Why should you turn off the Autofill feature in the password manager?

Advertisers have found a new way to track users. According to Freedom to Tinker, some ad networks are abusing tracking scripts to get the email address that the password manager automatically fills in to websites.

Advertisers have found a new way to track users. According to Freedom to Tinker, some ad networks are abusing tracking scripts to get the email address that the password manager automatically fills in to websites.

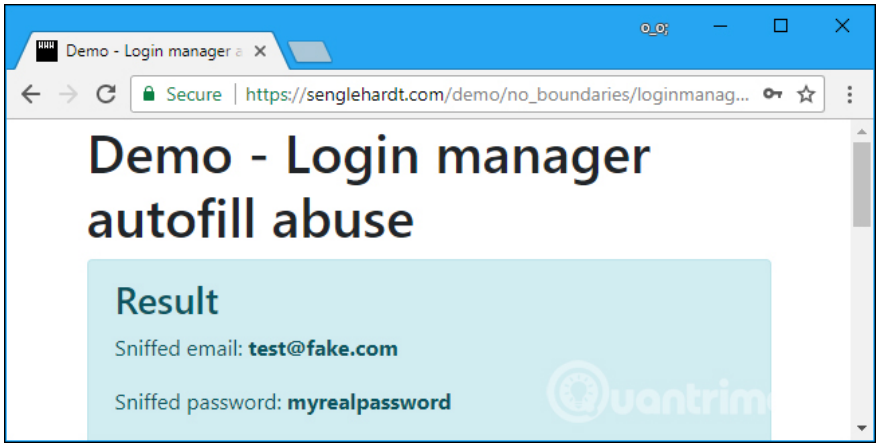
But this situation is even worse when they can use this technology to get your password, if you want. This affects all password manager users such as the built-in password manager in Chrome, Firefox or Edge or browser extensions like LastPass. Therefore, users should turn off the autofill feature to avoid this problem.

How does autofill leak your information?

When saving your username and password on the website, the password manager will remember this information and then it will automatically fill them in the username and password boxes on that site. Password manager will make login faster because you just need to click " **Login** ".

But some third-party advertising scripts used by most websites are being used to track users. They run in the background, create fake login boxes and passwords that users can't see and collect credentials that the password manager automatically fills in.

You can see your problem by visiting this website. Enter a fake email address and password and you will be prompted to save it in your browser password manager. It will then be automatically filled in the background, with the script recording the email address and password. This website does not show any problems if using LastPass extension.

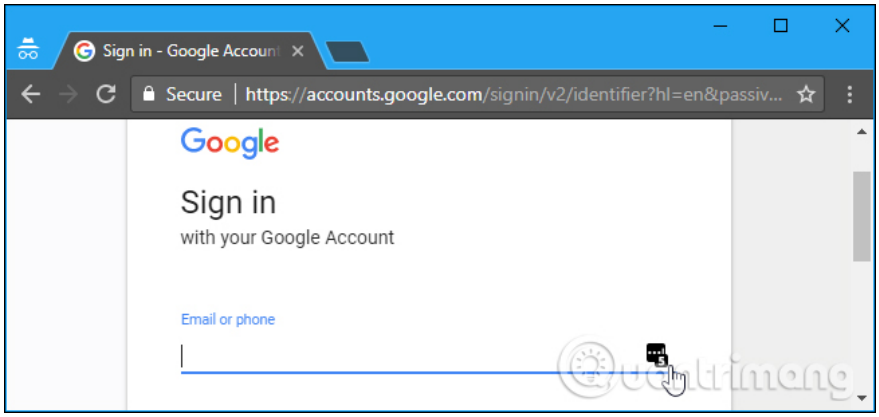


The need for password manager

This issue demonstrates the importance of using unique passwords on a website. According to Freedom to Tinker, this is not just a theory-based attack, advertisers actually used it on the top million websites today to get user names and email addresses, but nothing prevent them from taking your password if they want.
If an advertiser gets your password on the site, they can use that information to log in to this site. This is terrible but not the worst. If you use the same password for other accounts such as email, that person can access your email account and use it to access other accounts. That is the worst thing that can happen. This is why you should still use the password manager and use different passwords for different accounts.

Protect yourself by disabling the autofill feature

However, users can still reduce the risk from these scripts by turning off the autofill feature in the password manager. For example, if you use LastPass extension (not currently affected by these scripts, but theoretically possible), the autofill feature will fill in the login fields with your login credentials to simply Click "Login". If you disable the autofill feature, you will have to click the LastPass icon in the password field and click on the username to enter the saved information. This will protect your information from being stolen.

