

Protection from Web tracking via browsers & browser extensions

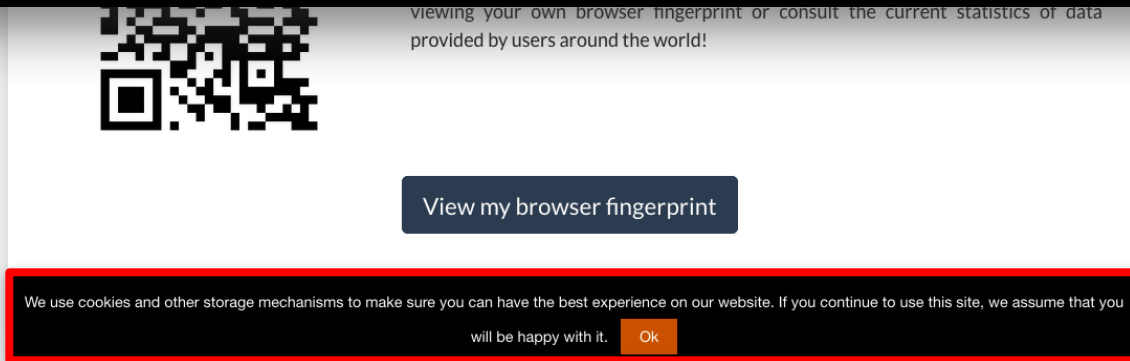
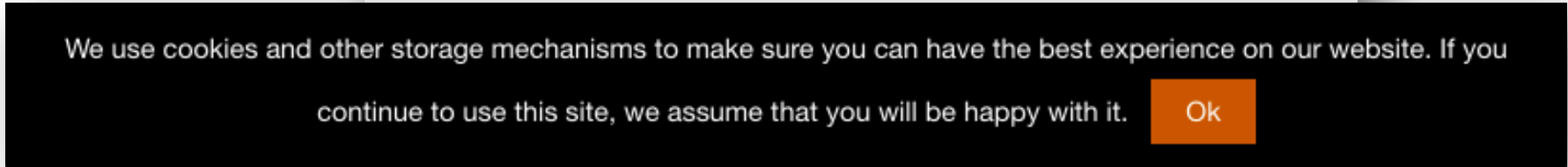
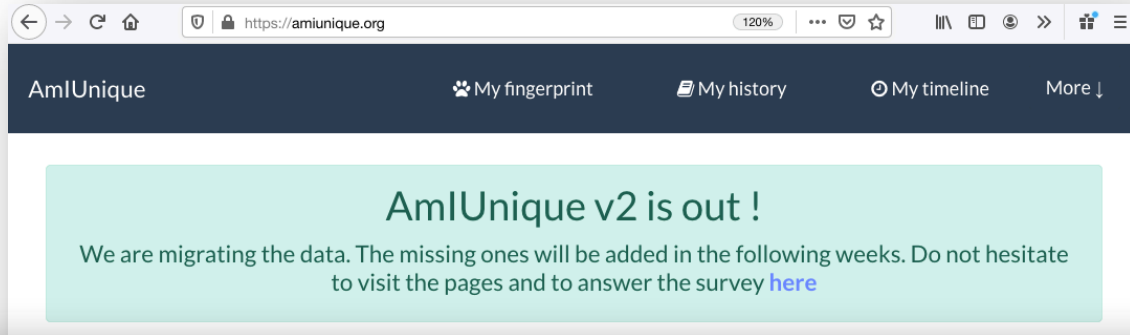
Nataliia Bielova

