Online privacy protection

Below is a guide to security features you should consider before logging in to any new online service.

TipsMake.com - Your **personal data is available on the Internet. Any thoughts you share on Twitter or all status updates you post on Facebook, and even the latest purchase with your credit card can be accessed on the Internet.** Even if you can find it handy to put such information online to access them immediately, your point of view may change as advertising services interrupt a lot of fish ads. Very attractive personality.

Below is a guide to security features you should consider before logging in to any new online service.

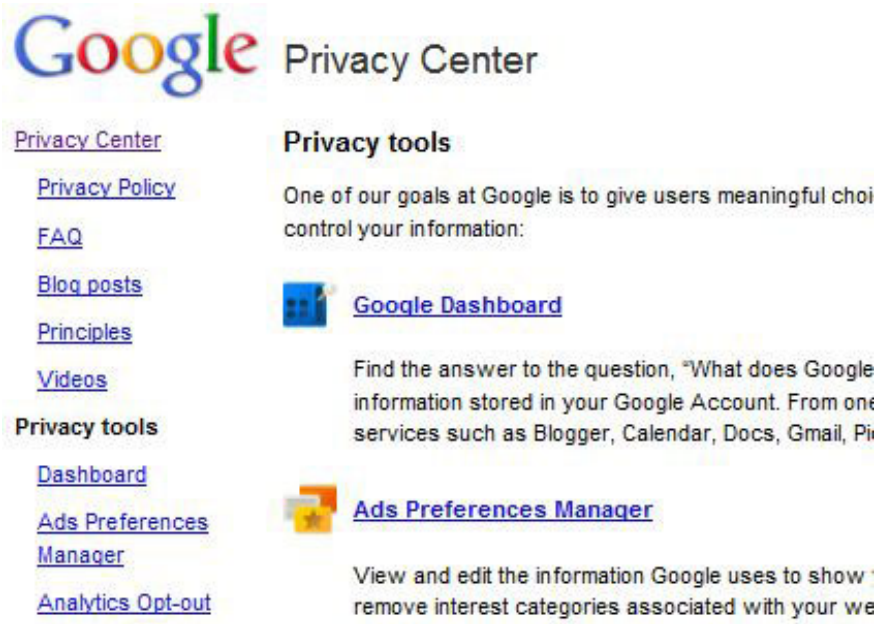
Do Not Track

The Federal Trade Commission (FTC) thinks that when you surf the web, you should also surf anonymously. A **Do Not Track policy** , " **Do Not Track** ," has been released, which may require online companies to respect users' wishes for online tracking. Since advertising companies track the sites you have visited, the Do Not Track policy will help you eliminate this process. Although the FTC has made official guidelines, Google's browsers, Microsoft and Mozilla still have their own anti-tracking features.

However, none of these features is really ideal. Mozilla's Firefox browser requires websites to identify a sub-command, forcing the server not to track requests for page access. Microsoft's Internet Explorer 9 uses a reliable list of sites that track trends to block them, and Google's Chrome browser simply stores user preferences. Although each method has its own limitations, web design standards - World Wide Web Consortium (W3C) - now believes that Microsoft's approach can be an Internet standard.

What about Google?

When you type a search request, will someone follow you? Under Google's privacy protection policy, the company will monitor what people often search for so they can apply autofill, which helps them better participate in your search needs. The company also captures the URL you type into their browser whenever they want to access the site. In fact, this is the same as Microsoft applies to its search engine Bing and Internet Explorer.



Both Google and Microsoft follow personal interests. However, Google has changed itself by making the terms more transparent and transparent. Google's security center is known for its easy-to-use FAQs questions and explanatory videos on YouTube. Meanwhile, Microsoft's personal page is merely a document without a specific example, it's hard to know what's going on.

