NAVIGATING THE ONLINE: SEARCHING, BROWSING, AND EXTENSIONS

BROWSERS' BROWSER BROWSERS

A web browser is a software application used to browse, search, and display content on the World Wide Web. Today, some of the most popular web browsers, like Internet Explorer, Mozilla Firefox and Google Chrome are installed on most operating systems. And it is easy to notice the increasing threat coming from online criminals that try to take advantage of web browsers and their vulnerabilities. Some of the biggest networks, like Google, also have the ability to keep tracking you even when you're not signed in or on their page and follow you around the Internet to serve you with "relevant" advertising and content. Since almost everyone on the internet has some sort of account with a Google service, one can only imagine, the amount of data on civilians they hold.

So, securing our browser is one of the first steps we need to take in order to assure our online protection. Here are a few things you can do:

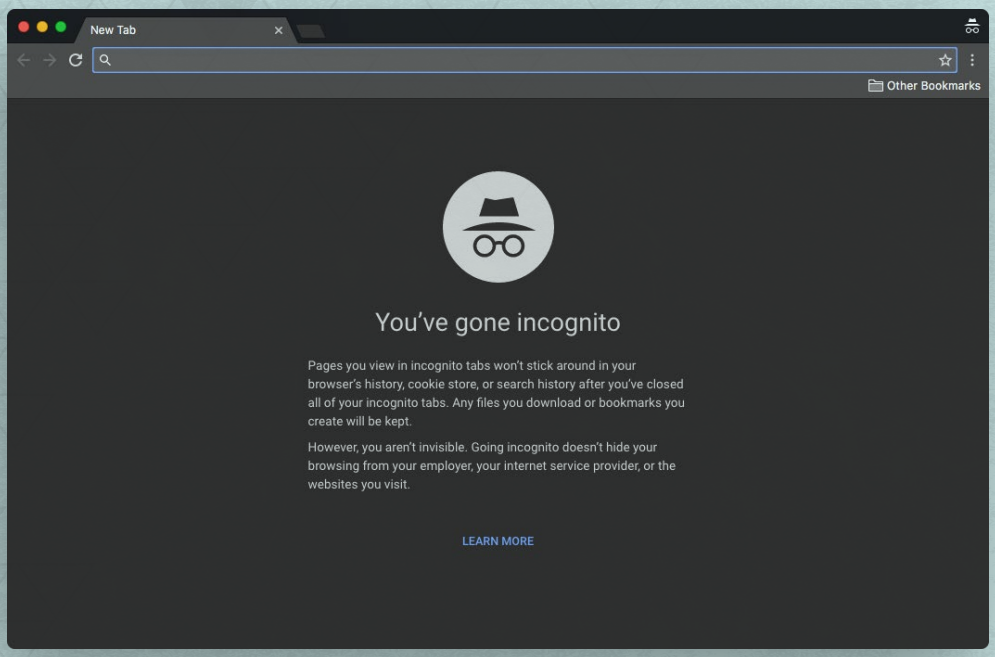
- Customize the settings on your browser for maximum security
- Add security extensions to your browser
- Use Alternative Search Engines

Changing your default browser settings will give you more control over who has access to your data.

GOOGLE CHROME

In recent years, the use of the Google Chrome web browser has significantly increased. As more and more people use it, there are a few actions we can take to also increase our online security.

To start making the necessary modifications, we need to access the settings area. Please make the necessary changes in case you are using a different version of Google Chrome.

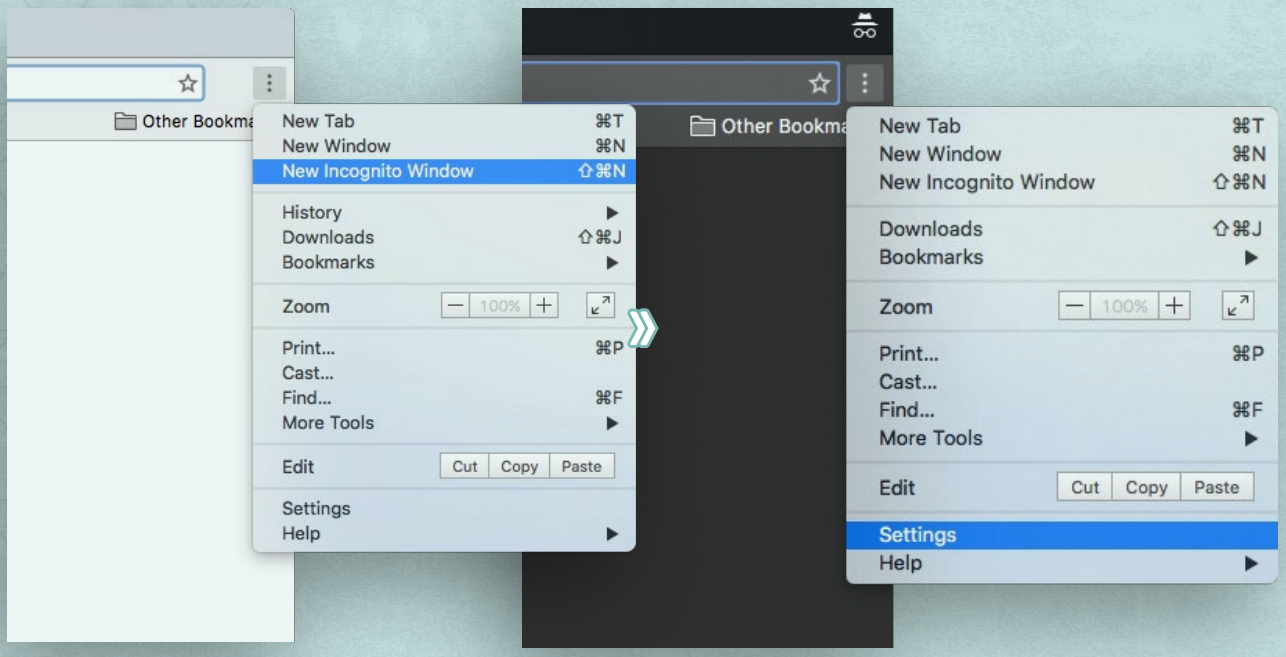


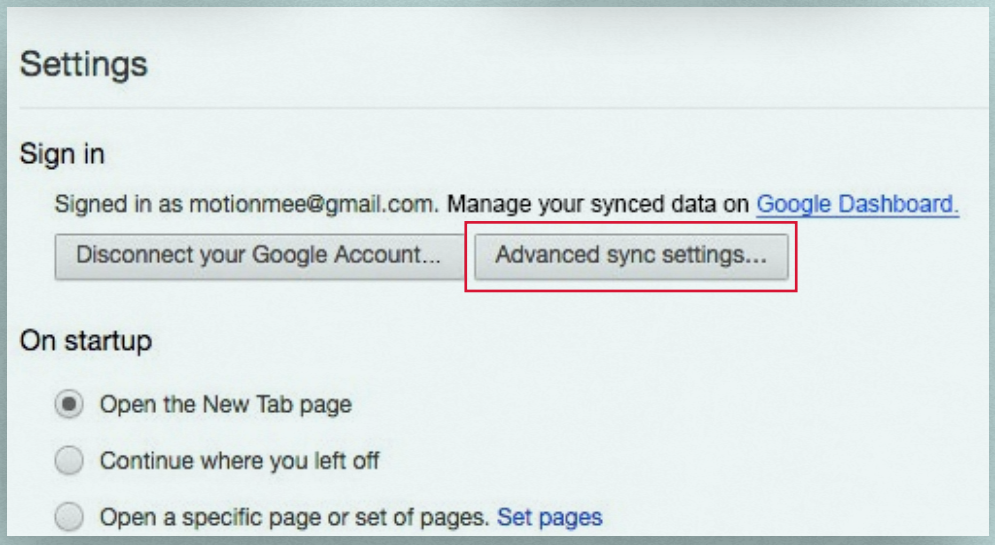
Chrome → ⋮ → Select "New Incognito Window"

