Privacy practices on Google Chrome

On Google and Chrome, security issues are quite confusing. If you are worried about this issue, you may find that they have almost no privacy, often tracking web browsing, collecting personal data and using it all for advertising purposes.

On Google and Chrome, security issues are quite confusing. If you are worried about this, you may find that they have almost no privacy, often tracking web browsing, collecting personal data and using it all for advertising purposes (annoying). HA for some people).

If using Gmail, Drive, Google +, . of the Google system, then surely you will have many personal data scanned by Google's algorithms. But at least with a few options, you can protect yourself when using Chrome.

Essential security settings for Google Chrome

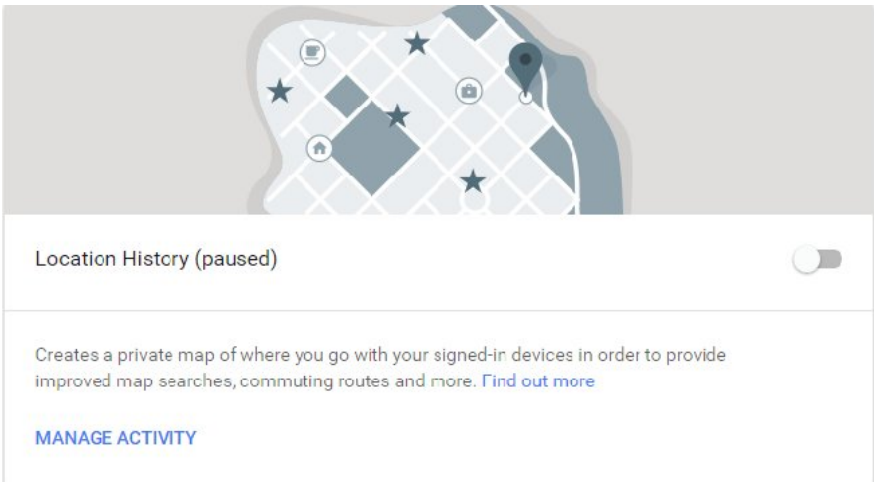
1. 1. Disable location history
2. 2. Change your search engine to not be tracked
3. 3. Limit cookies
4. 4. Use Google security check feature
5. 5. Activate "Do No Track" and "Safe Browsing"
6. 6. Limit the synchronization
7. 7. Encrypted data synchronization
8. 8. Turn off web services
9. 9. Use the Ask before access feature
10. 10. Turn off Google Activity Control
11. 11. Periodically "clean up" extensions
12. 12. Install security enhancements
13. 13. Disable the 'Privacy and Security' settings
14. 14. Do not save addresses and payment methods

1. Disable location history

Location history is notoriously bad. Most people don't know that this feature tracks your movement anywhere, allowing you to keep track of where you are logged into your Google account at any time of the day (or in other words this is can know who has accessed your account).

To turn off this feature, go to the account page by clicking on the avatar on the top left of Google, Gmail, or other Google services, then click **My Account** . Next, click **Personal info & privacy** > **My Activity** > **Activity Controls** , and scroll down to **Location History** page (click **Manage Activity** here to see how the service has