Nataliia.bielova@inria.fr

Security and ethical aspects of data

Université Cote d'Azur

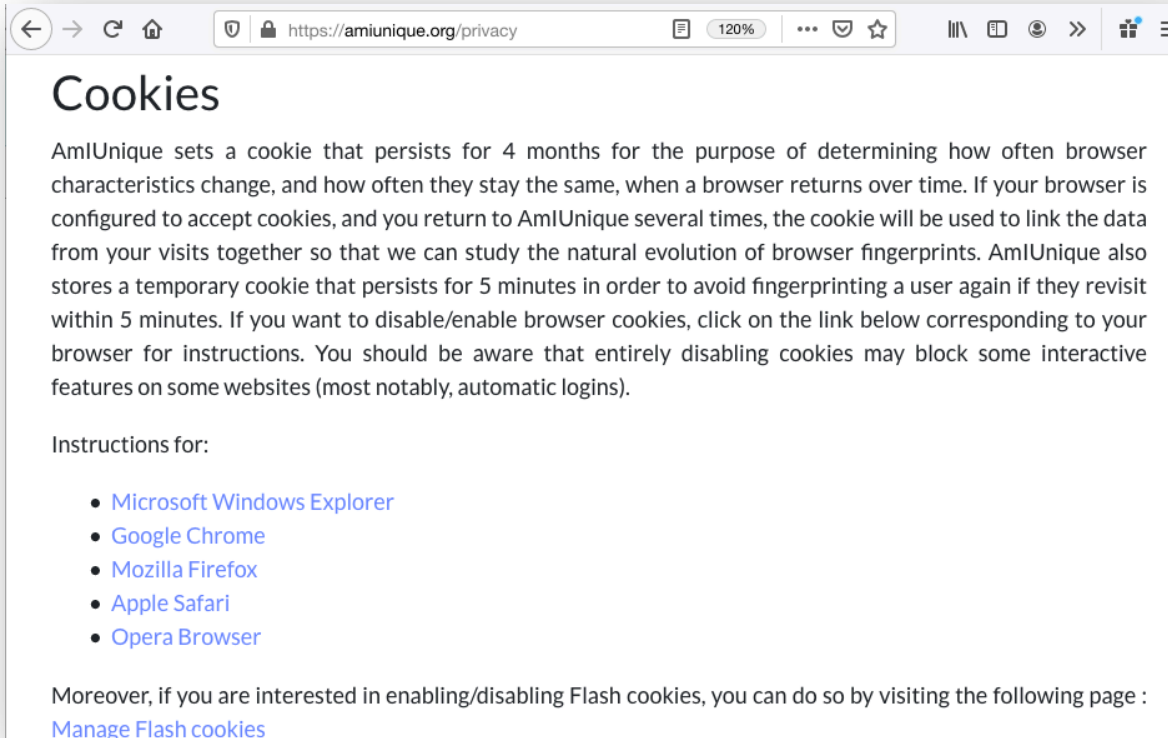
I see a cookie banner. Does it mean they ask my consent?



Which cookies require consent?

This depends on the **purpose** of the cookie....

Where to find a purpose of a cookie? In a privacy policy or cookie policy!



The screenshot shows a web browser window with the address bar displaying 'https://amionique.org/privacy'. The page title is 'Cookies'. The main content explains that AmlUnique sets a cookie that persists for 4 months to track browser characteristics and link data from multiple visits. It also mentions a temporary cookie for 5 minutes to avoid fingerprinting. A link is provided for instructions on disabling/enabling browser cookies. Below this, a list of browser instructions is shown, including links for Microsoft Windows Explorer, Google Chrome, Mozilla Firefox, Apple Safari, and Opera Browser. At the bottom, there is a link to 'Manage Flash cookies'.

Cookies

AmlUnique sets a cookie that persists for 4 months for the purpose of determining how often browser characteristics change, and how often they stay the same, when a browser returns over time. If your browser is configured to accept cookies, and you return to AmlUnique several times, the cookie will be used to link the data from your visits together so that we can study the natural evolution of browser fingerprints. AmlUnique also stores a temporary cookie that persists for 5 minutes in order to avoid fingerprinting a user again if they revisit within 5 minutes. If you want to disable/enable browser cookies, click on the link below corresponding to your browser for instructions. You should be aware that entirely disabling cookies may block some interactive features on some websites (most notably, automatic logins).

Instructions for:

- [Microsoft Windows Explorer](#)
- [Google Chrome](#)
- [Mozilla Firefox](#)
- [Apple Safari](#)
- [Opera Browser](#)

Moreover, if you are interested in enabling/disabling Flash cookies, you can do so by visiting the following page : [Manage Flash cookies](#)

Exercise – BONUS in the final evaluation!

- Look at your cookie storage in your browser.
- Pick one domain and cookie
- Find a cookie policy clearly explaining what is the purpose of the cookie.
- Document all these steps in the following table (example for amiunique.org)
- Repeat for a different domain/cookie if no purpose is found.
- Send the final document along with the paper report.

Cookie domain	amiunique.org
Cookie name	AmlUniqueld
Cookie policy	https://amiunique.org/privacy
Purpose of a cookie	the purpose of determining how often browser characteristics change, and how often they stay the same, when a browser returns over time.