Using Chrome's Incognito Mode means that when you close your browser, a number of traces created during the session are automatically cleared: your browser, search, web form and download histories, as well as cookies and temporary files.

- What is saved and deleted when you close the browser is already pre-defined—you can't customize 'private browsing mode' to suit your own needs.
- Only your browser history from this incognito session will be cleared. Your history from previous browsing sessions in 'normal mode' are unaffected.
- Trackers in the websites you visit can still collect data about you, including your browser history.
- Incognito mode does not give you anonymity on the internet.

- To access the settings area for Google Chrome, click the ⋮ button at the top right corner of the browser and select **Settings** from the drop-down menu.
- As soon as you access the Settings area, you will notice **Advanced Sync Settings** at the top, in the Sign-in section.

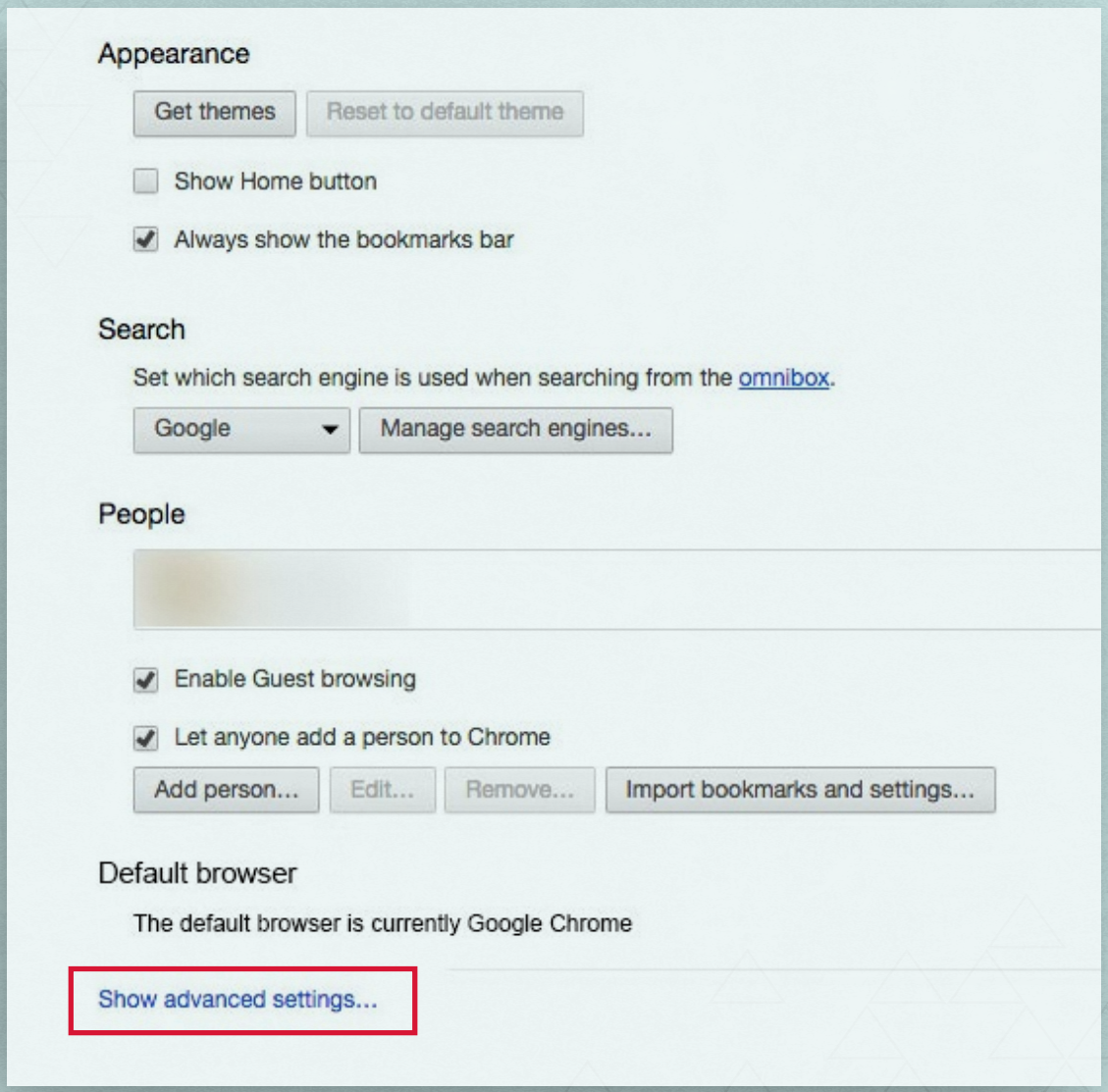




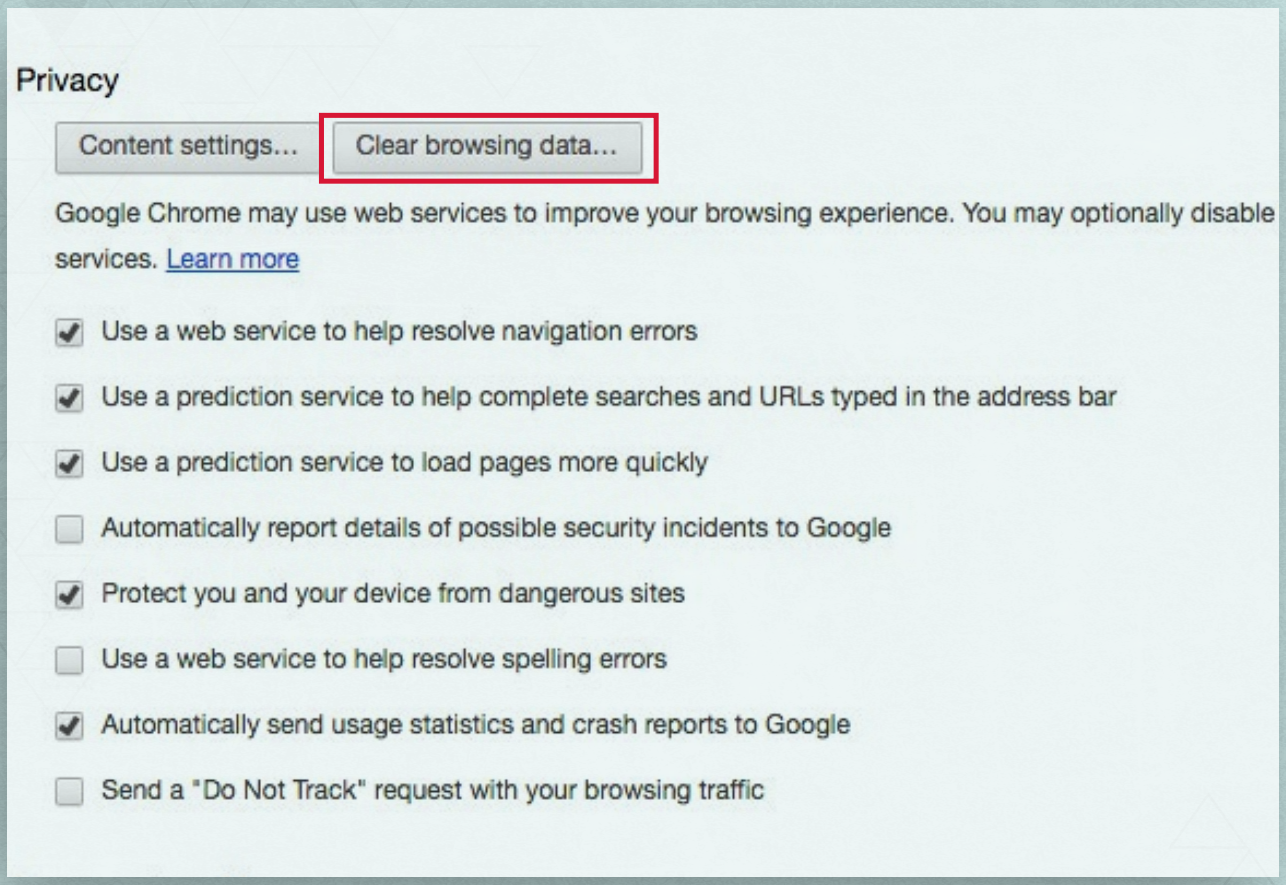