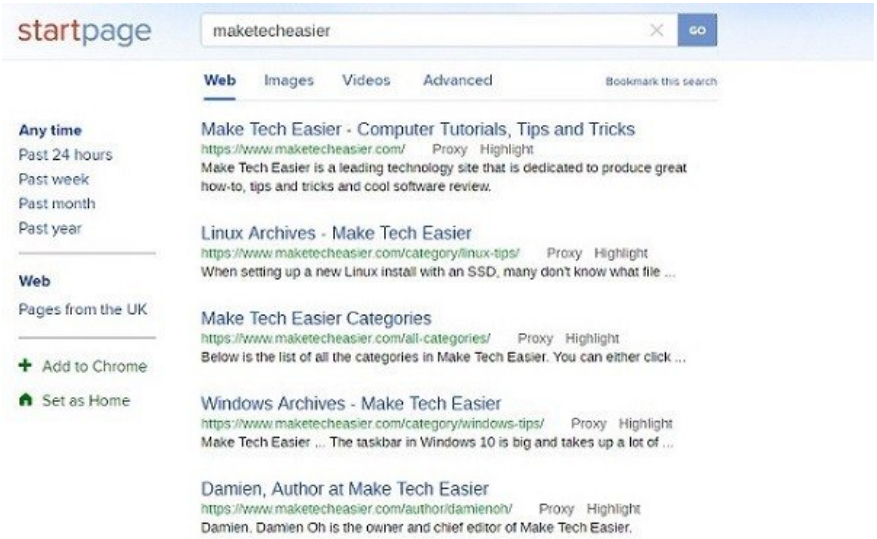
tracked you. Finally, select the **Location** color slider **History** to turn it off.



2. Change your search engine to not be tracked

This is really an easy way to do it, but it must give up the habit of using Google to search. Therefore, get out of that routine and use a more friendly search engine to use as a default alternative.

Today, DuckDuckGo is a popular and widely used tool, furthermore it does not track any of your searches, encrypt data and all personal devices. But another option worth considering is Startpage running Google search by proxy, which gets all the search results from Google without telling Google you're browsing. When looking through the search results, click on the **By Proxy** option under each site result so the site you choose will not be able to track you.



3. Limit cookies

When talking about websites and ad networks that track user behavior, frequent use of cookies is mentioned. The browser stores these files so that web pages work as expected by users. Without them, users will start from the beginning whenever accessing a website.

Cookies are very important to websites. They allow users to log in to an account or add items to a cart.

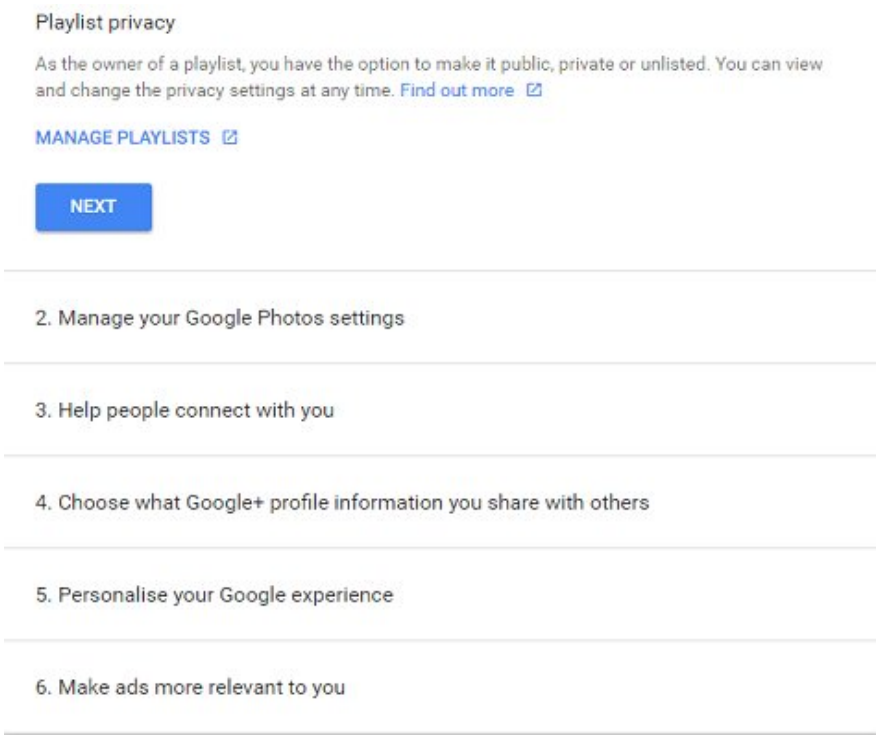
But websites can store whatever they want in these files. The same is true for ad networks. That is why it is necessary to restrict which cookies are allowed to be used on your computer.