Purposes exempted of consent	Purposes needed of consent
Local Analytics	Non-local analytics
Session user input	Advertising
User-security for a service explicitly requested by the user	User-security for a service not explicitly requested by the user
Social media plugin for a functionality explicitly requested by the user	Social media plugin for a functionality not requested by the user
Session Authentication	Persistent Authentication
Short-term User Interface Customization (or personalization and design cookies)	Long-term User Interface Customization
Load Balancing	
Session Multimedia Content Player	

OK, let's simplify...

- Does the cookie description falls into one of these categories? If yes, which one?
 - Analytics
 - Advertising
 - Customization
 - Authentication
 - Social media
 - Load balancing
 - User Input
 - User security

Exercise (2)

- Read the following cookie descriptions automatically extracted from the cookie policies.
- Try to link them to one of the proposed categories...

<https://framaforms.org/cookie-labelling-1576226769>

Protection from Web tracking

Plugins and extensions (add-ons)

- **Plugins** were created to render the content not supported by the browser

- Flash Java



- **Extensions (add-ons)** add or modify the default behavior of the browsers

- Adblock Plus LastPass Pinterest



LastPass...



Extensions for privacy protection

- Extensions “**ad-blocking**”
 - Block visible advertisements
- Extensions “**tracking-blocking**”
 - Block invisible tracking
 - ✓ Example : request for an invisible image with third-party cookies



Ad-blocking ≠ tracking-blocking!

« Ad-blocking » extensions

• AdBlock



AdBlock Plus

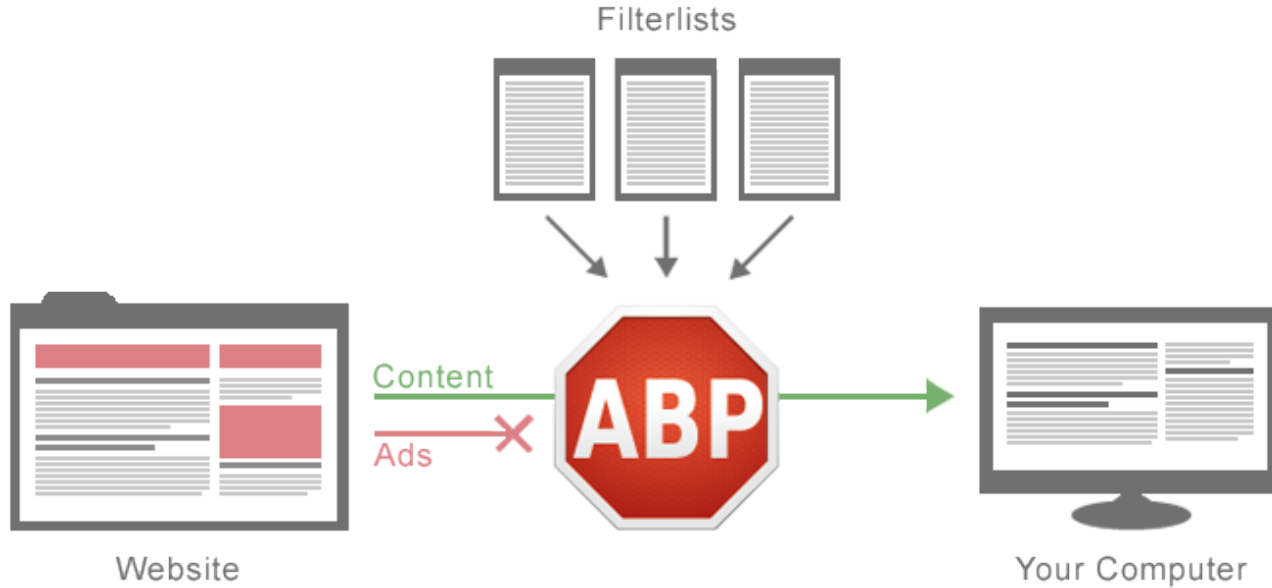


uBlock Origin



- Use the same consumer lists that detect ad companies
- Block requests to domains presented in the lists

How does AdBlock Plus work?



