Security tips for Google, Facebook and online services

Recent information about US government secret activities, the intensification of infringement of personal information and the appearance of your avatar on Google Ads has raised a problem: Fish Information Your online personality is only protected when you can keep an eye on them.

Recent information about US government secret activities, the intensification of infringement of personal information and the appearance of your avatar on Google Ads has raised a problem: Fish Information Your online personality is only protected when you can keep an eye on them. But when these data are on the server in some remote place, they no longer belong to you.

There has been a lot of information about our daily lives posted online, mainly to bring convenience: **Gmail** and **Outlook.com** to store email, **Dropbox** and **SkyDrive to** help your data store. Can be used anywhere, anytime. **Windows 8** helps you find information with the default Bing tool, Google Now even offers the information you need before you realize you need them.

But convenience always goes hand in hand with loss of control, and this has caused problems with personal information security.

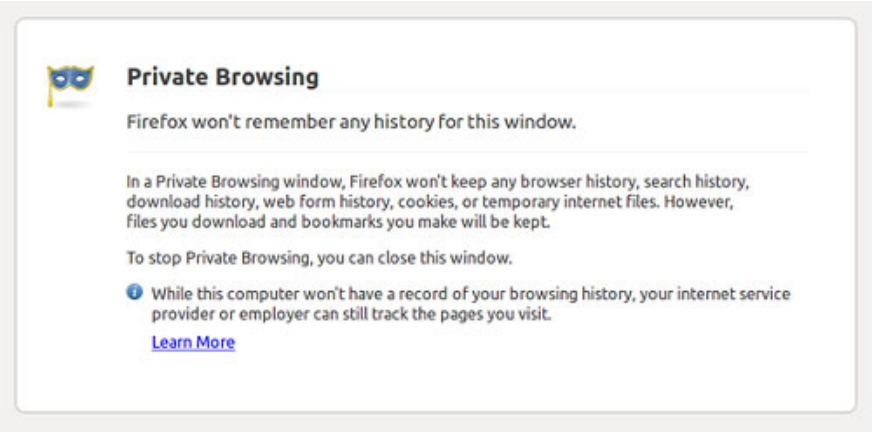
This article can show you some simple ways to help you minimize your online personal information. But before you start, remember that these tips are all familiar to you. You can follow all the instructions in this article, tighten security with just a few tips below or go deeper into security.

Prevent Google

When it comes to reducing the amount of personal information online, we have to start with Google. Imagine what your company owns: Search history, websites you've ever visited, contacts you sync to Gmail, apps that have been downloaded from Google Play, location data from Android, Chrome and Maps, Google Drive document repositories . sounds more than you think, right?

On their side, Google controlled the data very carefully, and received good reviews in the " *Who has your back"* survey of EFF (Electronic Frontier Foundation - Association to protect the rights of computer users). calculation). But Google also has the right to deep access to your data, something worth thinking about in the context that Google has just announced plans to use your real name and photo for online advertising (that's not it yet). including Microsoft's *"Scroogle"* campaign.

Stopping using Google doesn't seem to be a viable option for most people, which gives Google a monopoly. Even if you switch to using Microsoft services, your data warehouse is still on the server. So what can we do if we want to reduce the amount of data sharing online?



First, try to **stop Google from collecting and sharing your data** . Using the browser security mode will help you remove tracking cookies, including those of Google, when you turn off the browser. You can also ask Google to stop searching for information in your browsing history by editing Google's personal settings.

Another solution is to replace Google services that you can replace with more secure services. Are you using Google Docs but don't really need its online storage? Try using open source **Libre Office software** . If you only

need basic photo editing features, replace **Picasa** with **Paint.net** .

And Facebook

Google may have a wide range, but when it comes to systematizing your social relationships, no company can match Facebook. And like Google, Facebook is basically impossible to get rid of from our lives. You need it to register your favorite services, play games, chat, and keep in touch with friends.

Tweaking personal settings in your Facebook profile can help prevent prying eyes from other users - but infringement can come from Facebook itself. So how to protect your personal information without giving up this social network?

It's easy: Stop pressing like it is constantly and consider disabling unnecessary pages. Don't add information to your profile like a life event, where you used to be .

Finally, decide if you want to continue sharing your online photo repository. Think about whether anyone really admires them, or are they just helping Facebook's face recognition algorithm?

Facebook can also follow you when switching from one site to another by inserting a like button into these pages. Make sure you log out of Facebook to avoid things like this, or use the web browser security mode.

Finally, you can also delete your Facebook account if you can (and want to) get rid of virtual relationships online.

Storage "cloud"

If you've ever accessed your *"cloud"* repository, you probably won't want to give up this gadget. However, you can take control of that online data warehouse by encrypting them. This will help prevent intrusions (like what happened with Dropbox and Apple).

Remember that when services (like Dropbox) encrypt your data on their servers, they also hold the decryption key in most cases. That means you can't control when and who can unlock those encrypted data (but this also contributes to making it easier to use these services - only Please enter your login information and press **Enter** !).

Meanwhile, *"cloud"* storage *providers* like SpiderOak or Wuala can never touch those decoding keys, meaning that only you can decrypt your data. (Don't ever forget your password!) Also, you can encrypt data on SkyDrive, Google Drive, Dropbox, Sugarsync, or any other online storage service using the tools like **TrueCrypt** or **BoxCryptor** .

Or, if you want to access your data store anytime, anywhere, but don't trust to give it to anyone, use a networked storage drive. like Western Digital's My Cloud to create its own cloud storage.

Other services

We just talked about the online accounts you use often, but what about the other accounts you have linked to your social network? Visit the **settings** of Facebook, Twitter or Google+ to see a list of applications and services linked to your account. And if there are any applications or services that you haven't used for a long time, simply remove their access.

Speaking of applications and services, there is a simple way to protect your data store: **Regularly delete accounts you no longer use.**

The surface of the iceberg

Now at least part of your data is under control, and you can take care of other things. However, we only touch the surface of restricting who can trace your browser while online.

If you want to be safer, try Abine's DoNotTrackMe add-on for a week and see how many cookies have been blocked. You can also use standalone email boxes using the POP3 protocol to store e-mails and remove messages from server providers.

Today, completely isolating the Internet is impossible, but taking a moment to review your personal data store can be a great help to your security and privacy. And remember, how deeply you learn about security is entirely up to you.