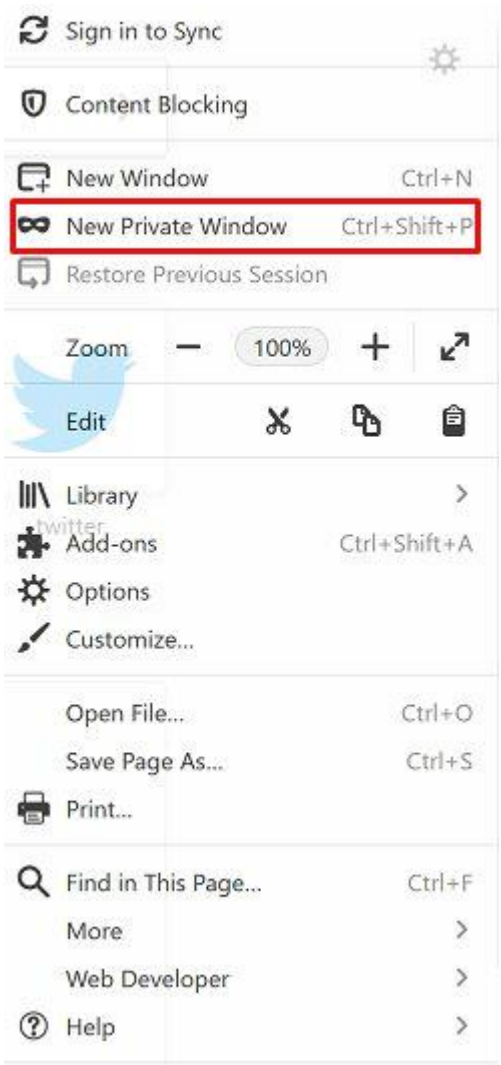
Managing Privacy Settings in Mozilla Firefox

As with all other modern web browsers, Mozilla Firefox offers several features that help sending your data via the World Wide Web. By default, Firefox connects to Mozilla, Google and Yahoo servers. It is not recommended disabling this function, as it is very useful. This article will explain what other options you have to make an informed decision.

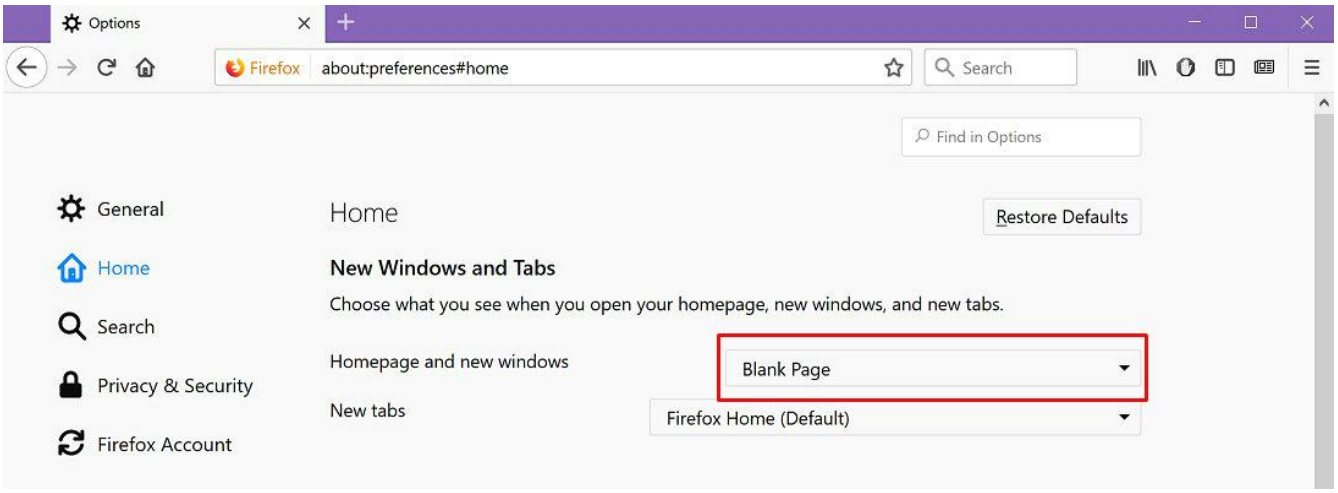
If you simply wish to visit websites without leaving a “track” on sever or your own computer, you can open the new window in private mode by going to **Menu > New Private Window**.