<https://adblockplus.org/about>

Configuration of AdBlock Plus

ABP
Adblock **Plus**
Settings

General

Whitelisted websites

Advanced

Help

CONTRIBUTE

[About Adblock Plus](#)

General

Determine what Adblock Plus shows and hides on websites

PRIVACY & SECURITY

- Block additional tracking [?](#)
- Block social media icons tracking [?](#)

ACCEPTABLE ADS

Allow Acceptable Ads

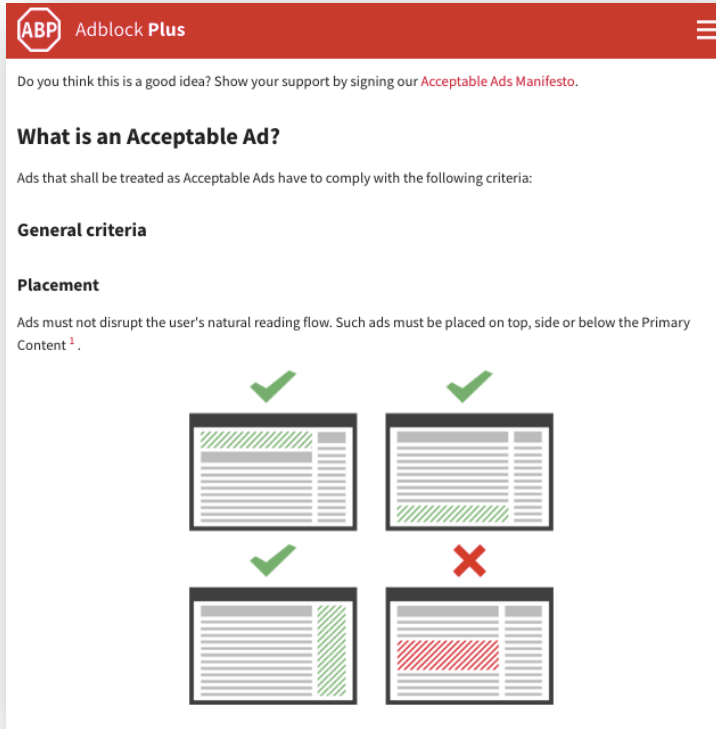
Acceptable Ads are nonintrusive ads. They are the middle ground between ad blocking and supporting content that generates revenue for website owners.

Acceptable Ads are not annoying and do not interfere with the content you are viewing. [Read more about the Acceptable Ads criteria](#)

Only allow ads without third party tracking **NEW**

Certain “acceptable ads”
are still allowed

Which ads are « acceptable »?



ABP Adblock Plus

Do you think this is a good idea? Show your support by signing our [Acceptable Ads Manifesto](#).

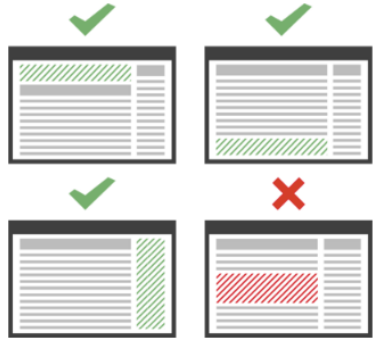
What is an Acceptable Ad?

Ads that shall be treated as Acceptable Ads have to comply with the following criteria:

General criteria

Placement

Ads must not disrupt the user's natural reading flow. Such ads must be placed on top, side or below the Primary Content¹.



- An action initiated by Eyeo (Ad Block owner)
- Which **ad is acceptable** ?
 - Well-placed, well-identified, not too big size...
- Large entities **have to pay** to show the ads even if their ads are already « acceptable »!

Configuration of AdBlock Plus

The screenshot shows the AdBlock Plus settings interface. On the left is a sidebar with the ABP logo and 'Adblock Plus Settings'. The main content area is titled 'General' and includes a description: 'Determine what Adblock Plus shows and hides on websites'. Below this are three sections: 'PRIVACY & SECURITY' with two unchecked checkboxes for 'Block additional' and 'Block social med'; 'ACCEPTABLE ADS' with a checked checkbox for 'Allow Acceptable Ads' and a link to 'Read more about the Acceptable Ads criteria'; and another unchecked checkbox for 'Only allow ads without third-party tracking' with a 'NEW' badge and a 'Learn more' link. A 'CONTRIBUTE' button and a link to 'About Adblock Plus' are also visible in the sidebar.

Tracking **is not blocked** by default !

Ad-blocking ≠ tracking-blocking!

Ad-blocking ≠ tracking-blocking!