To do this, go to **Privacy and security> Content settings> Cookies** . Please enable **Block third-party cookies** . For better security, users can only enable **Keep local data only until you quit your browser** , but this means that you will have to log back into the site the next time you open Chrome.

You can see all the saved Chrome cookies by selecting **See all cookies and site data** . Here, users can delete each cookie one by one or delete all of them.

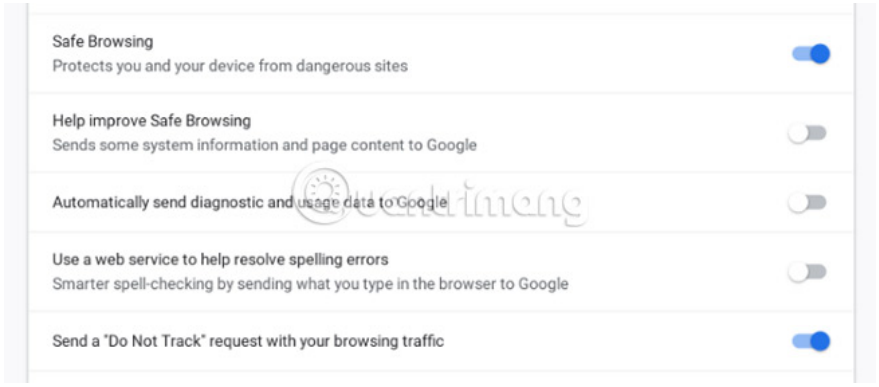
4. Use Google security check feature

Privacy Check-up is a web tool that allows you to customize sharing / security settings on other Google services such as Photos, YouTube, Google +, . This is understandable when you're on a website and This is how to ensure your activities are as secure as possible.



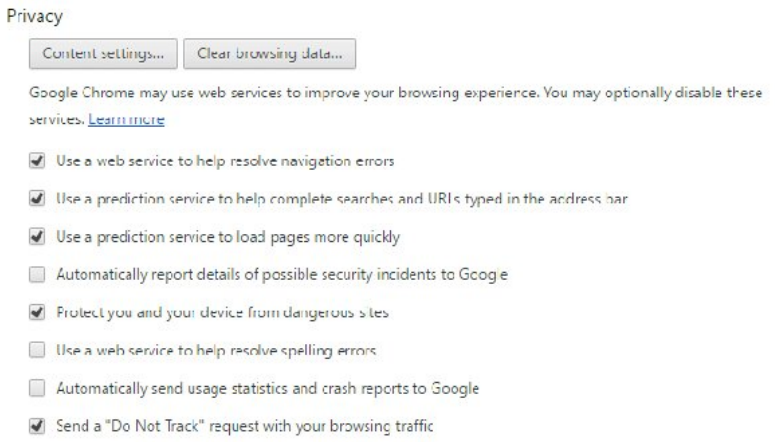
5. Activate "Do No Track" and "Safe Browsing"

In the **Privacy and security section** , there are also a few settings that users should activate. **Safe Browsing** is one of them. This feature may prevent some malicious or poorly opened websites from being opened in the browser.



People have mixed feelings about the **Do Not Track** feature because it is completely optional, although it prevents web sites from tracking your web activity. So, even if you activate it, it will work according to the decisions of the websites you visit.