Hiding recommended websites

Whenever you open a new tab in Firefox, it will show you a page with various website icons and links and display your **Top Websites** – those you frequently visit.

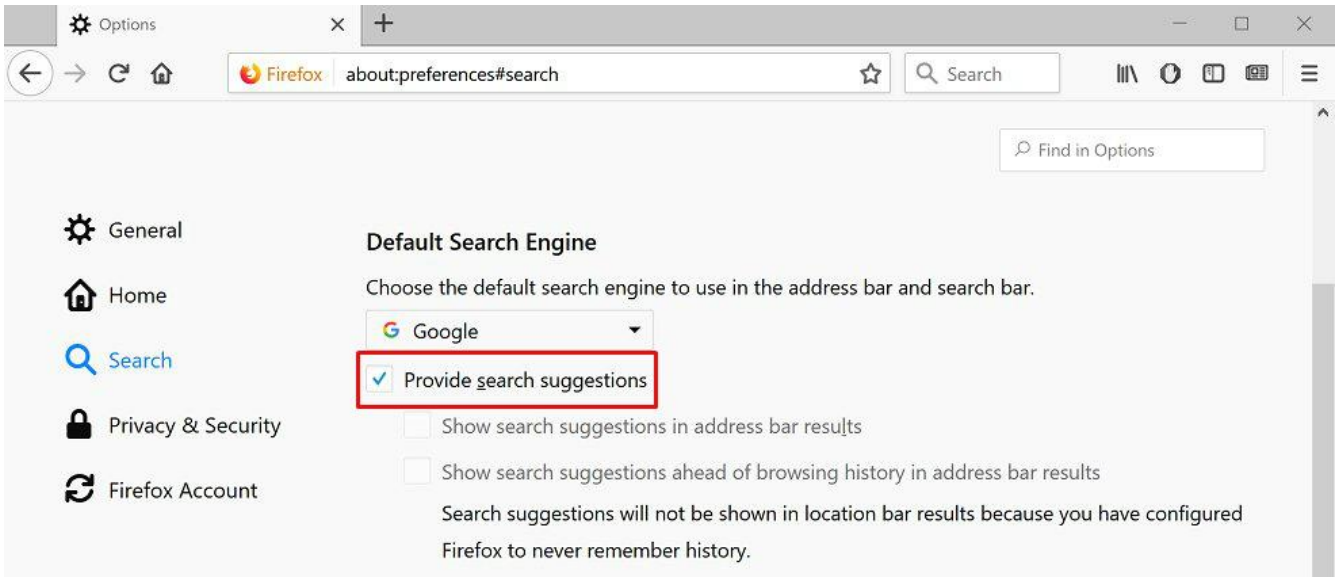
To prevent Firefox from loading and displaying the suggested websites' icons, click the **Gear icon** in the upper right corner of the new window and select **Blank Page** in the **Home Page and New Windows** section.



Adjusting search options

Several options are available in the **Search** section. Go to **Menu > Search**.

When you start typing a search query in the Firefox search box, browser immediately sends your keystrokes to Google search engine (default). Google, in turn, predicts what you want to find. If you do not want to see these suggestions, go to **Search** category on the **Firefox options** page and uncheck the following box **Provide search suggestions**. In this case, Firefox will not send search queries to the default search engine (until you press the **Ente**r button).

