Some ways to protect personal information should be known and used when surfing the web

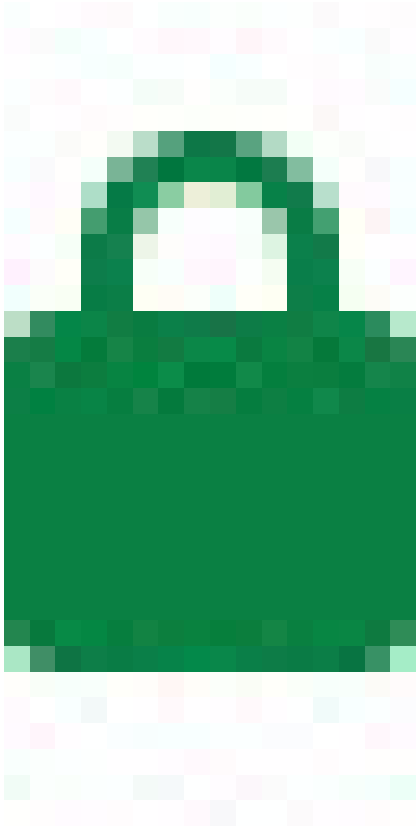
You may not know, but actually, whenever you surf the Internet or use any Internet service, you will disclose some personal information. So how do Internet users have to protect all data when surfing the web?

You may not know, but actually, whenever you surf the Internet or use any Internet service, you will disclose some personal information. So how do Internet users have to protect all data when surfing the web?

1. Avoid sites that do not use HTTPS protocol

When having to log personal information such as login information, identity cards, payment details . on any website that needs careful consideration, we should pay attention to avoid the website having HTTPS prefix means that anything you do there is not encrypted or web pages may have HTTPS prefixes on the home page, but on linked sites it is converted to HTTP.

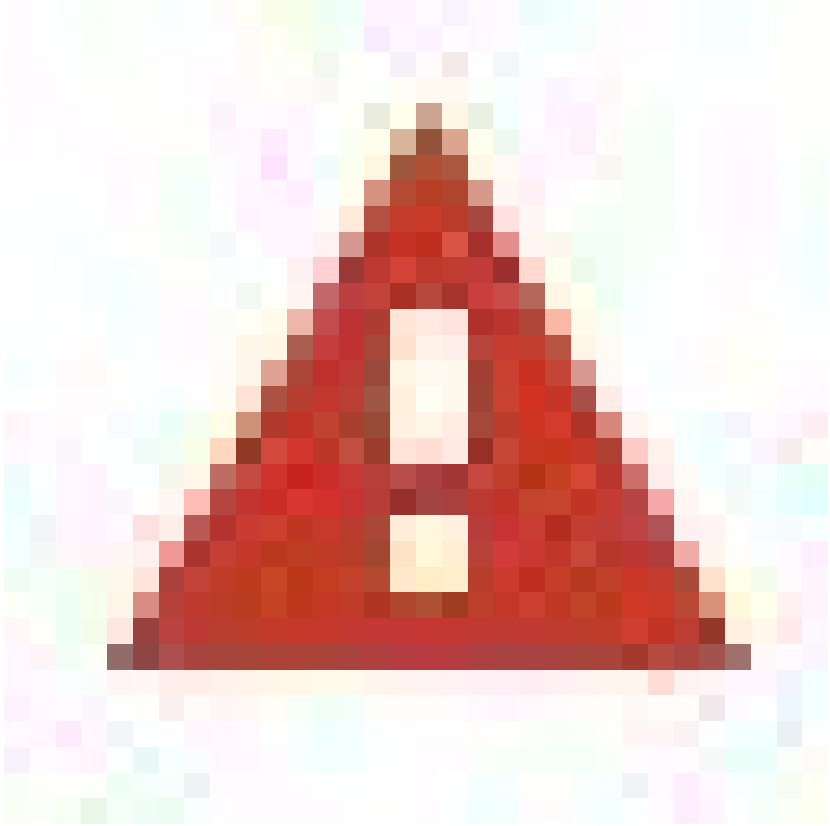
To know if the site is safe to access, you can check the security information about the site. In the Chrome browser, the security status appears on the left of the URL box. As follows:

1. 

Security key

2. 

Information or not confidential

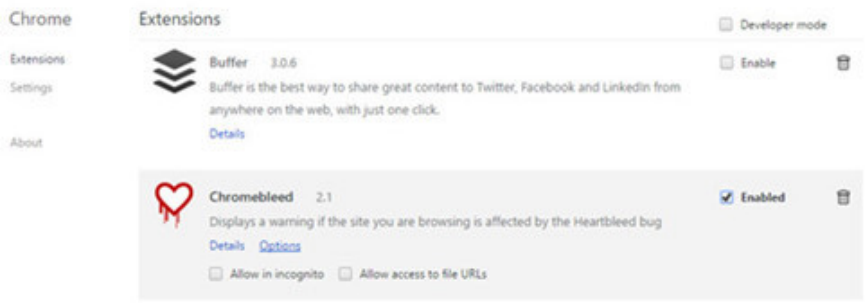
3. 

No security or danger

With Firefox, Chrome and Opera, if HTTPS links are found to be corrupted, the HTTPS Everywhere extension will automatically encrypt the browser contacts with the main site.

2. Limit the use of unnecessary plugins and extensions

It is possible that in the downloaded software to provide your browser additional security contains the vulnerability from which hackers can exploit to collect your personal information. And extensions are not updated, people using them can become targets of hackers.



For safety, you can turn off plugins that are not frequently used or not used in browser settings. Microsoft Silverlight, Adobe Flash and Java are the 3 major plugins you can disable because many websites no longer use them, YouTube no longer uses Flash and Netflix dropped Silverlight.

