browser performance.

If not managed properly, this can lead to browser crashes or crashes, reducing the usefulness of password management extensions. In contrast, desktop password manager applications only need to open when you need to copy or manage your passwords, instead of running continuously in the background.

4. Extensions do not work offline



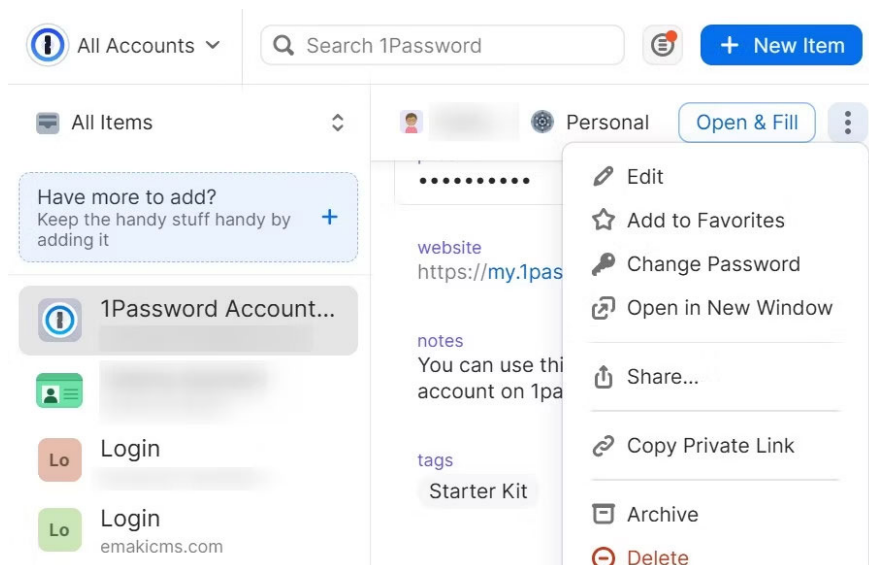
Password manager extensions retrieve credentials from the password manager's cloud storage, so they require an active Internet connection. If you are offline or have Internet connection problems, they may not be able to retrieve stored passwords and therefore may not be able to autofill them. Therefore, you will have to wait until your device reconnects to the Internet.

In contrast, dedicated password management applications for computers or smartphones often store passwords locally, allowing access to stored login information even when offline. Additionally, retrieving passwords from the device reduces risk compared to retrieving in the cloud, where passwords can be intercepted or exposed on unsecured networks.

5. User experience is not great

Another reason to avoid using password manager browser extensions is their cluttered interface and the additional confirmation pop-ups they introduce, which can clutter the experience. browsing. Additionally, with multiple extensions installed, you're bound to accidentally click and open conversations from other extensions.

Furthermore, browser extensions sometimes lack features found in desktop apps, and when they are available, they are often hidden in additional menus, making navigation difficult than. When managing multiple accounts on the same website, browser extensions can automatically fill in the wrong login information for the account, disrupting your workflow.



In contrast, desktop apps typically offer cleaner, easier-to-navigate interfaces, often offering the same features or more capabilities without annoying pop-ups. With manual copy-pasting, you eliminate workflow disruptions that can occur if browser extensions don't autofill. Additionally, precise details can be easily selected when managing multiple accounts.

You finished reading the article "**Reasons not to use password manager browser extensions, even though they are very convenient**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.