Google Chrome gives you the possibility to sync your settings and data with other systems or mobile devices where you signed-in with your Google account. This does create a vulnerability risk, since you are required by default to connect with your Google account on a device that also syncs with your other systems or devices.

To improve your security, you need to set a passphrase, which is an additional credential required to sync your devices.

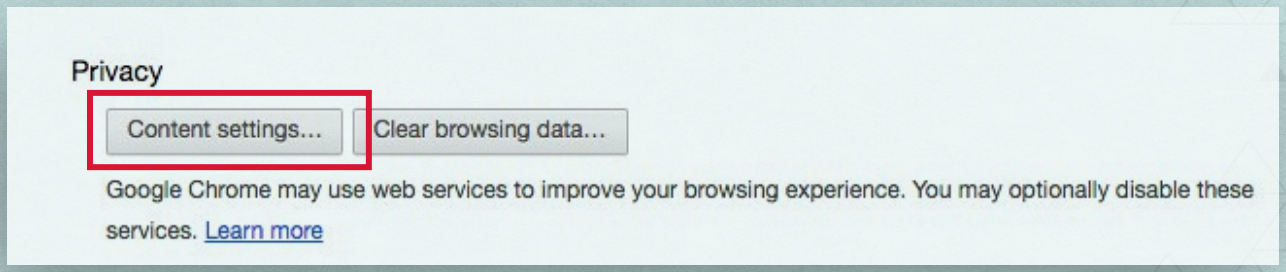
- If you scroll down at the bottom of the page, you will see a **Show Advanced Settings** option.
- Click the link in order to access the advanced settings available.
- The **Clear Browsing Data** option gives you the possibility to delete your browsing history, so don't forget to use that option if you are using a computer in a shared environment.



- The **Clear Browsing Data** option gives you the possibility to delete your browsing history, so don't forget to use that option if you are using a computer in a shared environment.

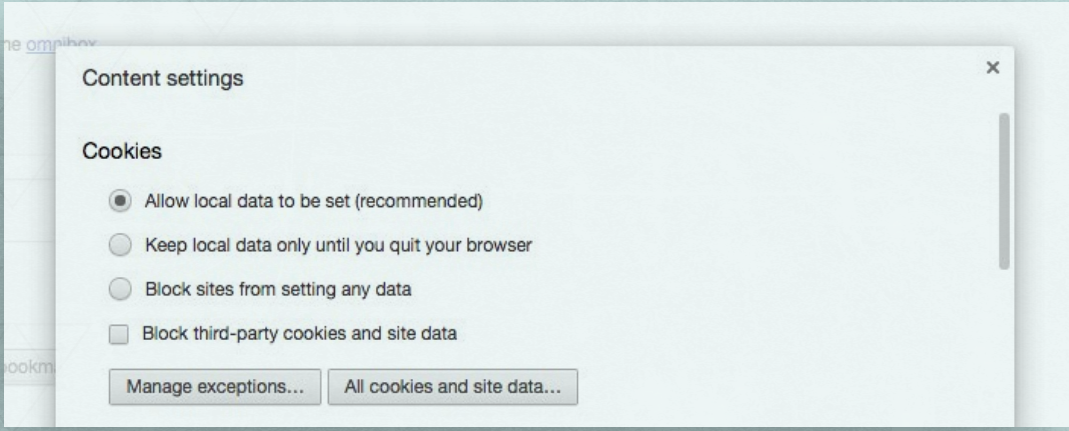


- The **Content Settings** option gives you more possibilities to address and improve your overall browsing security.