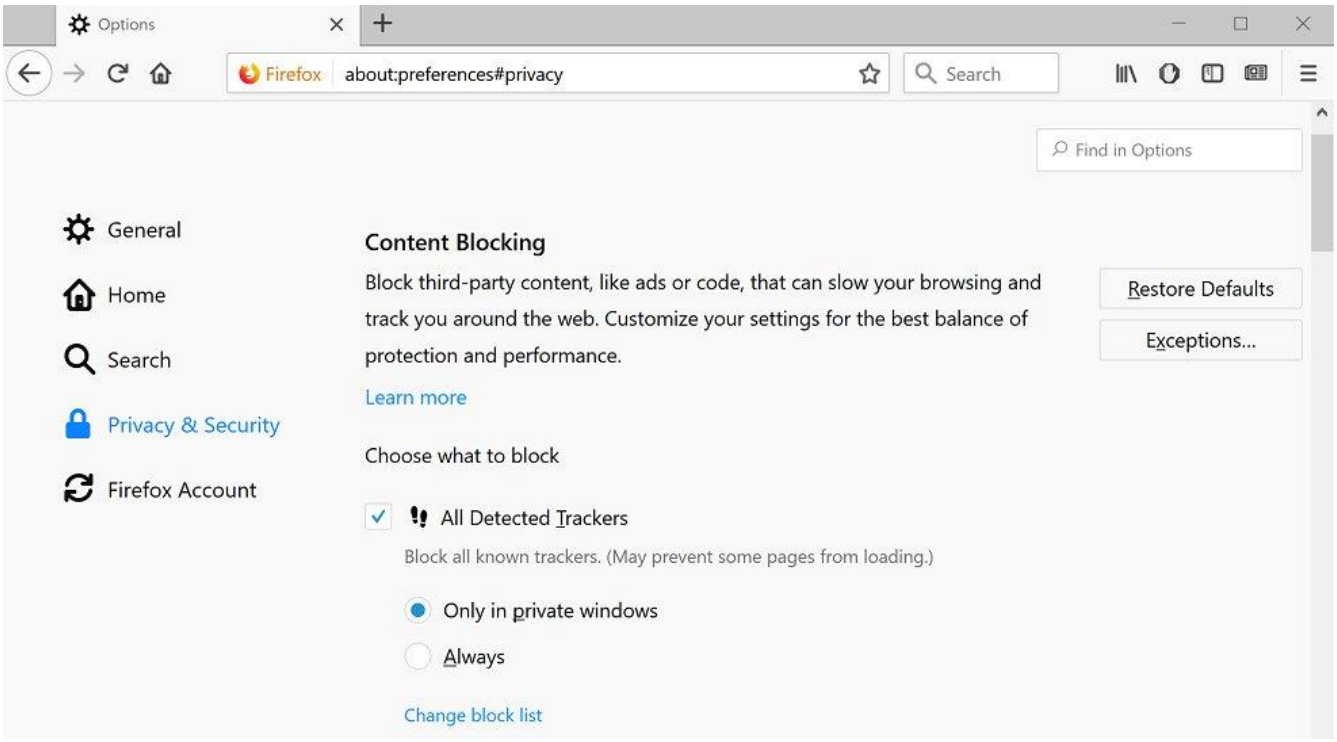


If you enable the option called **Show search suggestions in address bar results**, you will also see prompts already in the address bar.

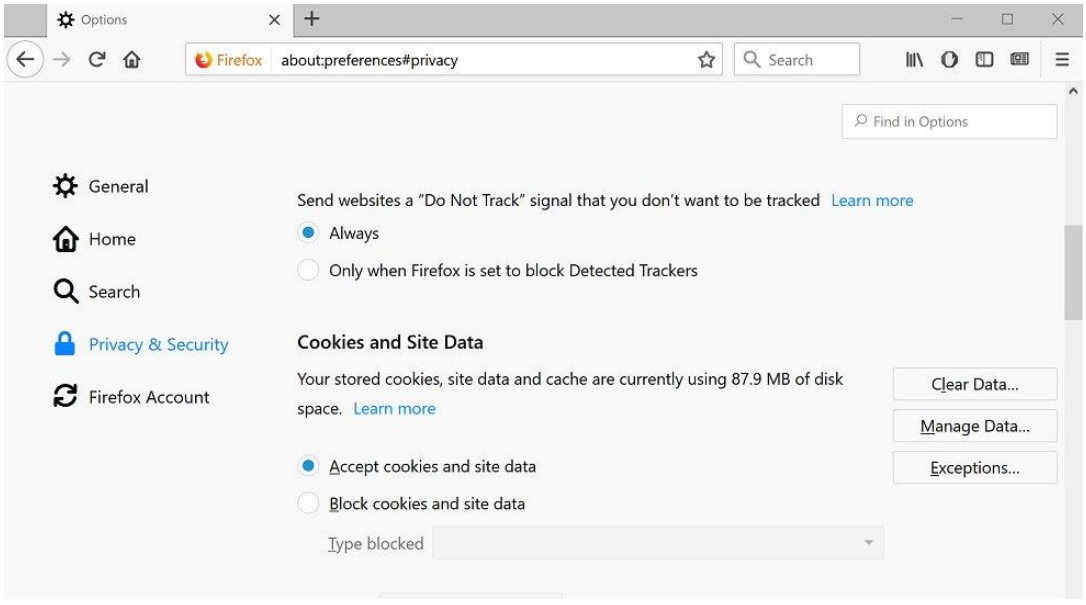
Configuring privacy settings

Corresponding settings are located in the **Privacy and Security** section of the main **Firefox Settings** screen. Here you can:

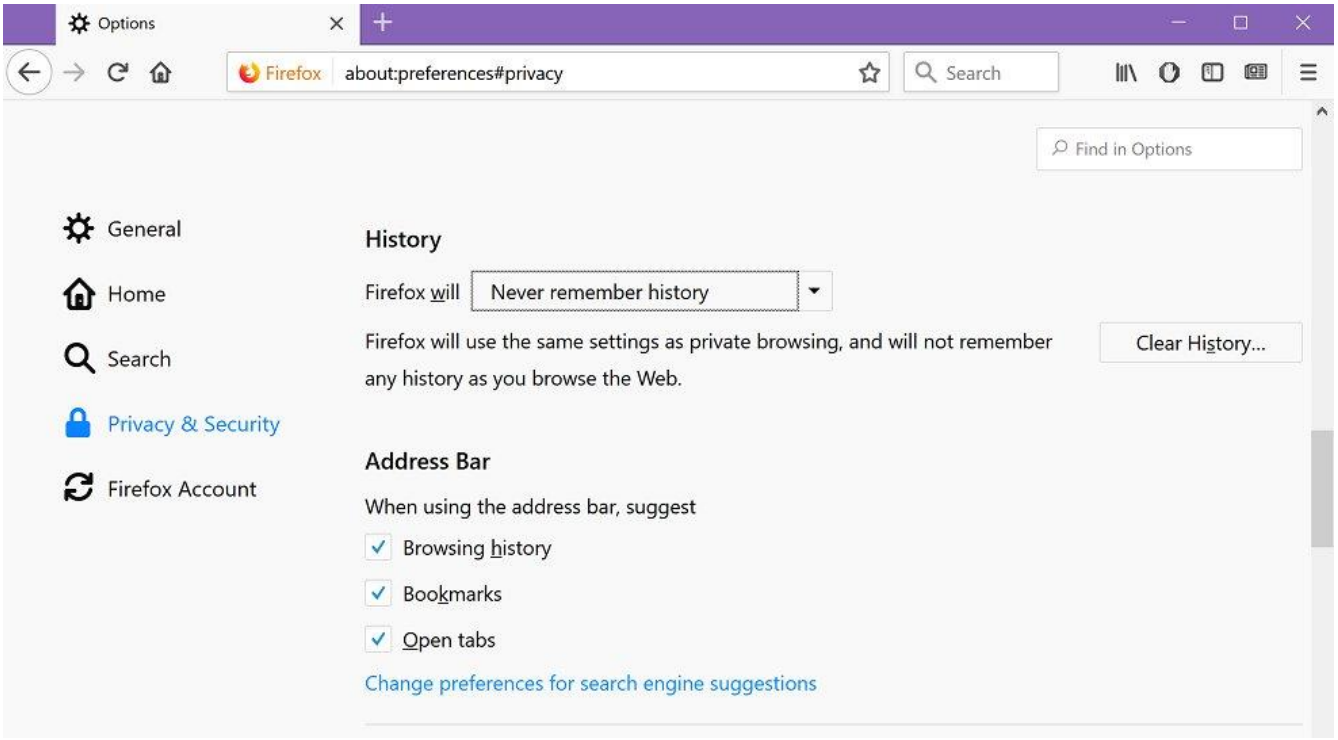
- **Use tracking protection to block known trackers.** Firefox automatically includes a tracking protection that blocks all known web trackers. By default, it is enabled for new private windows. You can click **Change block list** and select even more aggressive way of protection.



