9 Windows Privacy Settings You Should Change Right Now

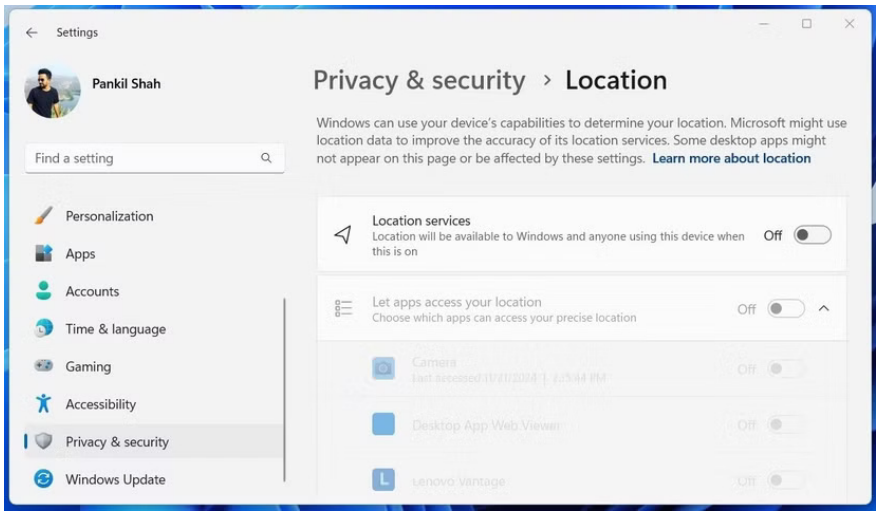
Windows computers collect all sorts of data about you. While this is meant to improve your experience, it can also raise privacy concerns.

Windows computers collect all sorts of data about you. While this is meant to enhance your experience, it can also raise privacy concerns. That's why it's important to take control of your data and protect your privacy by adjusting the following key Windows settings:

1. Turn off location services

Apps on your Windows 10 or 11 PC can track your location. While this can be useful for certain purposes, such as maps or weather apps, other apps can also access this information to track you.

If you're not comfortable sharing your location, you can easily turn off location services on Windows. To do this, open the **Settings** app and go to **Privacy & security > App permissions > Location . Then, turn off the Location services** toggle . Alternatively, you can leave this toggle on and allow or block location access for specific apps as needed.

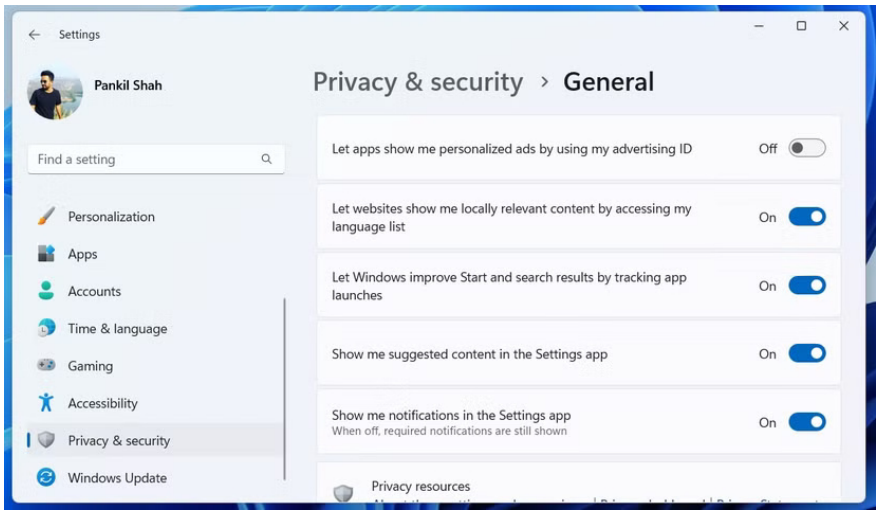


2. Turn off ad tracking

Windows assigns each user an Advertiser ID—a unique code that tracks a person's online activities. Microsoft then uses this data to show personalized ads across apps and services. If you don't want to see these ads and want to protect your privacy, you can easily turn off ad tracking in Windows.

To do that, all you have to do is go to **Settings > Privacy & security > Windows permissions > General** and turn off the **Let apps show me personalized ads by using my advertising ID** toggle .