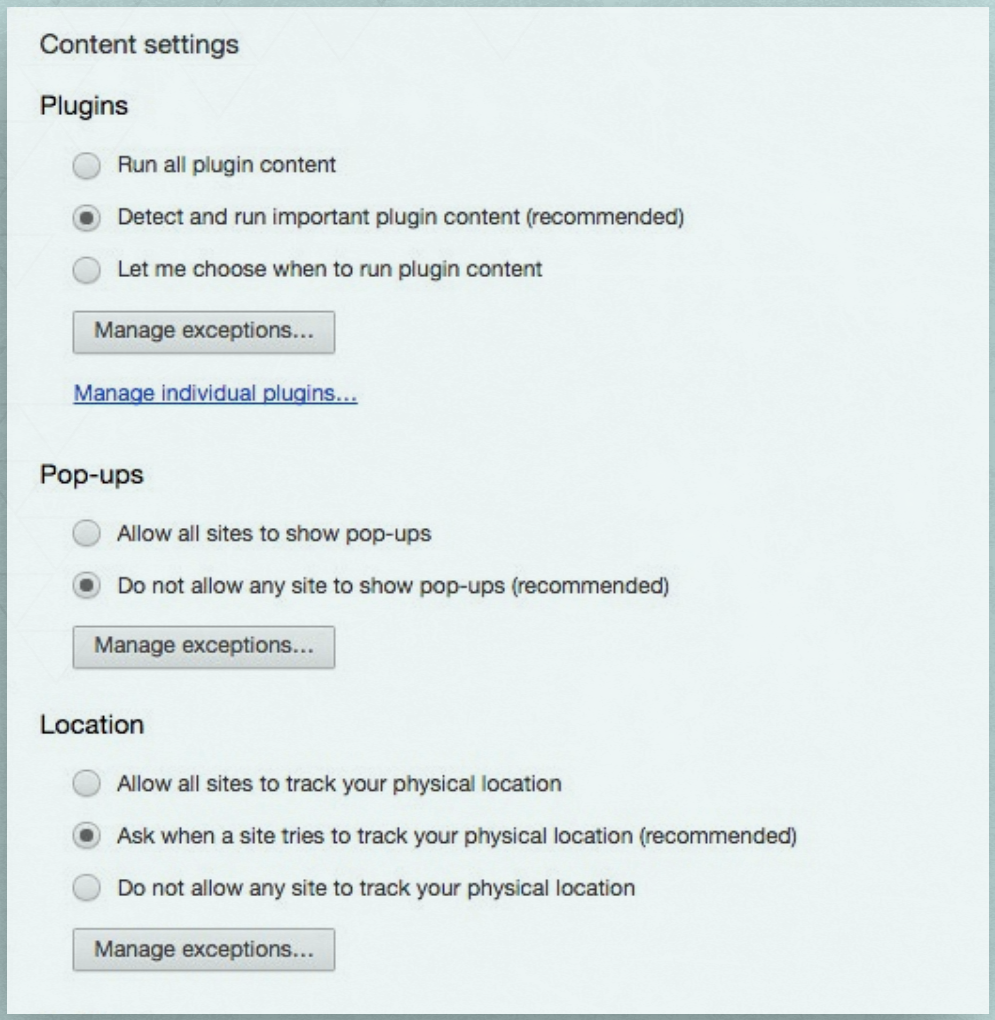


If you want to restrict cookies from being stored on your browser and using the collected information about your browsing habits, use the available options.

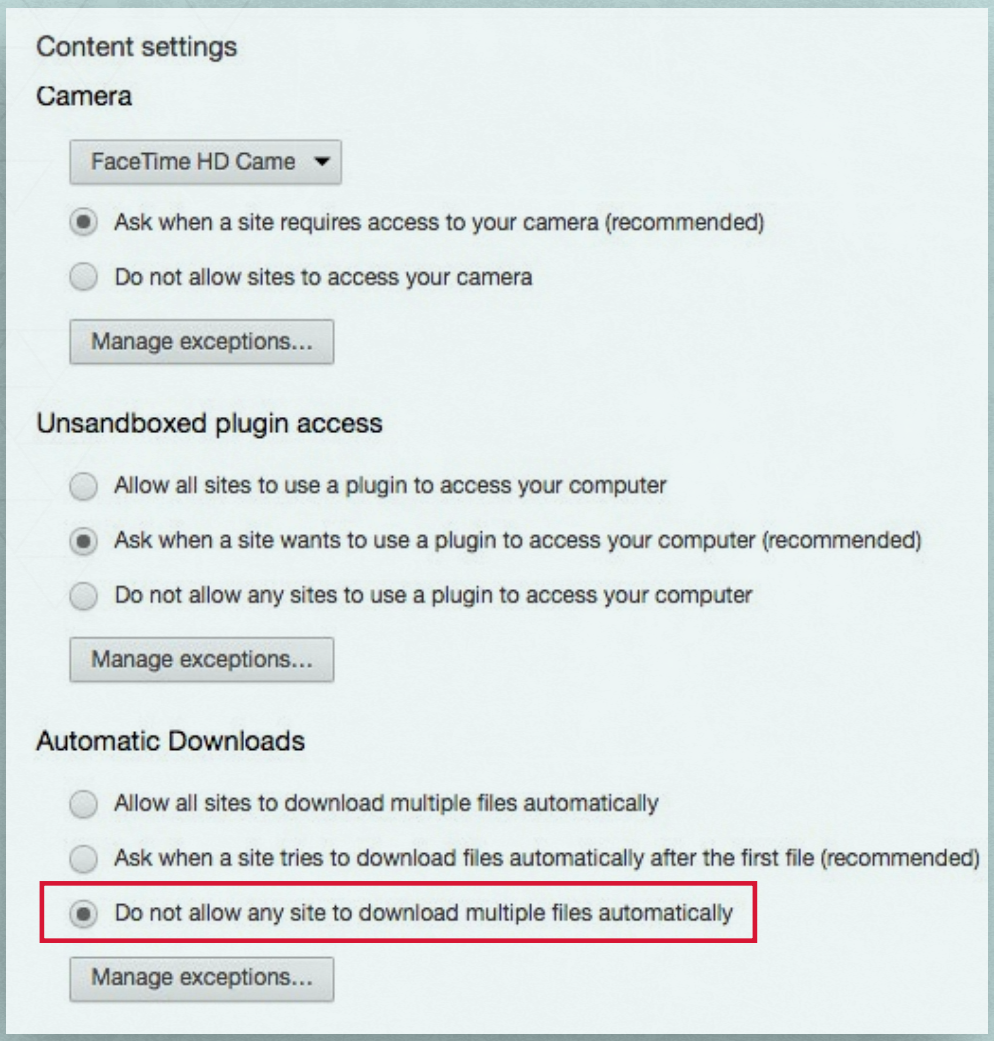
- To make the necessary changes in the **Content settings** window, you will need to scroll down in order to access the other options.



- Scrolling down, you find other options: You can control the behavior of your browser plug-ins, you can block pop-ups from disturbing your browsing session and you can stop a website from tracking your physical location.



- If you continue scrolling down to the bottom of the **Content settings** window, you will find the option to block websites from using a plugin to access your computer. There is also an option to block sites from downloading multiple files automatically on your computer, This can also further protect you from being exposed to sites that try to deposit security threats on to your device.



MOZILLA FIREFOX

Mozilla Firefox is another popular web browser and there are a few steps we can take to improve its security settings. To increase your protection against online threats in Mozilla Firefox (version 32.0.2), you need to access the settings area.

Private Browsing allows you to browse the Internet without Firefox saving any information in your browser history. You can set Private Browsing by default, or you can use it only occasionally.