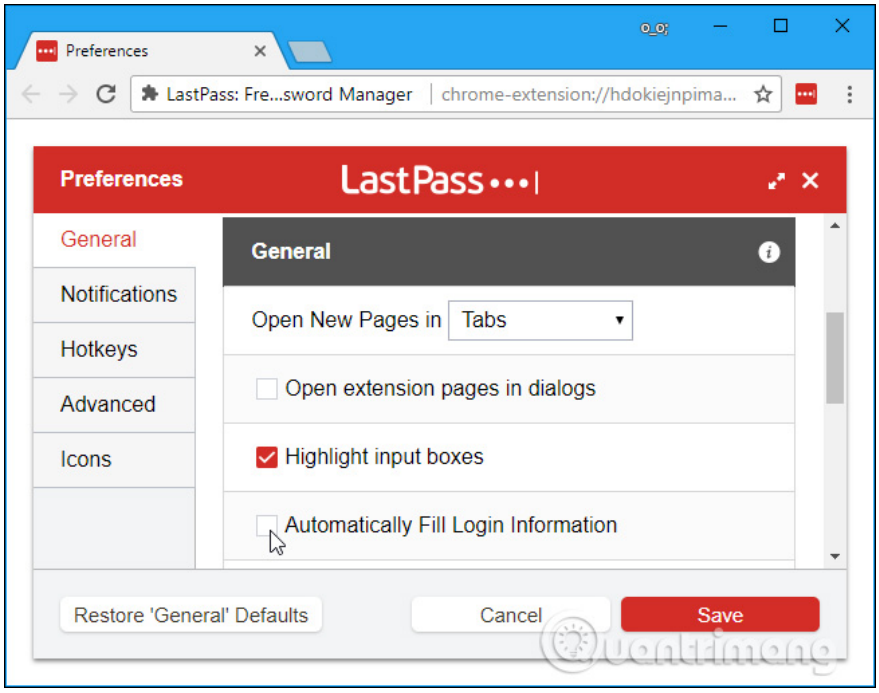


You can also choose to just copy and paste the username and password from the password manager. This operation will be safer but not convenient.

Unfortunately, most browser password managers do not allow users to disable autofill. There is no way to disable autofill if you're using the integrated password manager in Google Chrome or Microsoft Edge. Chrome has the option to disable autofill, but it only disables auto-fill data such as addresses and phone numbers, but not passwords. There is an option to disable auto-fill passwords in Mozilla Firefox's password manager, but it's hidden in about: config .

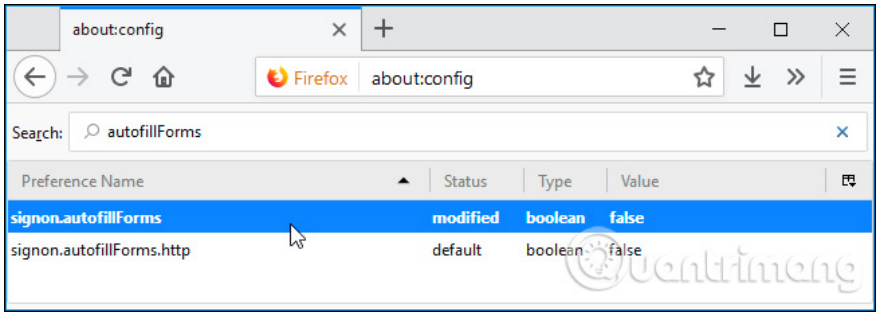
If you're using Chrome or Edge's built-in password manager, you should switch to a third-party password manager to get more control, like LastPass or 1Password. 1Password manager is not affected by this problem because it is not available_ autofill feature.

In LastPass, you can disable the auto-fill feature by clicking the LastPass extension button on the browser toolbar and clicking " **Preferences** ", unchecking the " **Automatically Fill Login Information** " option in the **General** section and then Click " **Save** " to save the changes.



If you want to continue using Firefox's password manager, type " **about: config** " into Firefox's address bar and press **Enter** . You will see a warning screen informing you that changing the various settings here may cause problems. Don't worry, just follow the instructions below and you won't encounter any problems, click " **I accept the risk!** " To continue.

Enter " **autofillForms** " into the search box and double-click the " **signon.autofillForms** " option to convert it to " **false** ". Firefox will not automatically enter your username and password without your permission.



If you are using another password manager, you should open the option and disable the " **autofill** " or " **automatically fill** " option to make sure that the password manager won't leak your personal information. half.

Developers of browser password managers and password manager utilities need to reconsider how to manage passwords to help users feel more secure. However, now you can turn off the autofill feature to reduce the risk of password theft.

See more:

1. Instructions to turn off the proposal to save passwords on the Web browser
2. Customize Firefox to automatically save passwords when logging in
3. How to view saved passwords on Chrome browser?

You finished reading the article "**Why should you turn off the Autofill feature in the password manager?**" 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.