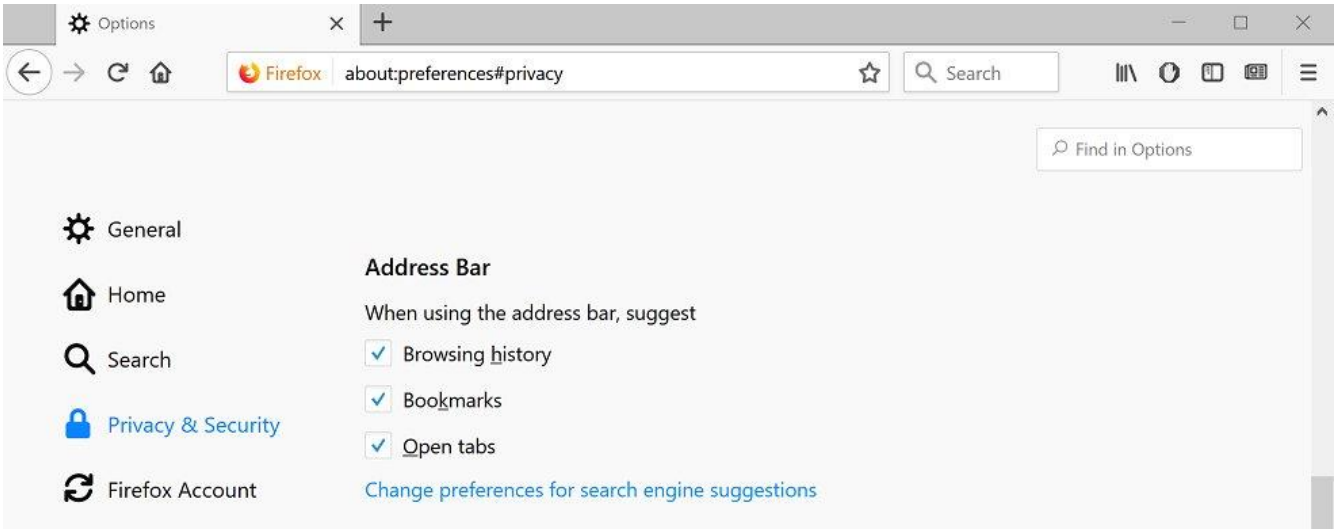
- **Send a Do Not Track request to websites**. Firefox automatically sends a **Do Not Track** request. You can adjust this option to send a **Do Not Track** request to all websites you visit. However, this is just a web browser request, and many websites ignore it.



- **Managing History**. Firefox may keep your history and also allow websites to set cookies. You may set Firefox to **Never remember history**. You can also select **Use custom settings for history** and configure advanced settings here. For example, you can tell Firefox to clear history when you close the browser.