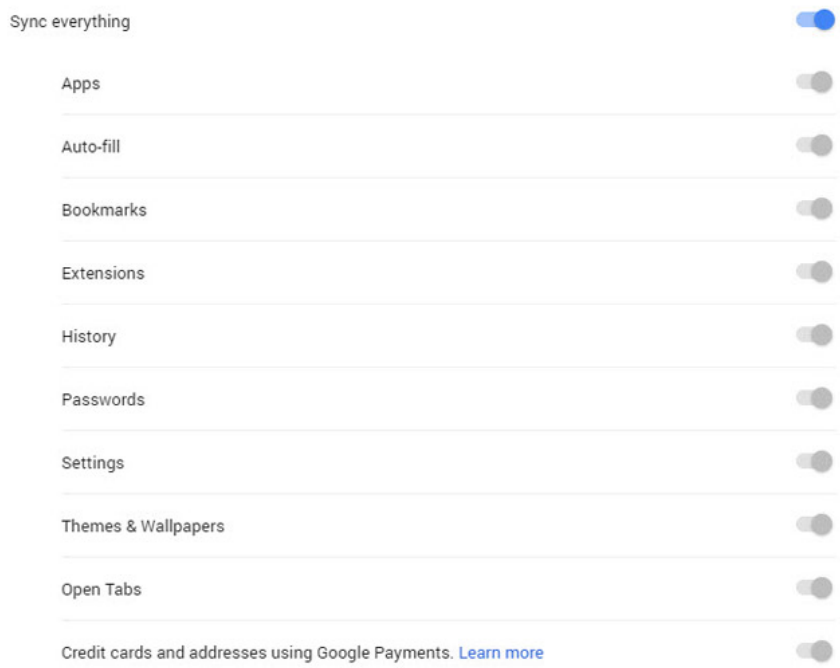
So here's how to activate: Select the **menu** icon in Chrome> **Settings** > **Show advanced settings** , then under **Privacy check** box **Send a Do Not Track request .**



6. Limit the synchronization

One of Google Chrome's strengths is that you can synchronize data (logins and passwords, bookmarks, etc.) between devices - for example, between your PC and phone. However, sending this persistent data can put your security issue at risk, so we recommend limiting synchronization.

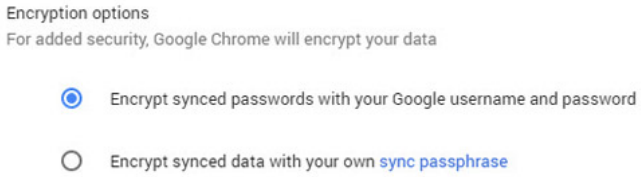
To do this, click **Settings** (three dots in the upper right of Chrome) and then click **Settings> Synchronization** .



As you can see in the example, **Synchronize everything** is set by default. We recommend deactivating the options you use frequently.

7. Encrypted data synchronization

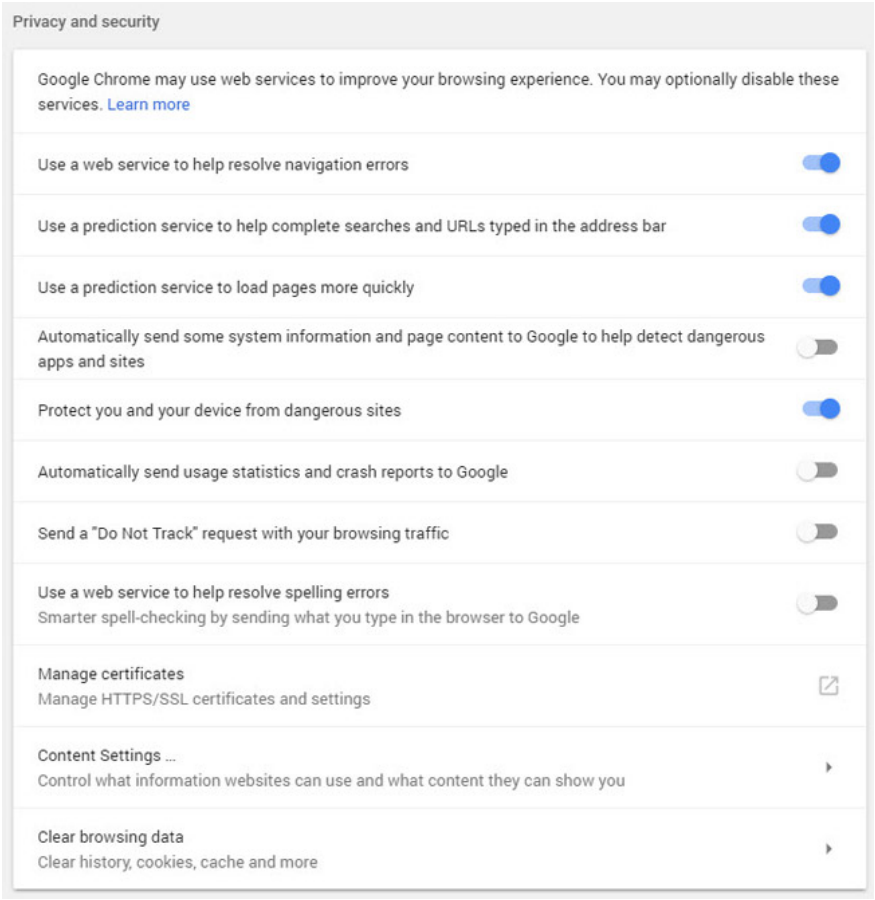
Still in the above menu, you will also find the **Encryption** option. Enable **Encrypt synced data option with your own sync passphrase** . Next, choose the password you can easily remember (but must be different from your Google account password).