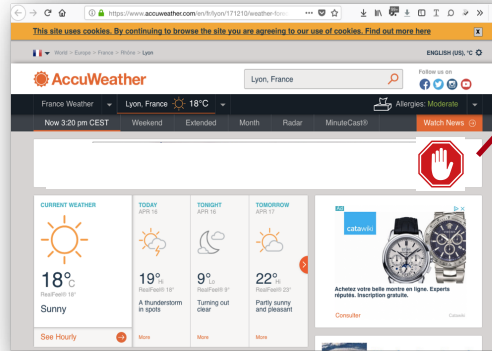
- Extensions block ads but **do not block all the tracking**



cookies stockés

tracker.com: id=123

http://accuweather.com



cookie: id=123

tracker.com

9h25, 27 june 2018 :
user 123 likes



10h00, 30 june 2018 :
user 123 visited
accuweather.com

profil

Tracking-blocking extensions

- How to detect a tracker ?
- Solution 1 : use **a liste of known companies** for tracking
- Solution 2 : use **rules based on the behaviour** of potential trackers
 - Example : third-party content that sets third-party cookies with a unique identifier

```
"Facebook": {  
  "http://www.facebook.com/": [  
    "facebook.com",  
    "facebook.de",  
    "facebook.fr",  
    "facebook.net",  
    "fb.com",  
    "atlassolutions.com",  
    "friendfeed.com"  
  ]  
}
```

Tracking-blocking extensions

- Extensions use **their own lists of known companies** for tracking

Disconnect



- Blocks from tracking upon installation

Ghostery



- **Doesn't block from tracking by default!**

Ghostery: activate blocking of trackers

The screenshot shows the Ghostery web interface. On the left is a navigation menu with items: Global Blocking, Trust & Restrict, General Settings, Notifications, Opt in, Purple Box, and Account. The main content area is titled 'GLOBAL BLOCKING' and features a search bar labeled 'Search by tracker', an 'Expand All' button, and a dropdown menu currently set to 'All'. Below these are several categories of trackers, each with an icon, a name, and a count of trackers:

- Advertising (1750 TRACKERS)
- Site Analytics (629 TRACKERS)
- Customer Interaction (277 TRACKERS)
- Social Media (100 TRACKERS)
- Essential (64 TRACKERS)

In the top right corner of the main content area, there is a 'Block All' button, which is circled in red. A red arrow points from this button to a callout box on the right.

Click on “Block All” to be protected from known trackers!

Tracking-blocking extensions

- One extension uses **rules based on the behaviour** of potential trackers

Privacy Badger



- How to detect cookies that contain an identifier?
 - Solution : find third-party cookies that are never shared between the users

Do browser extensions block all trackers?

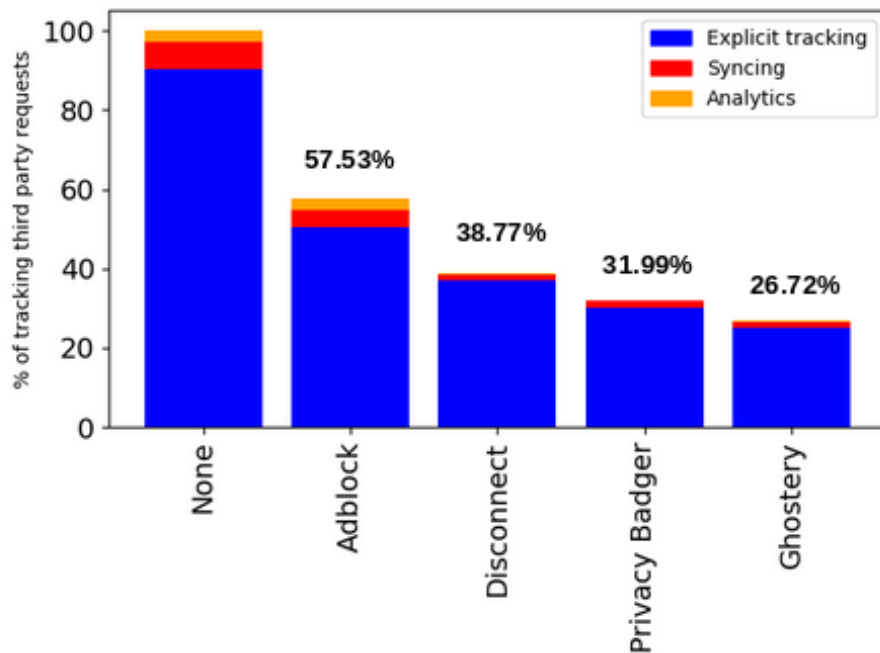
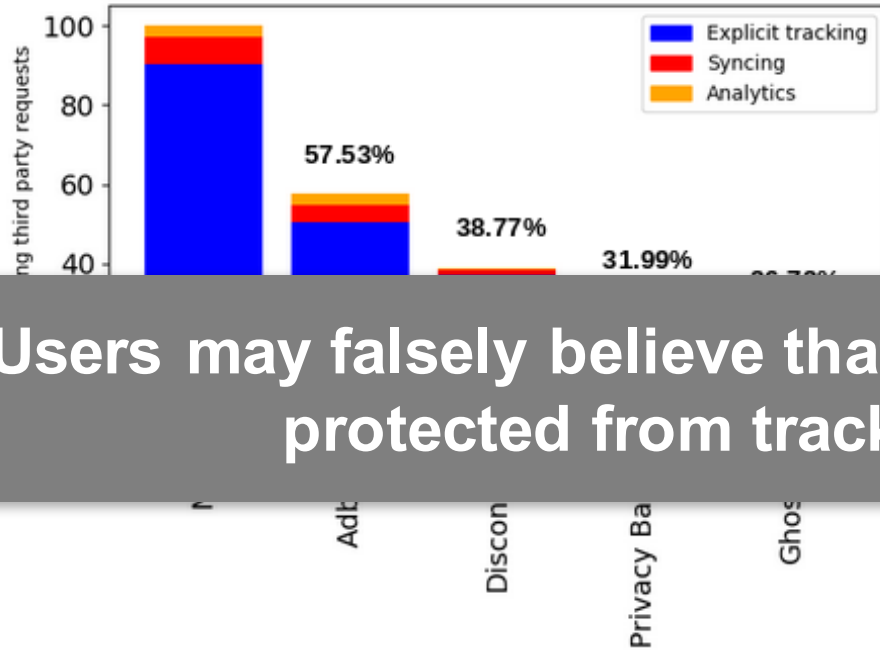


