5 ways to ensure users are not 'tracked' on the Internet

Spyware - Spyware has become more and more diverse in terms of quantity as well as much more sophisticated ways of operating. And most recently, they began to divert more focus on the history of the system through the browser in the user's browser, thereby easily gathering a lot of information about the websites they had left.

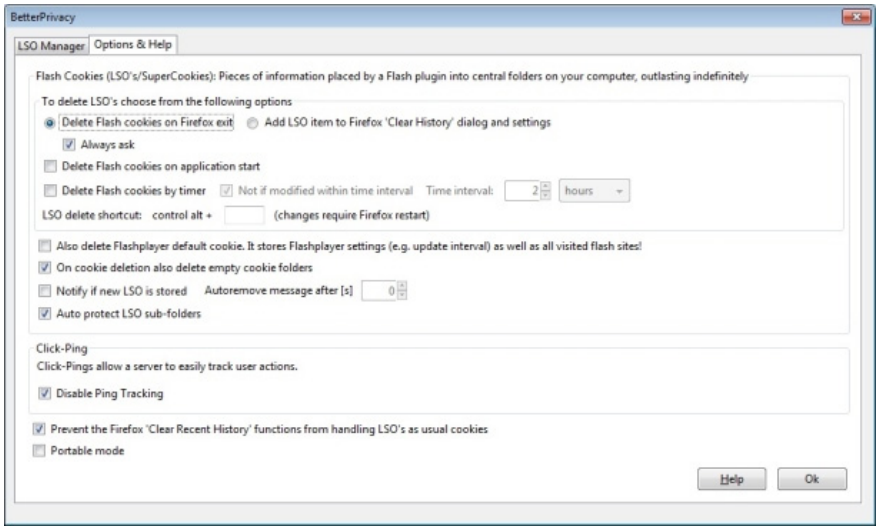
TipsMake.com - Spyware - Spyware is growing more diverse in quantity as well as more sophisticated way of operating. And most recently, they began to divert more focus on the history of the intrusive system within the user's browser, thereby easily collecting a lot of information about the websites they've been visiting. visit, even in privacy mode (cookies are completely ineffective). In the following article, we will introduce you some basic ways to minimize the risk of risk and change your personal settings when faced with these hazards.

Prevent super cookies and advertising information before they download themselves:

In May, **Microsoft** and **Adobe** reported that deleting cookies in IE 8 or 9 versions will also delete Flash cookies and **local shared objects - LSO** . Later changes require users to upgrade Flash Player from version 10.3 or later, as recommended by Microsoft at IEBlog.

The add - on components for Mozilla Firefox and Google Chrome browsers have added new functionality by allowing users to prevent LSO as well as other tracking files that can download themselves with the content of the website. there. That is Firefox's NoScript - add - on, which supports us in blocking **Flash** and **JavaScript** based on **side by side** and **source by source** mechanisms **.**

Besides, NettiCat's free BetterPrivacy application is also equipped with an attractive feature that allows users to decide whether to accept or not use any Flash cookies. On the other hand, the program will display a warning whenever a new LSO component is added, and set up a shortcut system to quickly delete the LSO. By default, **BetterPrivacy** will automatically remove all Flash cookies when we close Firefox:



A well-known and widely used support tool is AdBlock Plus for Firefox and Chrome. Not only does it help users in blocking and eliminating ads, but there are also more than 40 filters - filters available, which are suitable for detecting malware, malware on many different domains.