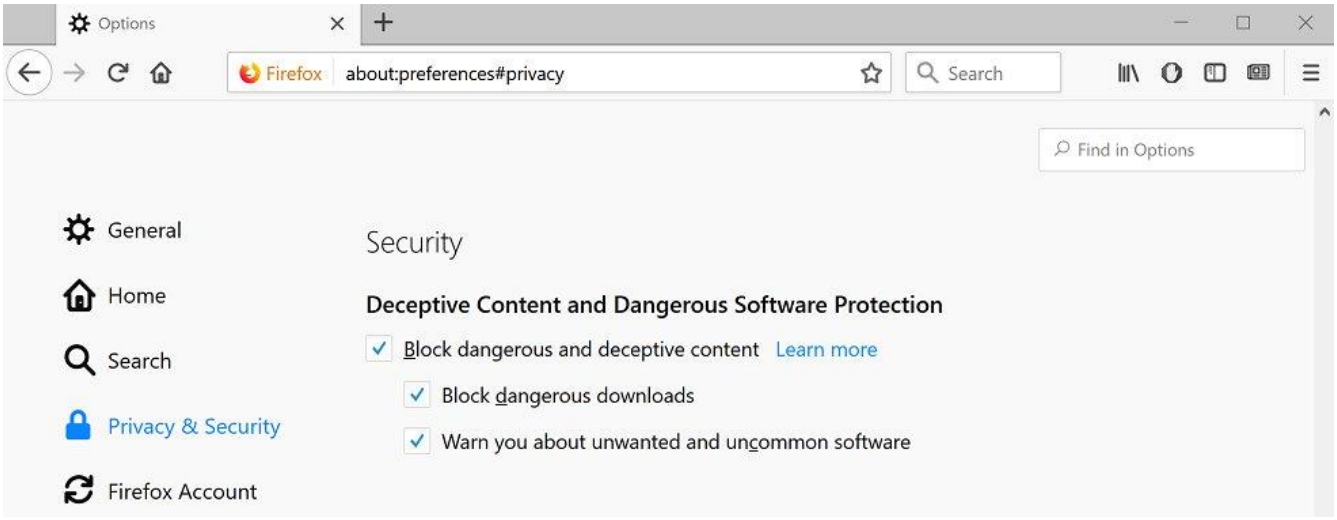


- **Address Bar.** Firefox will try suggesting websites based on you browsing history, bookmarks. Unfortunately, it can also show websites that you might not want other people near you to see.



Firefox Security Controls

The **Security** section of the Firefox web browser uses Google safe browsing services.



Block dangerous and deceptive content. Firefox downloads and updates a list of dangerous webpages from Google every 30 minutes. When you visit any website, Firefox compares the page address with the Google Safe Browsing list and blocks it if it matches a harmful site.

Block dangerous downloads. While downloading files from the Internet, Firefox may block the file if its address appears in the list of dangerous websites. Firefox will also send information about the file to Google Safe Browsing to check if it contains malicious software. For Windows users, Firefox only sends app data to Google if it doesn't belong to a trusted publisher. Files will not be sent if you downloaded them from a trusted source like Google or Microsoft.

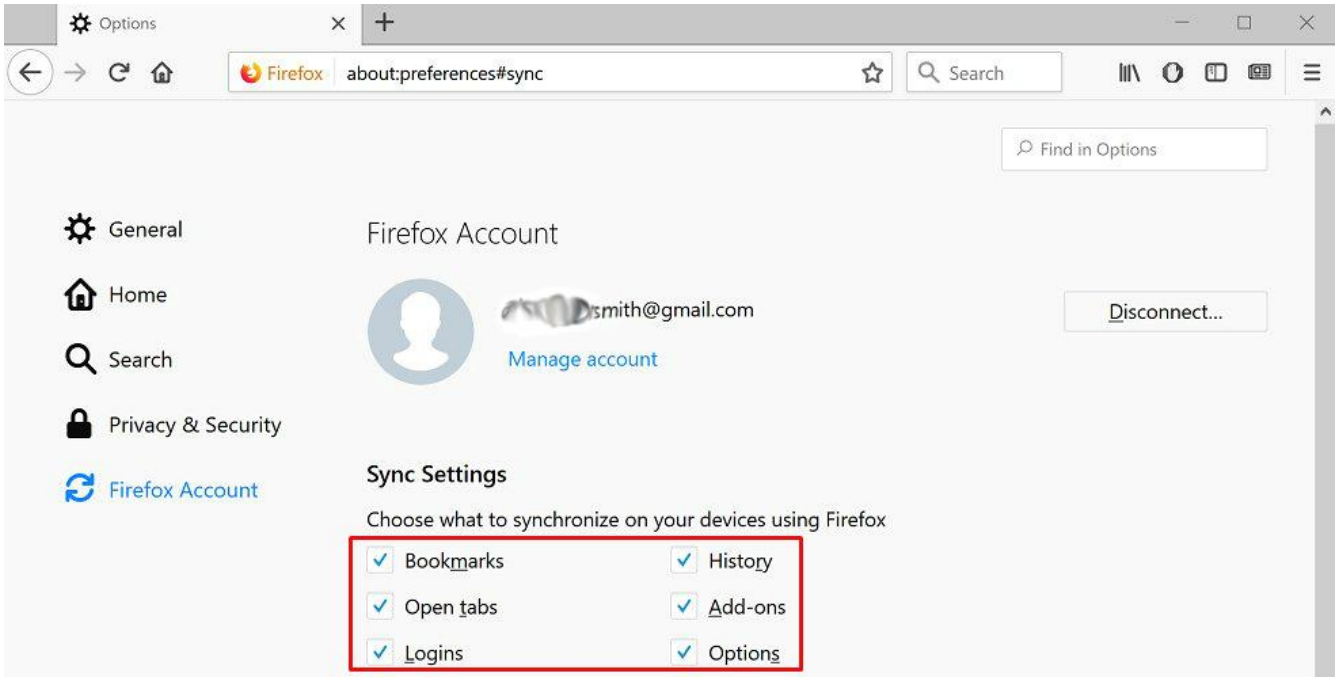
Warn about unwanted and uncommon software. Firefox will warn you before downloading software containing a PUP - potentially unwanted program. These are not viruses but things like adware.