Fig. 12. Third party requests allowed by privacy protecting browser extensions out of 4,519,975 tracking requests.

Do browser extensions block all trackers?



Users may falsely believe that they are fully protected from tracking!

Fig. 12. Third party requests allowed by privacy protecting browser extensions out of 4,519,975 tracking requests.

Firefox uses the same protection as Disconnect



General

Home

Search

Privacy & Security

Firefox Account

Tracking Protection

Tracking Protection blocks online trackers that collect your browsing data across multiple websites. [Learn more about Tracking Protection and your privacy](#)

Use Tracking Protection to block known trackers

Always

Only in private windows

Never

Exceptions...

Change Block List...

- **Firefox uses the same list of known trackers** as Disconnect
- No need to install Disconnect with Firefox if tracking protection is always on!

Browsers with integrated tracking protection

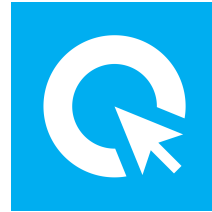
Brave



- **Third-party cookies are blocked** upon installation
- Tracking protection by **lists of** AdBlock et Disconnect

<https://brave.com/index/>

Cliqz



- **Third-party cookies are blocked** upon installation
- Tracking protection based on **the behaviour of third-party requests**

<https://cliqz.com/fr/>

What about Private browsing mode?



You've gone incognito

Pages you view in incognito tabs won't stick around in your browser's history, cookie store, or search history after you've closed all of your incognito tabs. Any files you download or bookmarks you create will be kept.

However, you aren't invisible. Going incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit.

[LEARN MORE](#)



Private Browsing with Tracking Protection

When you browse in a Private Window, Firefox **does not save**:

- visited pages
- searches
- cookies
- temporary files

Firefox **will save** your:

- bookmarks
- downloads

Private Browsing **doesn't make you anonymous** on the Internet. Your employer or Internet service provider can still know what page you visit.



Tracking Protection

Some websites use trackers that can monitor your activity across the Internet. With Tracking Protection Firefox will block many trackers that can collect information about your browsing behavior.

[See how it works](#)

How Private mode works?

- browsing history
- cookies
- searches
- ...

are stored only in the current separate “session”



Private mode is not so private...

- **Doesn't block** third-party cookies
 - neither in Firefox with Tracking protection ON
 - nor in Chrome
- **Browsing profile can be merged** with non-private session
 - if you log in inside and outside of private mode
 - if you visit websites that use browser fingerprinting

In general, private
browsing mode **does not**
protect from tracking!

Conclusion

- **Ad-blocking ≠ tracking-blocking!**
 - Extensions that block ads do not necessarily block tracking
- **Installation ≠ protection**
 - Always double-check that all the protecting options are chosen!
- **Advices to protect from stateful tracking:**
 - Browsers that protect by default (Brave, Cliqz)
 - Browsers with protection integrated (Firefox)
 - Combination of various extensions (Disconnect, Ghostery, Privacy Badger)