You will then be asked to enter your password every time Google Chrome wants to synchronize data, ie adding an extra layer of security.

8. Turn off web services

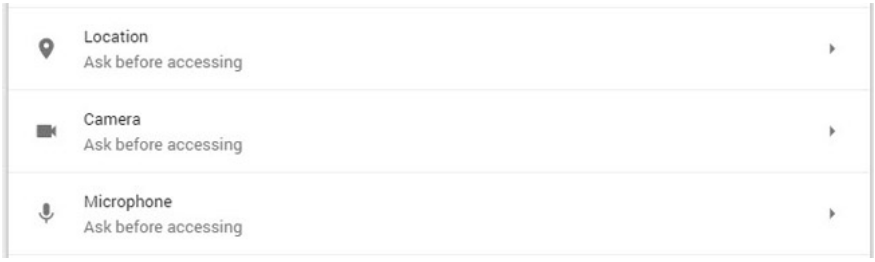
Google Chrome uses a number of external services to improve user browsing, as a spell checking service. This makes the browser constantly send information about your browsing or the text you write. Turn off these options to reduce the amount of data that is constantly being sent. Ideally, disable all and only keep the **Send a non-tracking request option with your navigation traffic** . With this option, the pages you visit will be added to the **Do Not Track** request and stop following you when you browse the web. Not all websites comply with this, but you should still activate it.



To activate or deactivate the service, go to **Settings> Configuration** and this time go to **Advanced Configuration** .

9. Use the Ask before access feature

Also in the menu **Settings> Advanced settings> Content settings** , you can take a moment to review how you set up additional utilities such as location, camera and phone. We recommend enabling the **Ask before access option** . This means that if a website needs access to your webcam, microphone or other devices, you will be notified. For example, this feature will prevent others from using the camera to track you.