It is recommended to leave all the above options enabled. They will protect you from phishing, hacked sites, and malicious or unwanted programs that may harm you.

Data synchronization

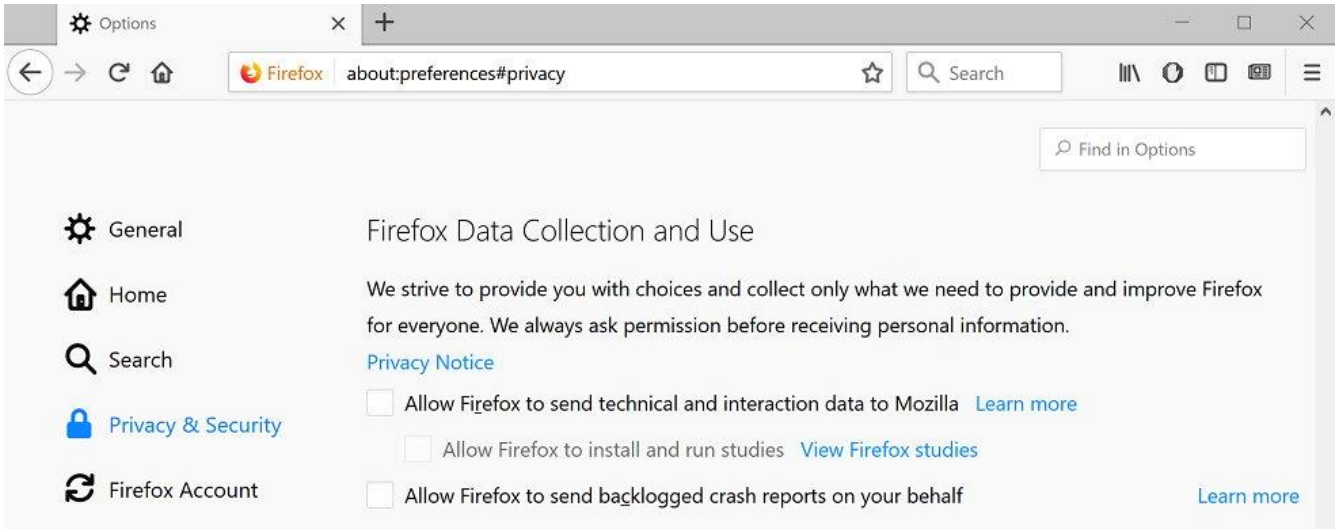
If you sign in into your Firefox account it will synchronize your tabs, history, bookmarks, add-ons, passwords, and connection settings across all devices. This data will be stored on Mozilla server and you can access it on any device. It helps to quickly get your browser data to a new computer by simply logging in with the Firefox account.

To control synchronization, go to **Firefox Account** section and select your options.



Firefox data collection and use

These options are available in the **Privacy and Security** section. You can choose what information Firefox browser will share with Mozilla servers.



Allow Firefox to send technical data and interaction data to Mozilla Firefox constantly monitors the status of your browser, including such information on how long it takes to launch the browser and what kind of crashes occur. You can view it yourself by clicking **Menu > Help > Troubleshooting Information**.

Allow Firefox to install and run studies. If you enable this option, Firefox will share additional information with Mozilla, including details on how Firefox works, what additional features and settings you use, what hardware and software is there on your computer. Mozilla will use this data to improve its browser performance.

Allow Firefox to send backlogged crash reports on your behalf. This option is also disabled by default. If you activate it, Firefox will send crash reports to Mozilla. These reports include information that Mozilla will use to diagnose problems and fix them.

If you go to **General > Firefox Updates** you can choose whether Firefox will automatically install the updates. It is strongly recommended leaving this option enabled. If you do not do this, you will not receive critical security updates, and malicious programs or websites you visit may attack your computer.

Source: Bestvpnrating.com