Setting private browsing by default can be done in two ways:

- 1. Find **multiple →** ☰ **→ Preferences → Privacy → select Never remember history**

or

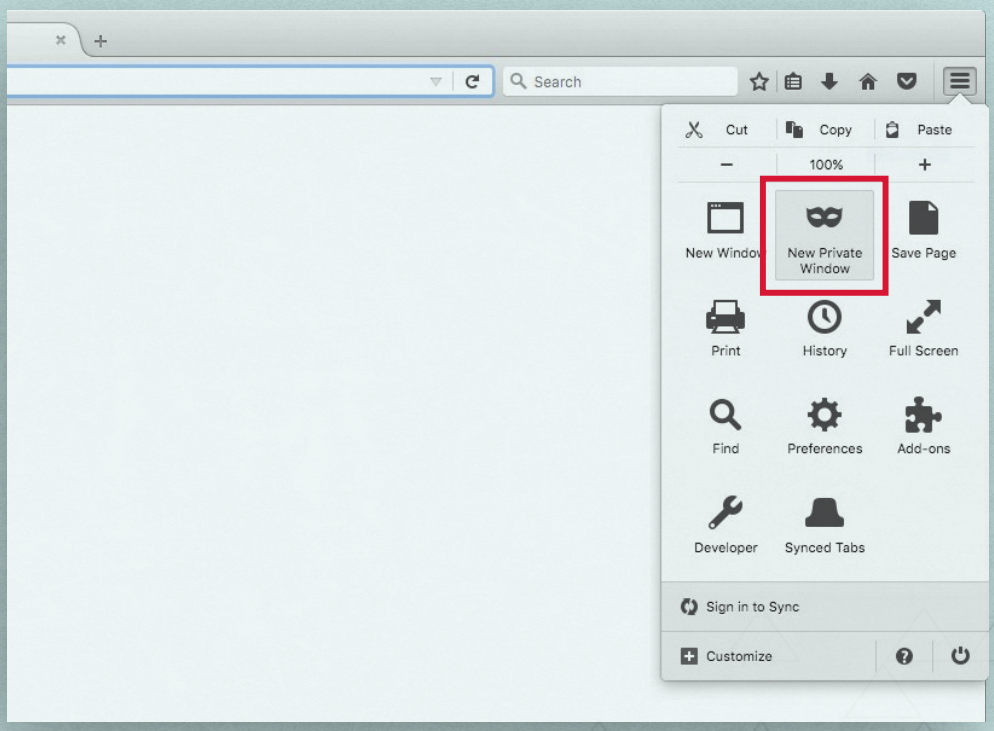
- 2. **Firefox →** ☰ **→ Preferences → Privacy → select use custom settings for history → check: Always use private browsing mode**

When you close Firefox, the following will be cleared: your browser, search, web form and download histories, as well as cookies and temporary files.

- What will be saved and what will be deleted is already predefined—you can't customize 'private browsing mode' to suit your own needs.
- Your history will only be cleared when you close the browser
- The trackers in the websites you visit can still collect data about you, including your browser history.
- Private browsing excludes the files you download and the pages you bookmark. These are saved.
- Private Browsing **does not make you anonymous on the internet**.

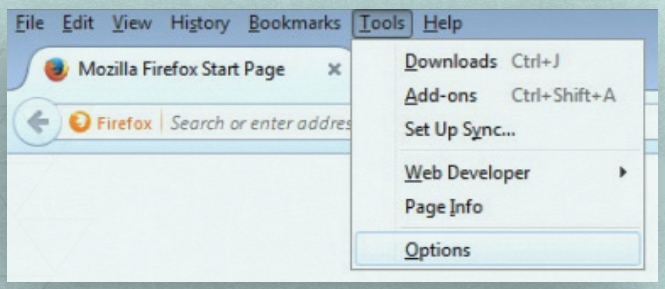
USING PRIVATE BROWSING OCCASIONALLY

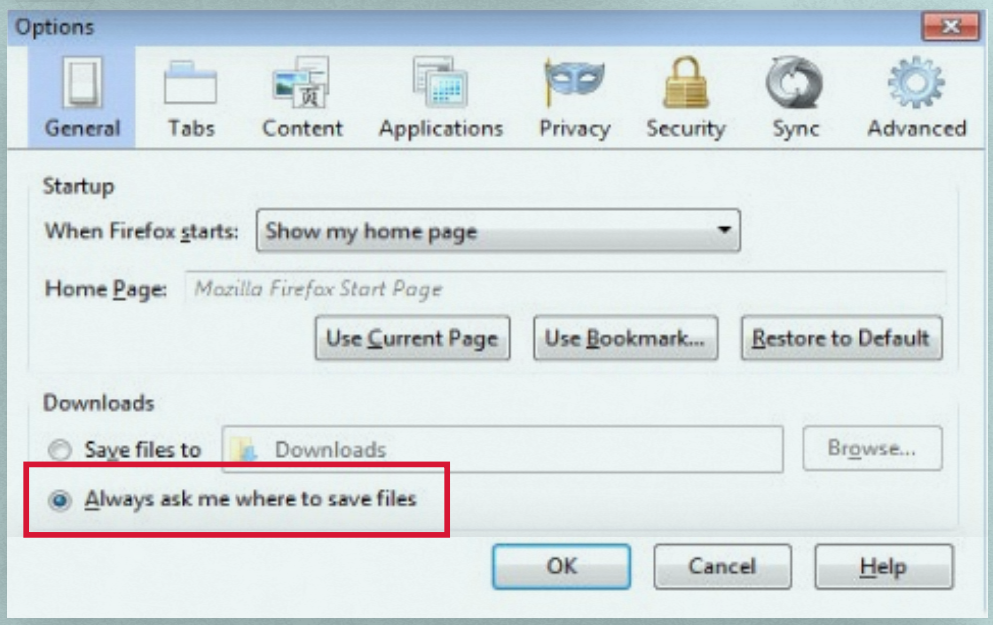
- Private Browsing' mode can also be used for a single window: **Open Firefox →** ☰ **→ New Private Window**



NOTE: Please make the necessary changes in case you are using a different version of Mozilla Firefox. To access the settings area, select **Tools and Options.**

- In the **Options** window, you need to access first the **General** category from the top menu.
- Under this section, you can select the option "**Always ask me where to save files**". This way, you won't have a web location trying to automatically save dangerous content to your computer. At the same time, you have the option to place suspicious content in a location where you can analyze it afterwards.





- In the Tracking section, check “**Tell sites that I do not want to be tracked**.” Selecting this option informs a website that you would like to opt-out of third-party tracking for advertising purposes. In the “**History**” section, choose your browser **Never remember history**, especially if you are using a computer from a public location or you know that computer is used by more people.

- For a more detailed configuration of your **History** section, select from the drop-down menu Use custom settings for history.

You can choose for example, to **always use private browsing mode**, which we highly recommend if you find yourself in a shared environment. Selecting this option ensures that when you finish your Mozilla Firefox session, all browsing, search and download history, and all the cookies are removed. For a more detailed configuration of your online browsing settings, choose from the available options.