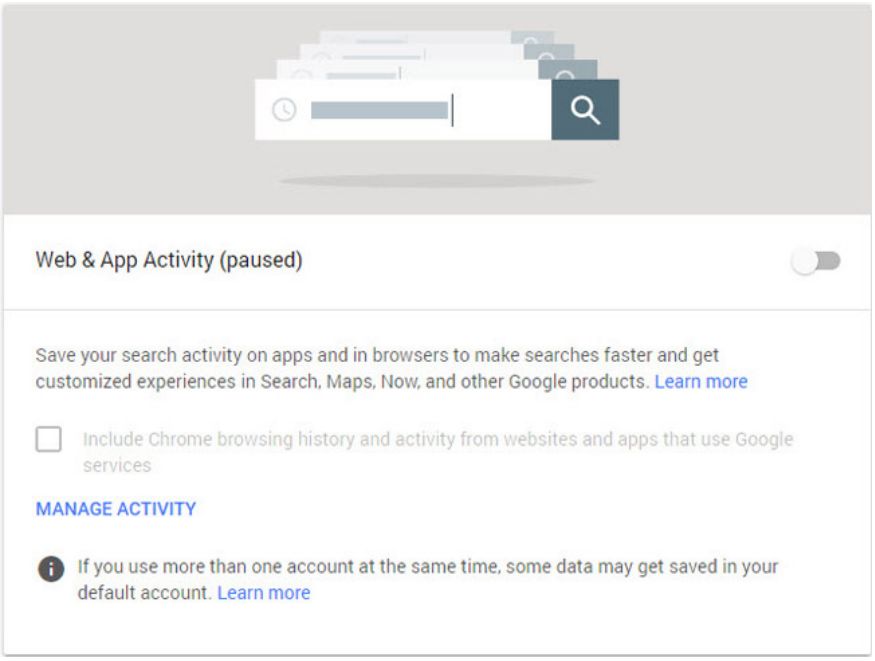


1. How to control camera access on Chrome to protect personal information

The same can be applied to additional utilities like Flash.

10. Turn off Google Activity Control

Chrome not only saves your browsing data, but so does Google. Every time you sign in to your Google account, Google will save your browsing data. This option, enabled by default, can be easily deactivated. To do this, visit the **Activity controls** option **of your account** and switch to **Deactivate** mode.

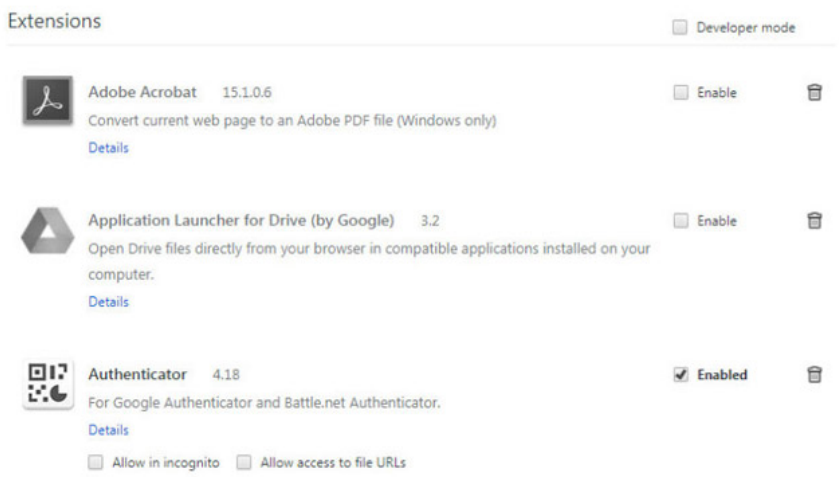


In addition, here you can configure many other aspects related to your browsing activity. If you have time, take a look at this section because it's really interesting (and you'll be surprised to know how much Google knows about you).

11. Periodically "clean up" extensions

We all love Chrome extensions, but we usually only install and use them for a few days, and then forget about them. What happens when the plugin constantly sends data to an external server? That's why we encourage you to review extensions, install them over time and 'clean' them periodically.

To do this, go to **Settings> More tools> Extensions** or directly to **chrome: // extensions /** in the navigation bar.

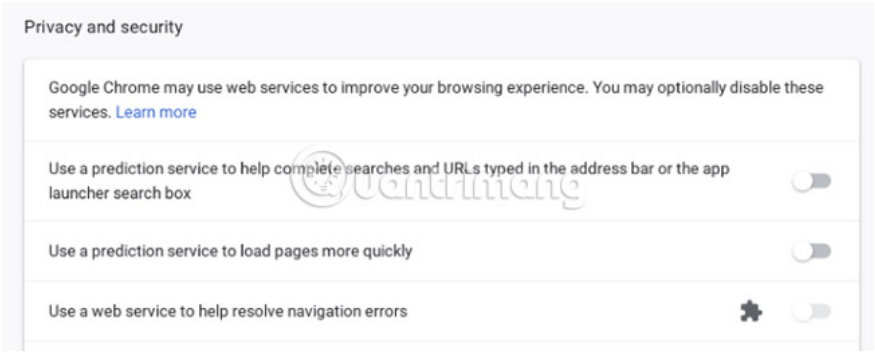


12. Install security enhancements

You have now deleted the useless extension and next is a good time to add some more practical extensions. In Google Chrome Store, there are many useful extensions to enhance security. Some suggestions below:

1. Unshorten.link analyzes links created with shortening tools, detecting real addresses before we click. Great utility to avoid malware.
2. Click & Clean has many functions, from deleting history with just one click to finding malware or even freeing up space on your hard drive.
3. HTTPS Everywhere: Pages that use HTTPS are more secure because all information is transmitted in encrypted form. This extension allows us to access HTTPS for all pages, although not by default.
4. Privacy Badger blocks third-party crawlers, intending to take our data.
5. WOT: Web of Trust helps you identify malicious or bad web sites.
6. LastPass: Free Password Manager is a useful password manager.

13. Disable the 'Privacy and Security' settings



Google has integrated some features into Chrome to improve the user's browsing experience. What's interesting is that these services involve sending data to the company's servers. This feature can be added to user accounts. Google then analyzes the data to sell more personalized ads.

Some features send data to Google each time a user enters a letter in the navigation bar.

This means that Google will see everything you search for and every website you visit, whether or not you use a Google search engine and even if you change your mind, decide not to visit the site or Start a new search. Are you comfortable when Google knows a lot about you?

Users can turn off these options by opening Chrome settings and going to the **Privacy and security section** .

Features to disable:

1. **Dùng service prediction ?? th?c hi?n** tìm ki?m tìm ki?m **và URLs typed trong** ??a ch? ??a ch? ho?c trình kh?i ??ng tìm ki?m (Use **prediction feature to help complete searches and URLs entered in the address bar or** search engine URL run the application).
2. **Use a prediction service to load pages more quickly** (Use the prediction feature to load pages faster).
3. **S? d?ng m?t d?ch v?** web ?? gi?i quy?t **giao d?ch l?i** (Use web service to help solve **navigation errors**)
4. **Help improve Safe Browsing** (Helps improve browsing safety)
5. **Automatically send diagnostic and usage data to Google** (Automatically send diagnostic data and use to Google)
6. **Dùng m?t d?ch v?** web ?? gi?i quy?t **l?i spelling** (Use **web service to help resolve spelling errors**)

14. Do not save addresses and payment methods

Whether you like to use the Internet or not, in the current context, it is difficult to avoid filling out online forms. Chrome will try to make this task easier for users by remembering the information or having to fill it often, such as email address, home address, phone number and credit card number.

But that means the user is creating a detailed record of unnecessary personal information. Even if the synchronization feature is turned off, someone with access to the computer can get this information. This can be dangerous if you keep your computer in a public place, or it can also lead to unforeseen consequences, when sharing your device with friends or other family members.

Users can ask Chrome not to 'remember' most of this information by visiting **People> Addresses and more** .

To prevent Chrome from storing credit card information, visit the **People> Payment methods** . Both of these options allow users to delete any information that Chrome may have stored.

Conclude

The above tips will greatly reduce the amount of information users put online, but they cannot completely prevent data collection from Google. Tracking users' browsing habits can still be done by other parties, including Internet service providers.

If you want to protect your privacy even more, consider changing your DNS settings and using a VPN.

Do not stop at normal browser and network settings. If you own a Chromebook, it's likely you already have a Google account. You may have provided Google with a lot of data. Fortunately, Google is very transparent about what it collects. Users can view their account and limit which data Google can access.

Although these tips will help you reduce privacy concerns through Chrome, Google actually stores your data for monitoring, and if you're using this service, the price is a Your privacy section on the web. Finally, if you feel uncomfortable with all of Google's curiosity, you can give up Google, and it's not easy to do it!

See more:

1. How to enable Site Isolation security feature on Chrome
2. 3 Chrome extensions enhance your security and safety
3. How to enable redirection blocking to malicious websites on Google Chrome