Improved browser security and speed:

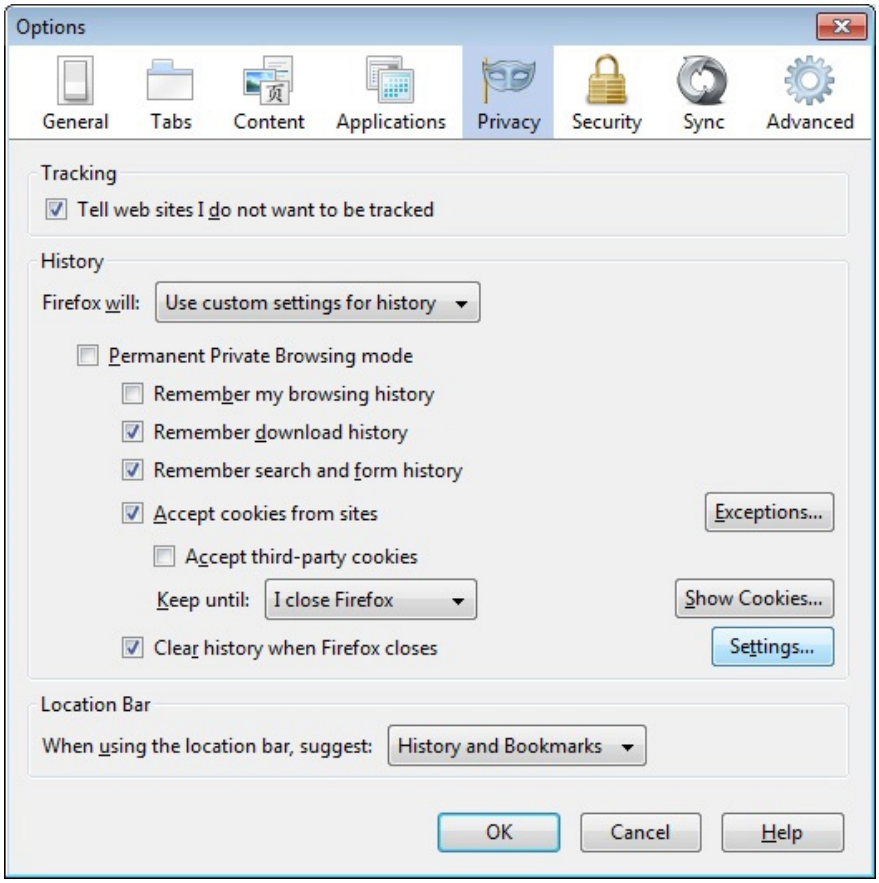
If someone thinks OpenDNS is not a security measure in the Internet environment, they are wrong. This online service replaces the user's **Domain Name System** with their existing platform system, with much faster and safer performance. OpenDNS Basic service package with individual user ads can be upgraded to OpenDNS VIP with a maintenance fee of **$ 10** for a year, besides some other services such as for K-models. 12 and business organization.

The main operating mechanism of **OpenDNS is** based on the **web-cache server** 's network system, and stores the entire content of the 'close' website with more browser accessibility, besides minimizing the possibility of minimizing Multi-threaded data delivery is not really necessary. This server system also has the function of filtering and classifying inappropriate content or containing potentially harmful information depending on the user mode applied.

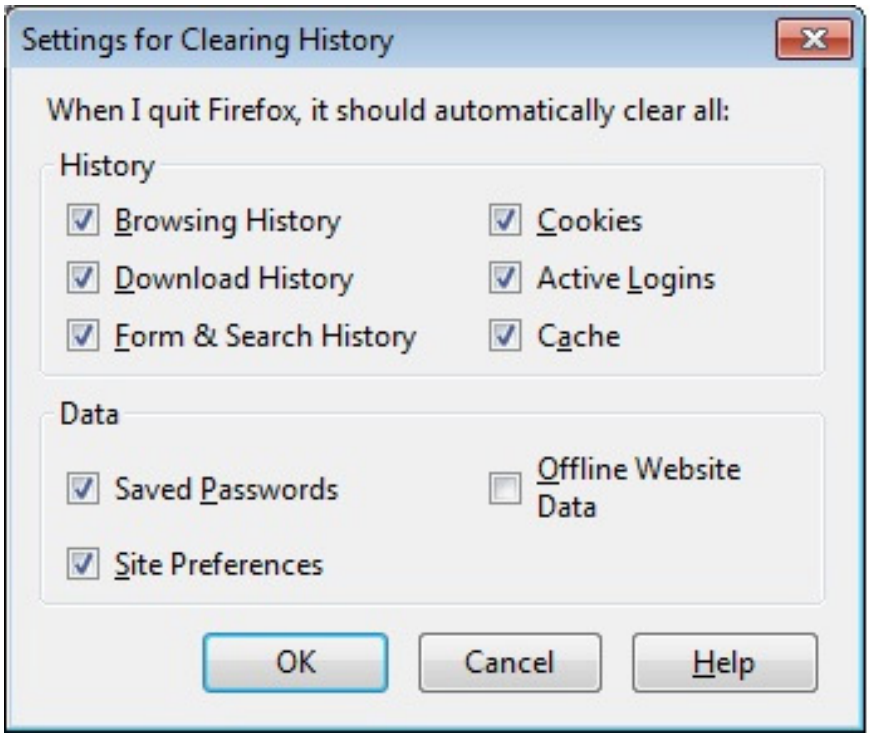
Set the mode to automatically delete history, cache and cookies when the browser is turned off:

In fact, there are many reasons to keep the user's history, cache and cookies. But at the same time this will leave a lot of our traces on the Internet, on the other hand they will have a pretty big impact on the speed of the browser. Depending on the perspective of each person, this is good or bad, in terms of technical aspects, storing cookies, history and cache will help us access familiar websites faster, and for those who love High demand for security, this is absolutely unnecessary.

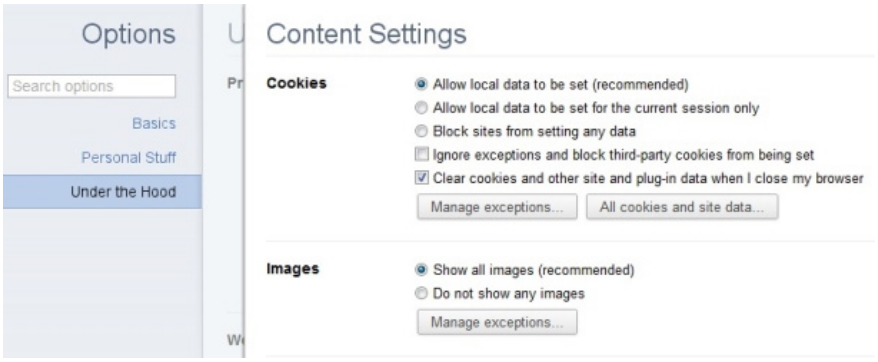
To fix this, you can use the **Bookmark** function for familiar website addresses. If you want to change Firefox's settings to this storage feature, open **Tools> Options> Privacy** and choose **Never remember history** in the menu displayed as a Firefox drop-down, or **Use custom settings for history** with More options. Then, check the box **Clear history when Firefox closes:**