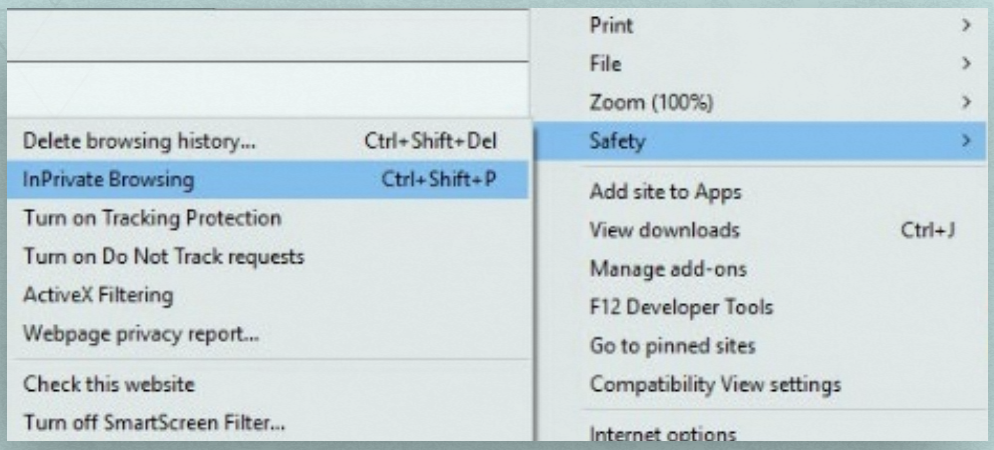
INTERNET EXPLORER

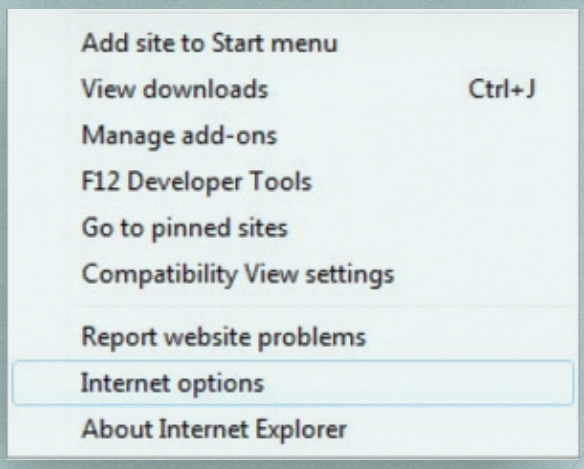
Microsoft Internet Explorer[27] is one of the most used web browsers in the world since it arrives pre-installed in our Windows operating systems. It supports Java and other active content, and it also implements ActiveX technology. While it is not the safest, and in fact, we do not recommend it at all, if you must use it, we recommend the following changes.

NOTE: To improve your overall security configuration in Windows 11, you need to access your browser settings area. Please make the necessary changes in case you are using a different version of Internet Explorer.

You can start a private browsing session in Internet Explorer (also called InPrivate Browsing).

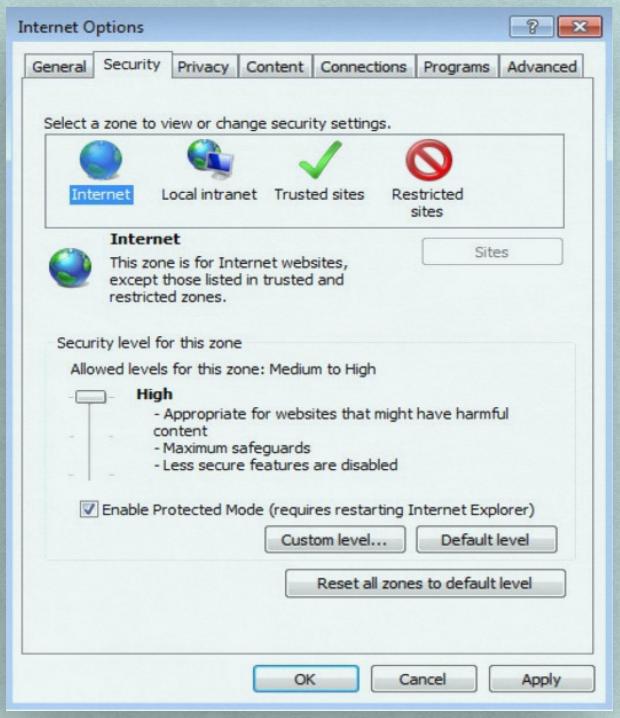
- Click on **Settings → Safety → InPrivate Browsing**. You can also use the keyboard shortcut Ctrl+Shift+P to launch it. Alternatively, you can right-click on the IE taskbar icon and select **Start InPrivate Browsing**.





[27] https://heimdalsecurity.com/blog/ultimate-guide-secure-online-browsing/

- To improve your Internet Explorer settings, access the **Internet Options** area.
- Go to the **Security** tab from the top menu.
- In this area you can locate: **Your trusted sites and security zones** for your computer. You also have the possibility to customize each security zone.



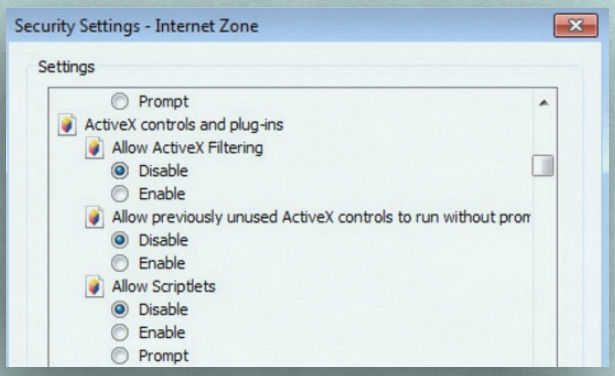
- For the Internet zone we recommend selecting the **High security level**. This selection will disable some browser features, such as ActiveX, Active scripting and Java, which can act as security breaches creating opening for threats to occur.

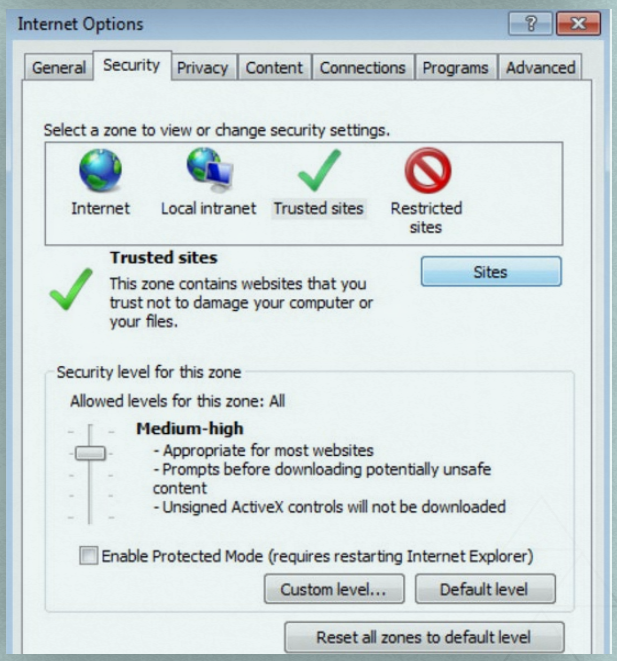
- To customize the security settings for a zone, choose the **Custom Level** option.