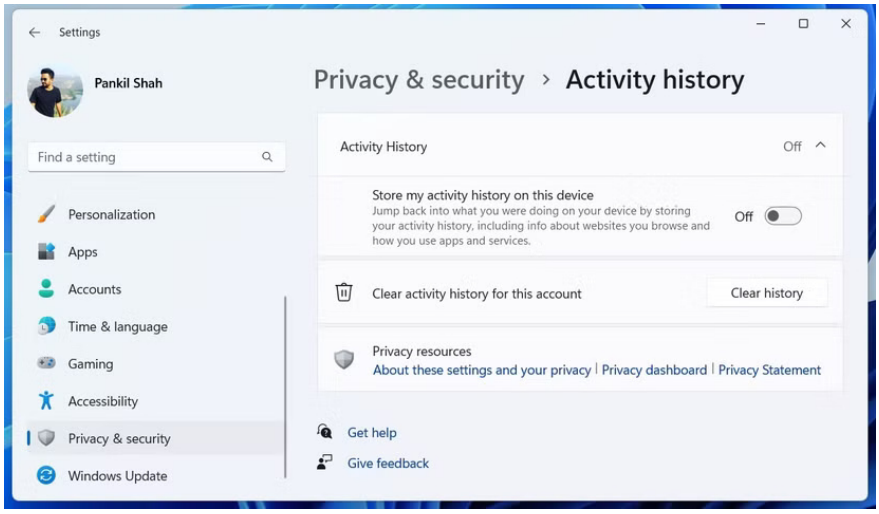
Turning off ad tracking is a simple and effective way to take back control of your personal data and limit how much Microsoft knows about your online habits. While you'll still see ads, they won't be as personalized.



3. Turn off Activity History

Windows' Activity History feature keeps track of your actions, such as the apps you've used, the files you've opened, and the websites you've visited. If you don't like the idea of ??recording your activities, you can turn this feature off.

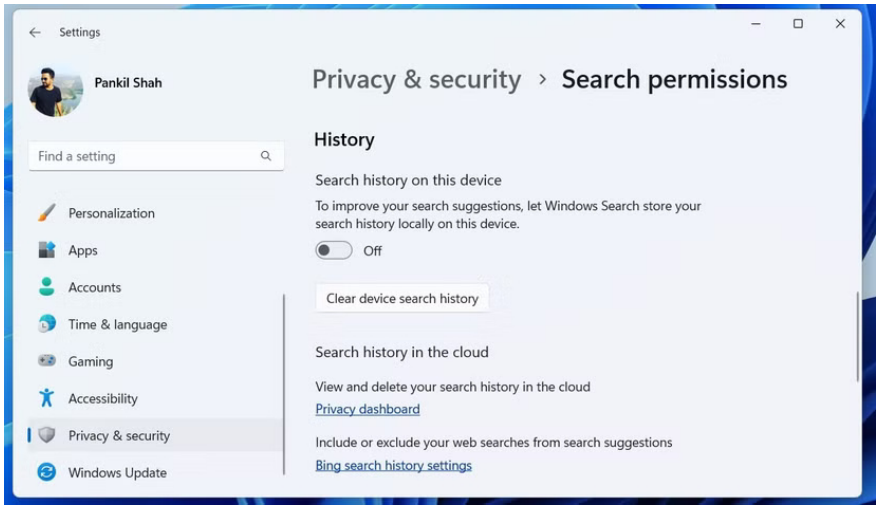
To do this, go to the **Privacy & security** menu in the Settings app and click **Activity History** . You can then turn off **the Store my activity history on this device** toggle to disable the feature. Alternatively, you can use the **Clear history** button to delete existing data collected by Windows.



4. Turn off Cloud Content Search and search history

By default, Windows search not only searches your local files, but also pulls content from the web, including OneDrive, Outlook, and other Microsoft services you use. On top of that, Windows keeps a record of all your search queries, all with the aim of improving your search experience.

Fortunately, you can prevent Windows from pulling results from the cloud and storing your search history. To do this, go to **Privacy & security > Search permissions** and turn off the toggles under **Cloud Content Search** and **History** . Then, click the **Clear device search history** button to delete your existing search data.

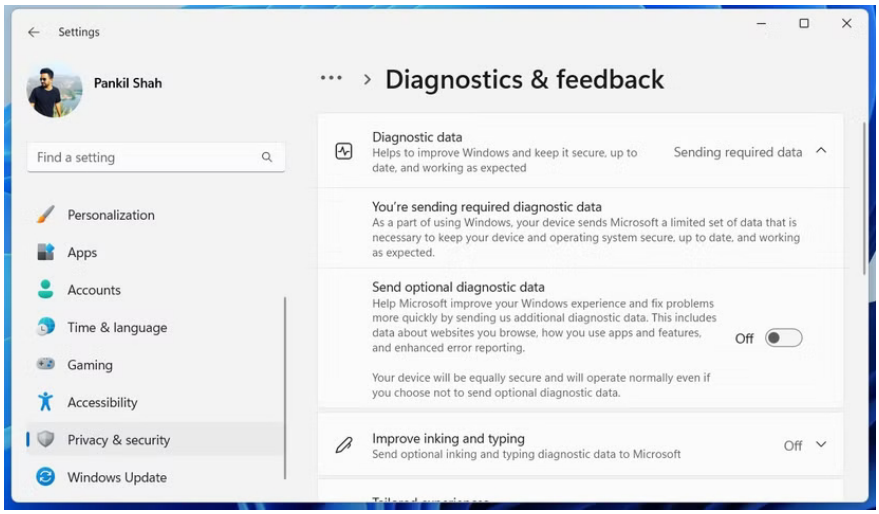


5. Prevent Windows from sending diagnostic data

To help ensure Windows runs smoothly and provides a bug-free experience, Microsoft collects all sorts of diagnostic data from your computer. This data can include details about how you use apps, how you interact with features, and errors you encounter. While this helps Microsoft improve its operating system, it can be annoying if you prioritize privacy.