See also: How to remove and disable plug-ins in the browser?

3. Avoid being followed

In order to load web pages correctly, we are often asked to allow websites to access the location, screen size or browser version data you use. If you agree, a lot of information, such as hardware, plugins, has been installed . can be forwarded by additional plugins like Adobe Flash and Java. This keeps you tracked even if the tracker is disabled because the information can be combined to create browser-specific data.

4. Be careful with the browser's autofill feature

Information such as your name, address and date of birth will be filled in the required forms with the browser's auto-fill function. But certain browsers, including Chrome, Safari and Opera as well as the LastPass password manager extension, may be tricked into revealing saved personal information that users don't detect.

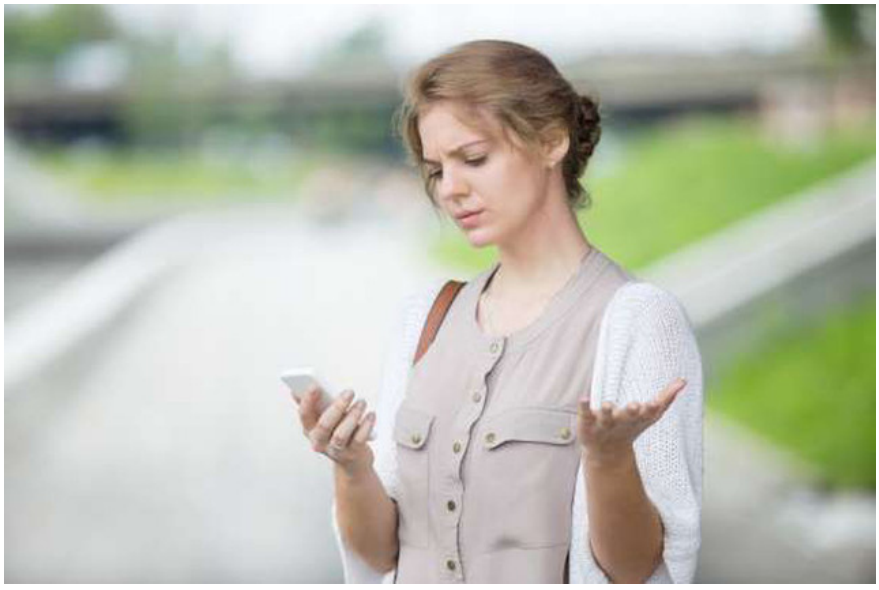
Specifically, when accessing a malicious website, you will be asked to enter harmless information such as your name and email address. If you type, the browser's auto-fill feature will add other information saved in the browser or LastPass. Combining all this information, bad guys can trigger credit card fraud.

Therefore, before filling in personal information on any website please be careful. Log out of LastPass, delete your credit card information from your browser, or turn off auto-fill completely to ensure your personal information is secure.

6. Shop anonymously to not be "rotten"

When users visit an anonymous website, you can use the Internet more comfortably, not afraid of being monitored by the browser. So, when shopping online you should check the service price through an anonymous website or other device to avoid being "cut down". A typical example is the online travel website Orbitz, which caused a stir in the online community in 2012 when it was discovered that this site is "pushing" for customers who rent Mac rooms at a higher price. with computer users who often visit their site.

7. Turn off the Airdrop feature in public places



AirDrop is a method of transferring content (photos, music, videos) from Apple iOS devices together. The operation of Airdrop is similar to that of "shooting" photos using Bluetooth on Android phones. So, in public, users should turn off this feature or set it to work only with people in your contacts to avoid bad guys taking advantage of crude, dirty pictures. via Airdrop.

8. There should be another email backup

In this technological age, all jobs can be solved by email simply and easily. But in the middle of a pile of important emails that you have been attacked is really a bad thing. To avoid such bad things, set up a backup email, this way you won't be afraid of falling into the wrong position without technology firms' exit lines.

9. Use a hard-to-guess password

According to a study, it is shown that in 2018 many people still have the habit of using a password that is their full name or date of birth, serial number . to use, which makes it easy for hackers to know and steal your data.

To keep your information safe and secure, the longer you set the password, the more secure you are. Therefore, you should set yourself a password that is easy to guess with you but difficult to find for others.

10. Check if you have ever been hacked

In the past decades, many cyber attacks have occurred, so that users can easily check the information of their email address has been hacked or not, many websites have appeared to help users can More peace of mind during use.

How to do it is simple: Enter your email address on those pages. This routine check is highly recommended. Or if you feel insecure, you need to change your email password immediately.

11. Do not turn on auto play on Youtube

Turning on auto-play mode is a habit of many people today. However, this use also has two sides, it can also help you more convenient during use. However, this way also makes you suffer from the application "drive" to unwanted content.

So, when using YouTube, turn off this spontaneity feature and manually click to search for content that interests you, not "interested" YouTube.

12. Stay alert

Keep in mind one thing, when you are online, someone will always follow you. Maintaining such a sense is a good habit to set up.

Accordingly, you need to avoid sharing information publicly, allowing applications to access your address book.

The world will become more and more closely connected, so each person should also be more aware in protecting personal information.

13. Secure old accounts

There are accounts that you may not use anymore, some emails that don't touch or a social network account . even if you don't use them anymore, yet they are still active every day and may have Store lots of information about you.

So either you choose to completely delete your account, or update your new password and choose an authentic two-step security solution to increase data security.

See more:

1. Encryption to protect information on tablets
2. 8 ways to protect simple digital personal information
3. 5 Facebook privacy settings you should know

You finished reading the article "**Some ways to protect personal information should be known and used when surfing the web**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.