- In this area you can enable or disable specific security options for your selected Internet area. To return to the default levels for the selected Internet zone, simply click the “Reset” button.

- If we return to the initial window and click the **Trusted sites** option, we find a security zone for sites which are safe to access.

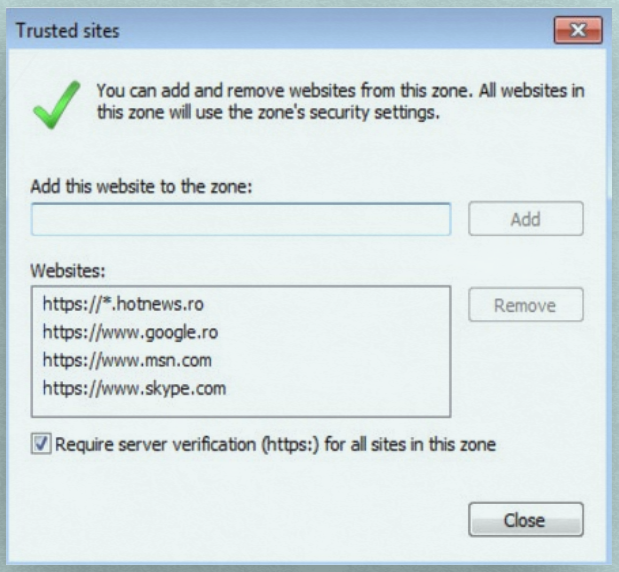
- If you consider a particular website to be a safe online location that can be trusted, you can choose to add it to this area. To do this, click **Sites**.





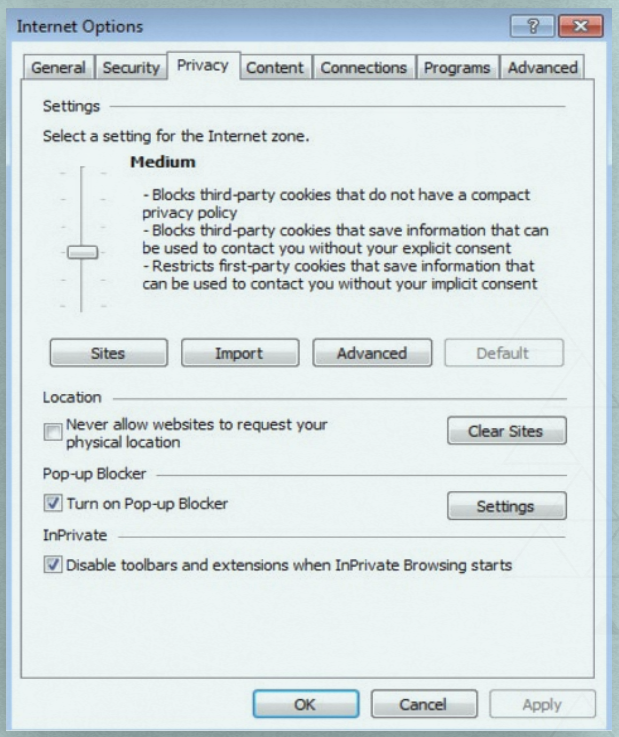
In this area, you can choose to add the website to a list of safe web locations. You can also choose to remove a site from the list.

The **Trusted sites** zone is useful if you chose the High security level for the Internet zone. Setting the High security level in the Internet zone causes browser features like ActiveX and Active scripting to stop functioning, and you may encounter some websites that don't function normally after that. To solve this, simply go to the Trusted sites zone and add the site that doesn't function as it should. Adding the site to the Trusted sites zone means that the website will work normally, by loading the browser features that are not allowed to function in the High security level.



The **Privacy** tab contains various settings for cookies in Internet Explorer.

Cookies are text files that are placed in your computer by websites you access. They contain data and information the sites store about your browsing habits or your preferences. In this space you can use the preset privacy rules available by using the slider and select one of the settings for your Internet zone. For example, choosing the High level will block cookies from most websites.



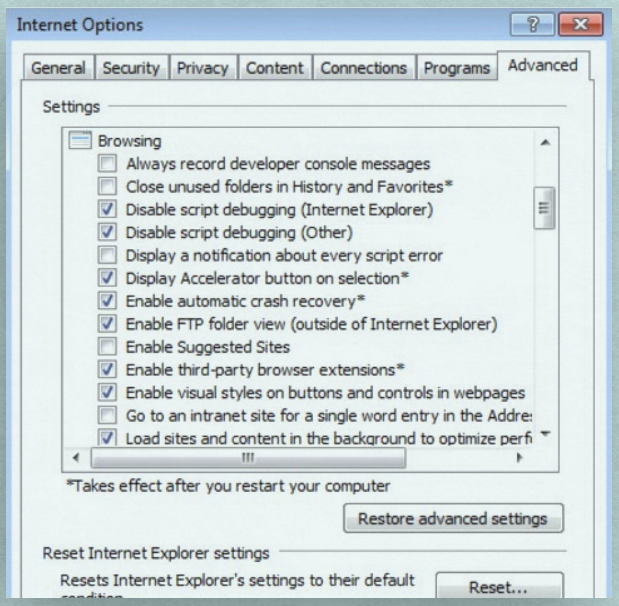
If you want to make modifications, you have other additional options.

To improve your security, select the **Advanced** button available.

This area contains settings that apply to all security zones.

- From this tab, we recommend you to **uncheck Enable third-party browser extensions** option.

If you leave it checked, different types of toolbars and addons are enabled on your system and this may affect your privacy. Many add-ons have proved to monitor your browsing habits or even attempt to collect private data from your browser.



EXTENSIONS FOR A SAFER ONLINE SESSION

Adjusting your browser settings will enhance its security to a certain degree, but for complete protection installing further security extensions will be needed.[28]

Browser extensions are small software programs that improve and personalize your online experience.

With so many extensions (or add-ons) out there, it is difficult to make the right choice. Some of them address your need for privacy, others, your need for protection and security while you access your online tax information or log into your banking account, for example.

When using a browser extension you have greater control over your browser behavior. You can block ads from some websites and pop-ups that may act like carriers for financial and data stealing malware. At the same time, you have the possibility to block others from breaching your privacy settings.

TIP: We want you to also be aware how these extensions work to provide security and also how to test these extensions

PRIVACY BADGER

EFF's Privacy Badger is a browser add-on that stops advertisers and other third-party trackers from secretly tracking where you go and what pages you look at.

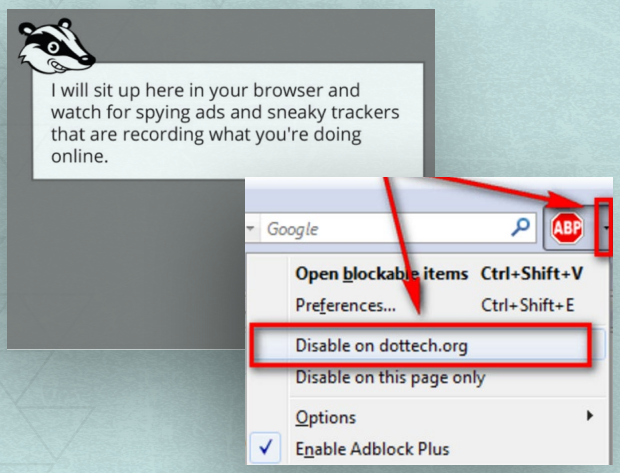
If an advertiser seems to be tracking you across multiple websites without your permission, Privacy badger automatically blocks that advertiser from loading any more content.