While you can't stop Windows from collecting and sending all data, you can opt out of sharing optional diagnostic data with Microsoft by adjusting your settings. To do so, go to **Settings > Privacy & security > Diagnostics & Feedback > Diagnostic Data and turn off the Send optional diagnostic data** toggle .

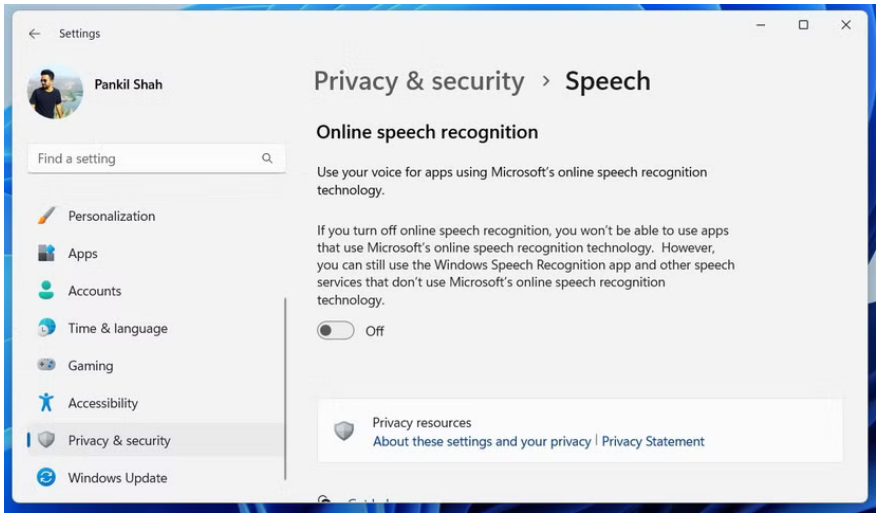
As mentioned in the Settings app, turning this option off won't affect your device's performance or security - Windows will continue to run normally.



6. Turn off Online Speech Recognition

Some apps on your PC rely on Microsoft's Online Speech Recognition technology to process voice commands and transcribe speech. However, if you don't use apps that require speech recognition, turning this feature off can give you peace of mind, ensuring that your voice data isn't being collected without your knowledge.

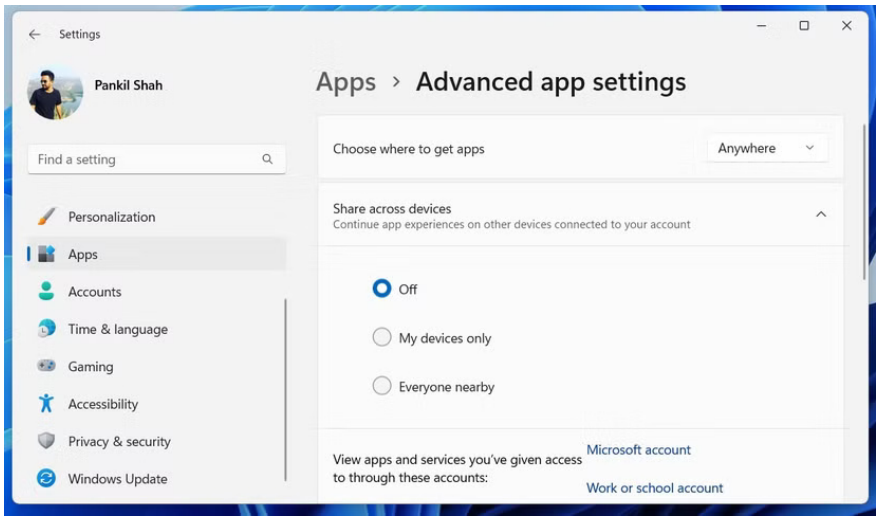
To do this, just go to **Settings > Privacy & security > Speech and turn off the Online speech recognition** toggle . Note that turning this setting off won't affect your ability to use voice typing on Windows.



7. Turn off experience sharing feature

One of the benefits of using a Microsoft account on your Windows PC is that you can sync your activities across all your devices using the same account. However, this can also put your privacy at risk by making your data more accessible across platforms.