Social Network

Although Twitter lacks a security center, they still have a privacy policy and options. For example, under the **Settings** menu item, Twitter allows you to add locations to tweet. This seems very interesting, because all other functions are confirmed on location data, except on Twitter you will have to enable this feature. Besides, Twitter also gives you the option to remove all location data from where you previously tweeted if you wish. Another option that also has the ability to keep you safe is that only your followers can view them. And Twitter also displays all applications that automatically re-upload your posts on Twitter (such as Facebook), so you have the option to revise that access anytime.

LinkedIn also has a security setting option. Like Twitter, LinkedIn can protect contact lists from anyone who is not affiliated with you. For greater security, LinkedIn will only display the contacts you usually share, not the entire list - at least without your permission. Still, LinkedIn's ease of use on security settings is still far behind both Facebook and Twitter.

Mashup pages

Unfortunately, the biggest security concern comes not only from browsers, search engines, or social networking sites, but also from sites that collect information from other sites, also known as 'mashup'. For example, FriendFeed, displays updates you create on both Facebook and Twitter. In order to use such a service, you will have to make sure whether the 3rd party services are trusted or not.
What happens if these pages collect data from your bank account or credit card? One of the most popular financial content sites is Mint.com (now part of Intuit). Mint has anonymously collected data from more than 4 million users. You can subscribe to this site anonymously, so that your name and address are not part of your account information. In addition, your credit card and username and bank account password will be stored on a separate server. The company's privacy policy also states that they 'only provide a' read-only 'view of your transaction information. So far, Mint has not had any data infringement announcements.

3rd party application

It is very dangerous for a third party to write code for a service. You probably remember last fall, Facebook revealed that application developers for this social networking site may have leaked personal information about its users; apps like FarmVille and Texas Hold'em seem to have sent their Facebook ID numbers to at least 25 advertisers and data. A class action takes place against Facebook when they let these 3rd party applications access data. With more than 500,000 'appealing' apps on Facebook, the number of people who stand up to the social network can continue to increase.

App stores like Apple, Google, like Facebook, may have difficulty controlling all of the apps written - although Apple, with the 'use of garden protection' method, also just stop at trying level. That's why third-party security apps like Lookout Mobile Security can help. Such tools can report an application's security breach, which is equipped with information and you can decide whether to delete the application.

Cloud security

Data storage in the cloud can solve problems, allowing you to access your files from anywhere. However, it also causes other concerns, such as someone accessing your personal data without permission. One way to overcome this risk is to select cloud services that include data encryption.
For example, Dropbox file hosting service implements a Secure Sockets Layer (SSL) encryption protocol every time you upload a file, and uses strong AES 256 encryption algorithm for cloud storage data. . Besides, Mozilla also provides a cloud-based synchronization service for Firefox, which can encrypt bookmark data before they leave your computer.

Steps should be taken

When signing up for a new service, you should always read the security terms carefully and look for options. Good security policies will also tell whether or not a service tracks your activities and sells that information to third parties - and they will have to make it clear that your data will come out. What if you agree with the service.

In addition, use the SSL protocol when accessing the Internet whenever possible. SSL also ensures that every time you use a wireless network, criminals will have to spend a lot of time eavesdropping. Not all websites currently support https: // (this page shows that they use SSL protocol) except for sites like Facebook, Gmail, Google, and Twitter.

What to do when it's too late?

If you discover that sites like Pipl, Rapleaf, and Spokeo list too much of your personal information, you will have to choose. First, go directly to Rapleaf site (this company will remove it if you request it). In addition, edit security information settings on Facebook, LinkedIn, Twitter, and delete as many personal information as possible on these social networking sites.

If, after a few weeks, you still see there is too much of your personal information on Bing, Google, Pipl, or Spokeo, think about hiring a reputable professional service. These services can cost you about $ 630 to $ 3000. However, try to protect yourself first.

To some extent, everyone has personal information stored somewhere on the Internet, out of their control. So, you should not pay attention to unimportant things; for example giving a general comment tweet on Twitter will also be recorded by search engines. Instead, think about abuse of information, such as identity theft (someone collects your personal information and uses it to commit fraud).