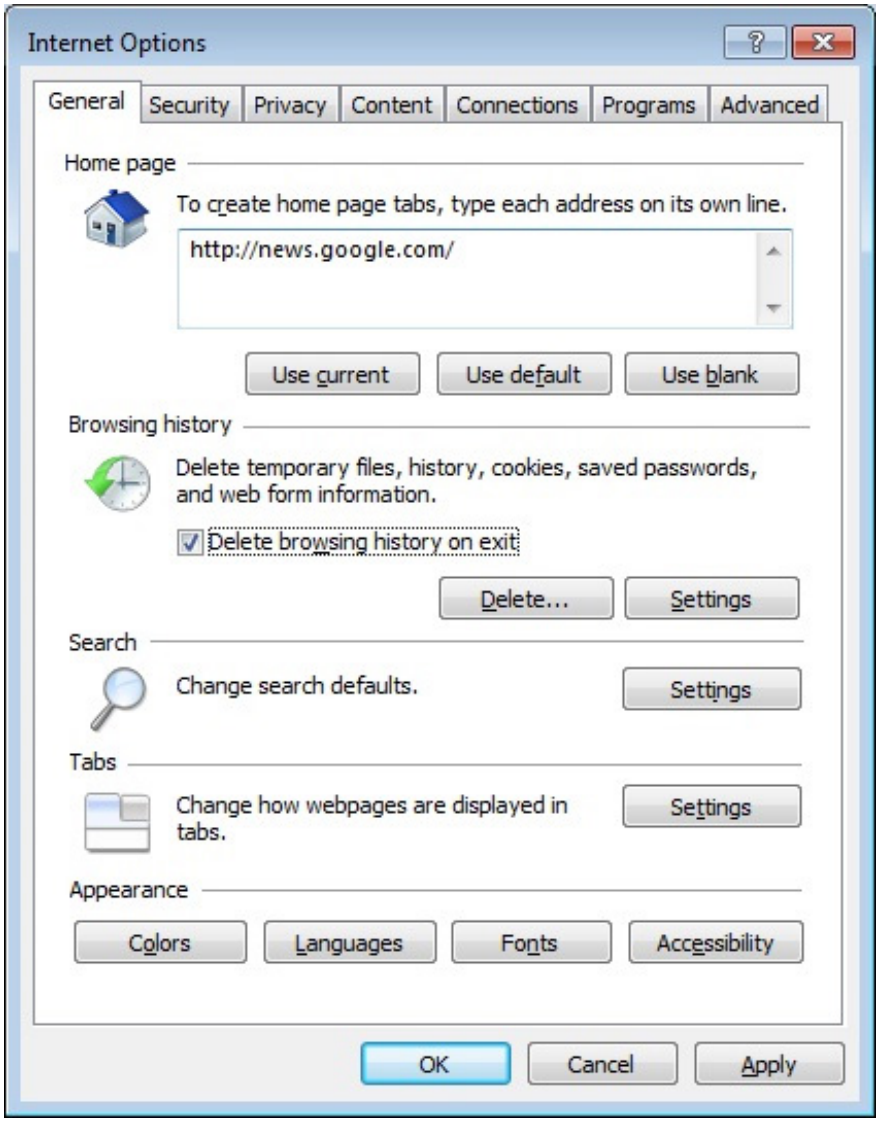
Click **Settings** , the browser will display the next settings panel with each type of user data you want to delete when you close **Firefox** , including:



Besides, **Private Browsing mode** is also a safe option, the browser will not save any information during the start to end time. Open the **Security** section of **Firefox Options,** uncheck the box in **Remember passwords for sites** . As for Google Chrome, you press the button with the Gear icon in the upper right corner and select **Options> Under the Hood> Content Settings** , check the box **Clear cookies and other site and data plug-in when I close my browser .** When you want to view all stored personal data, click **All cookies and site data:**



In **Internet Explorer** , likewise, select **Tools> Internet options> General** , check the box **Delete browsing history on exit:**



Should Sign - out every time using online services:

When using many web services that are linked together via an account, such as Gmail, Facebook . users often do not know that their personal data is being "shared" quite comfortably between this service. Therefore, to avoid the unfortunate circumstances that may occur, you should not share an account with many online services, do not use the Remember option when logging in, always **Sign - out** carefully when completing. into work.

Send and receive data from webmail accounts via Desktop application:

Currently, there are quite a lot of user comments around why we should use the email client program on the Desktop to support our daily work. The answer is to ensure security as well as improve working performance, you can refer to some of the following articles:

- Sync Gmail and MS Outlook contacts

- Data synchronization between platforms and devices

- Add Gmail account to Outlook 2010 with POP

Recently, the **Electronic Privacy Information Center - EPIC** pointed out that Gmail has violated the privacy policy of users when they accidentally or intentionally 'consulted' their personal information when sending emails with Gmail mailboxes. .

When performing a forwarding operation - **Forward** email from the webmail service to the client application on the Desktop, the content of the email received by the user still has to go through a review of Gmail before the email is actually forwarded. . But besides, there are still many other opinions that people have exaggerated about the incident of Gmail. More simply, we can enable **HTTPS** security for all transactions via Gmail, which is much safer than normal.

Good luck!