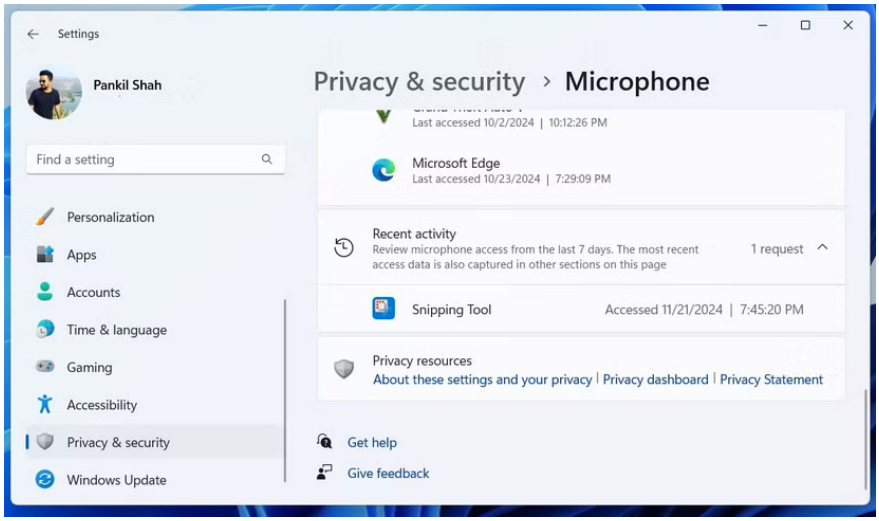
If you don't want this, you can turn off shared experiences on Windows. To do this, go to **Settings > Apps > Advanced app settings > Share across devices** and select the **Off** button .



8. Review which apps have access to your camera and microphone

Cameras and microphones are among the most sensitive devices on your PC because they can capture private moments or conversations. Since many apps require access to these features for legitimate purposes — such as video calls, voice recordings, or online meetings — completely disabling camera and microphone access may not always be possible.

To resolve this issue, it is important to review which applications have access to your camera and microphone on Windows. This will allow you to identify any suspicious applications or programs that may be invading your privacy and take the necessary steps to disable their access or remove them completely.



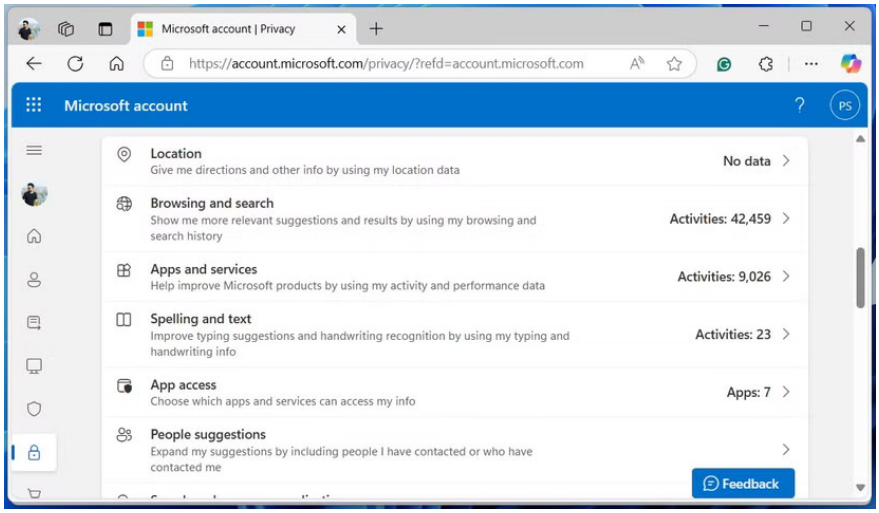
9. Use Microsoft Privacy Dashboard

Adjusting the privacy settings mentioned above in Windows will help protect your personal information in the future, but if you're concerned about the data Microsoft has collected, you can use the Microsoft Privacy Dashboard. This is a centralized tool that lets you view, manage, and delete the data associated with your Microsoft account across devices and services.

Here's how you can access and use the Microsoft Privacy Dashboard:

1. Open your favorite web browser and .
2. Click the **Sign in** button and sign in with your Microsoft account.
3. Go to the **Privacy** section and click the **Privacy Dashboard button.**

In the Microsoft Privacy Dashboard, you will find many options such as location activity, browsing history, search history, etc. You can go through each category to review and delete the data collected. Regularly managing your data through the Microsoft Privacy Dashboard is a great way to take an active role in protecting your privacy.



By taking the time to adjust these privacy settings on your Windows PC, you can significantly reduce the amount of personal data that is collected and shared without you realizing it. Whether it's turning off location services, disabling ad tracking, or reviewing app permissions, every step makes a difference and protects your information from unwanted disclosure.

So what are you waiting for? Update your privacy settings today!