To the advertiser, it's like you suddenly disappeared. Privacy Badger was born out of the desire to be able to recommend a single extension that would automatically analyze and block any tracker or ad that violated the principle of user consent.

Although extensions like Disconnect, Adblock Plus, Ghostery work well, (in fact Privacy Badger is based on the ABP code!), all of them require some custom configuration to block non-consensual trackers and could have some conflict of interests in their business model.

[28] https://heimdalsecurity.com/blog/ultimate-guide-secure-online-browsing/

The internet freedom non-profit EFF developed Privacy Badger to be heuristic, which means it gets better at creating blacklists and blocking websites as time goes on, making it unique when compared to other blockers. Out of the box, Privacy Badger won't block nearly as many third-party requests as the commercial options but it does get better over time with frequent use. It will discover which hosts to block, it will also create a whitelist for important sites that are visited on a regular basis.

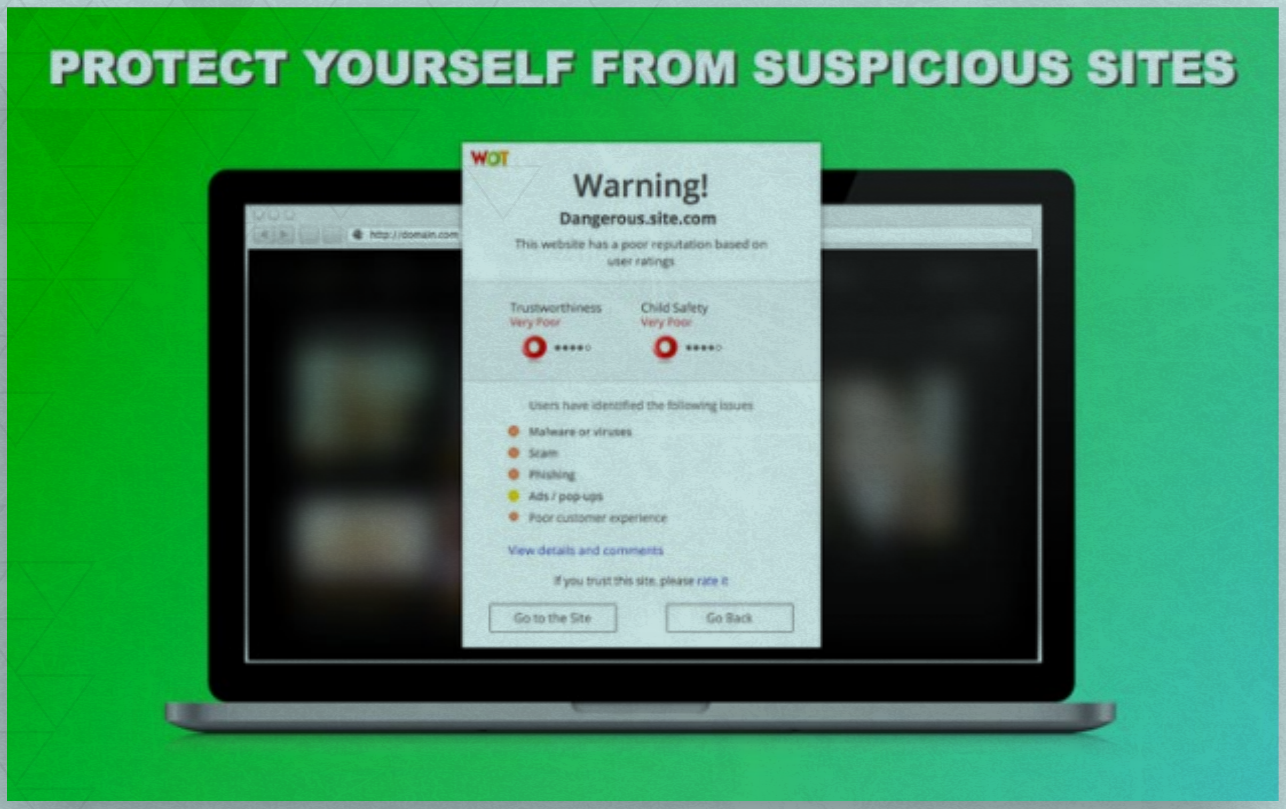


HTTPS EVERYWHERE

HTTPS Everywhere is an extension available for Mozilla Firefox and Google Chrome created by the Electronic Frontier Foundation.

WEB OF TRUST

Available for Mozilla Firefox, Google Chrome, and Internet Explorer, **Web Of Trust** ranks websites by reputation based on the amount of malware they host or tracking cookies they contain. Since it's an informational tool, it will not block ads, but its valuable information allows you to make an informed decision on your course of action.


PROTECT YOURSELF FROM SUSPICIOUS SITES
WOT
Warning!
Dangerous.site.com
This website has a poor reputation based on user ratings
Trustworthiness
Very Poor
Child Safety
Very Poor
Users have identified the following issues
Malware or viruses
Scam
Phishing
Ads / pop-ups
Poor customer experience
View details and comments
If you trust this site, please rate it
Go to the Site
Go Back

WHAT ABOUT SEARCH ENGINES?

Search Engines are big money for Google and Microsoft because what you search tells a lot about you and what your concerns are. Imagine if I search in one session about the cost of diapers, maternity centers, and child care, one could easily infer that I was thinking about children. Similarly if you are about to hold a protest and you search about non-violent direct action or the number for the lawyers guild, one could then infer you were thinking about a protest or some direct action. In essence who ever owns your search history owns you!

This is why choosing a search engine that does not track you is important. Currently all of your searches on engines like Google and Bing are used to help inform and create a very large Data shadow about you and your concerns. Imagine what that could reveal and how it could be used against you. The best option then is to use search engines that do not track you.

We recommend **DuckDuckGo**[29], but for folks who want to see a comparison the next page has some great options to explore. Try them and try them often. Once you find one that works switch!

[29] https://duckduckgo.com

DuckDuckGo	searX	startpage
Cookies: Does not use cookies by default	**Cookies:** Does not use cookies by default	**Cookies:** Does not use identifying cookies
Tracking policy: Does not track and profile users	**Tracking policy:** Does not track and profile users	**Tracking policy:** Does not store its users' IP addresses
Personal information: Does not collect or store	**Personal information:** Does not collect or store	**Personal information:** does not collect or share personal data
Encryption: Yes, HTTPS	**Encryption?** Yes, HTTPS	**Encryption?** Yes, HTTPS
	Owned and managed by: La Quadrature du Net	**Extra:** Offers a free proxy service that allows for anonymous online browsing