Microsoft Edge privacy settings to change right away

Microsoft's brand-new Edge browser lets you control how much data you share when browsing.

- 1

Illustration by Stephen Shankland/CNET

Microsoft's new Edge browser may share the same underpinnings as the popular Chrome web browser, but it takes a much more active role in minding your privacy than Google's browser does. Microsoft's Chromium-based browser for Windows 10 ($130 at Amazon) and MacOS gives you control over how you are tracked across the web and what browsing data Edge keeps. And it comes with an antiphishing and anti-malware tool called Microsoft Defender SmartScreen that monitors the websites you visit for fishy behavior.

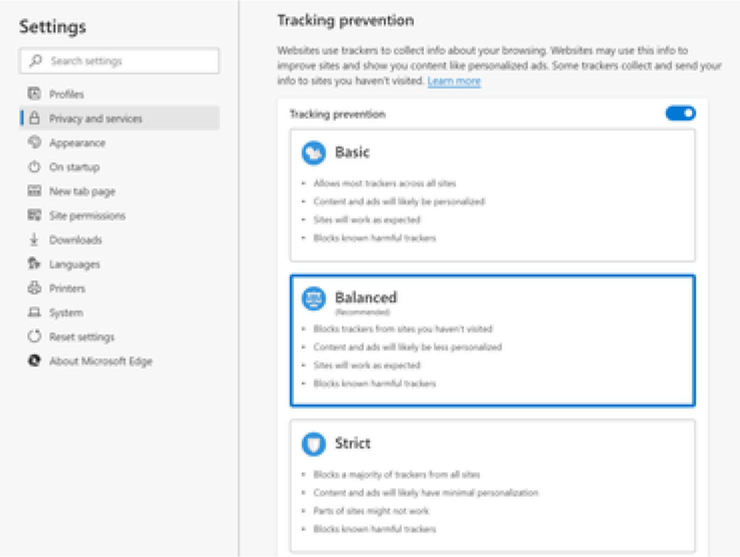
With the goal of minding your personal information, Microsoft Edge joins the Brave and Firefox browsers in protecting you from trackers that gather your browsing history, cryptominers that use your device's resources to mine cryptocurrency and fingerprinters that uniquely identify you based on your device. Meanwhile, Google Chrome's privacy tools are limited, although Google said it intended to beef up the browser's privacy-protection tools soon.

Here's how to use Edge's privacy tools to guard your browsing data.

Now playing: Windows 10: Features to try now
1:53

How to use Microsoft Edge tracking prevention settings

Like Brave and Firefox, the new Edge browser lets you tune your browser privacy settings to block trackers that monitor and collect your activity as you visit sites across the web. Here's how to manage Edge's privacy settings.



Tracking prevention

Websites use trackers to collect info about your browsing. Websites may use this info to improve sites and show you content like personalized ads. Some trackers collect and send your info to sites you haven't visited. Learn more

Tracking prevention

Basic

- Allows most trackers across all sites
- Content and ads will likely be personalized
- Sites will work as expected
- Blocks known harmful trackers

Balanced
(Recommended)

- Blocks trackers from sites you haven't visited
- Content and ads will likely be less personalized
- Sites will work as expected
- Blocks known harmful trackers

Strict

- Blocks a majority of trackers from all sites
- Content and ads will likely have minimal personalization
- Parts of sites might not work
- Blocks known harmful trackers

Edge lets you control your level of tracking protection.
Screenshot by Clifford Colby/CNET

1. Tap the three-dot menu in the top right, and select Settings.

2. Now, on the left, tap **Privacy and services**.

Edge gives you three tracking-prevention tiers to help you find a balance between how much you are tracked and the website functionality you may lose by blocking tracking.

3. Choose Edge's **Basic** prevention to allow most trackers but block the most harmful ones -- those used for cryptomining and those used for fingerprinting, which collect your browser and computer settings to create a unique profile of you. Select **Balanced** to block trackers from sites you haven't visited, as well as harmful trackers. And pick **Strict** to block most trackers from all sites. As you crank you the prevention, some sites may not work as you'd expect.

By default, Edge uses the **Balanced** setting.

How to clear Edge's browsing data

Edge also lets you clear your browsing history, either manually or automatically every time you close your browser.

1. In Edge's Privacy and services settings window, scroll down to the Clear browsing data section.

2. Tap the **Choose What to Clear** button to immediately clear out your browsing and download history, cookies and cached files. Tap the arrow to the right of Choose what to clear every time you close the browser to select which data you want Edge to wipe out each time you close the window.

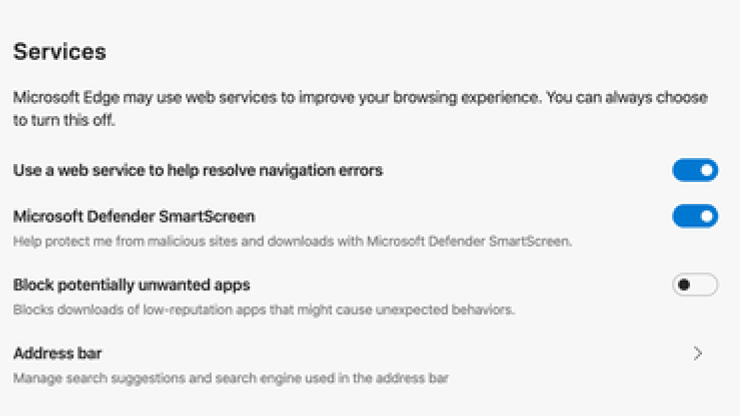
MORE ON BROWSERS

- **With Firefox, stop leaking your data across the internet**
- **If you care about privacy, this is the browser to use**
- **Chrome is not minding your privacy. Here's how to help it**

How to use Edge's other privacy and security tools

In the **Privacy and Services** sections of the Privacy and Services setting window, you can turn on and off other Edge tools that mind your data.

In the Privacy section, you turn on Send "Do Not Track" requests to ask websites to not track you. Unhelpfully, websites can use that request to build your online profile, and Apple has removed the Do Not Track request from Safari because of that. By default, Edge has this turned off.



Services

Microsoft Edge may use web services to improve your browsing experience. You can always choose to turn this off.

Use a web service to help resolve navigation errors ●

Microsoft Defender SmartScreen ●
Help protect me from malicious sites and downloads with Microsoft Defender SmartScreen.

Block potentially unwanted apps ○
Blocks downloads of low-reputation apps that might cause unexpected behaviors.

Address bar >
Manage search suggestions and search engine used in the address bar

Edge can steer you away from shady sites and apps.
Screenshot by Clifford Colby/CNET

In the Services section, you can use the Microsoft Defender SmartScreen tool to steer you away from shady sites. The tool checks the site you want to visit against a dynamic list of reported phishing, malware, exploit and scam sites to warn you of fraudulent websites.

Still in the Services section, you can have Edge block shady software by toggling on **Block potentially unwanted apps**.

For more, here's how to add extensions to the new Edge browser and how to download Windows 10 for free.