CSE 410 Spring 2025
Privacy-Enhancing Technologies

Marina Blanton

Department of Computer Science and Engineering
University at Buffalo

Lecture 2: Web Tracking

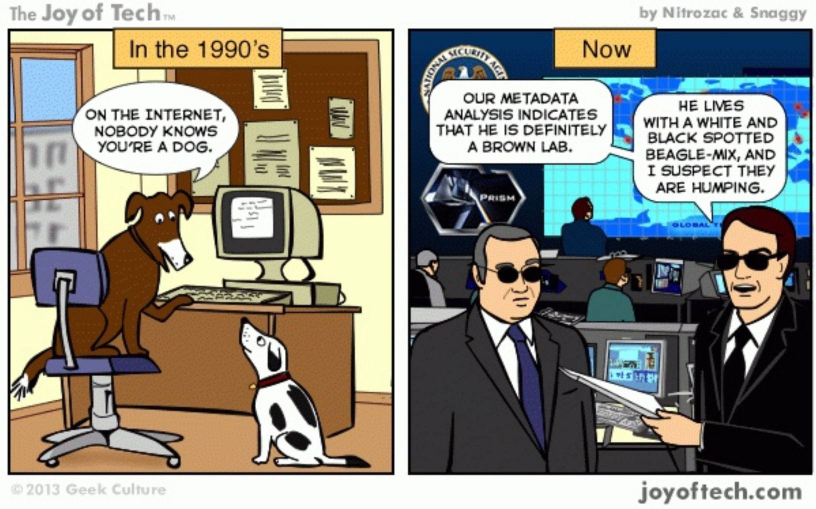
Anonymity on the Internet

Often if we don't specify our name or other personal information, our communication seems anonymous

Anonymity on the Internet

"On the Internet, nobody knows you're a dog."

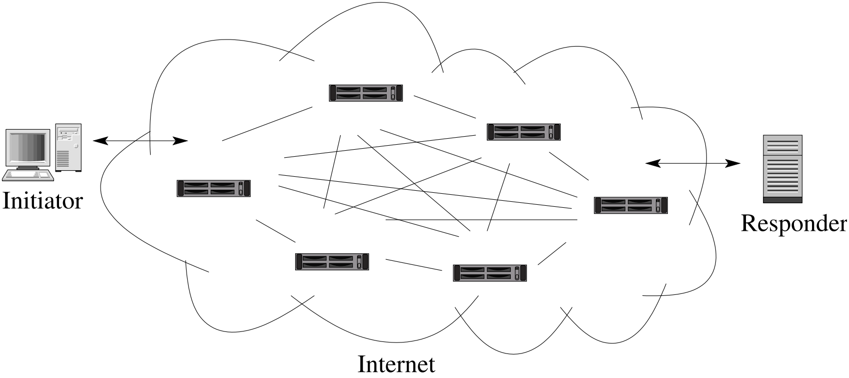
Anonymity on the Internet


The Joy of Tech™
by Nitrozac & Snaggy
In the 1990's
ON THE INTERNET, NOBODY KNOWS YOU'RE A DOG.
Now
NATIONAL SECURITY AGENCY
OUR METADATA ANALYSIS INDICATES THAT HE IS DEFINITELY A BROWN LAB.
PRISM
HE LIVES WITH A WHITE AND BLACK SPOTTED BEAGLE-MIX, AND I SUSPECT THEY ARE HUMPING.
© 2013 Geek Culture
joyoftech.com

Anonymity on the Internet

- Simple examples of why we are not anonymous:
  - if we read a web page, the web server knows what address the request is coming from
  - it we connect to a chat channel, the server knows what address we are coming from
  - if you send an encrypted message, the endpoints can still be recovered
- The more complex reality is that there is a great deal of tracking on the web beyond mere recovery of addresses

Basic Definitions



Basic Definitions

- Internet Protocol (IP) is a low-level communication standard that specifies how data is to be transmitted from one machine to another

- IP address is an address of a computer or device connected to the Internet
  - IPv4 is a 4-byte (32-bit) address x.x.x.x, where each x is in the range 0–255

- HTTP (and HTTPS) is a higher-level protocol that standardizes serving web pages

- JavaScript is a programming language for programs embedded in a web page and executed by the browser
  - allows for web pages to be dynamically generated and customized at the client side

Basic Definitions

- HTTPS enhances HTTP with security guarantees
  - HTTPS authenticates at least one end (the server)
  - it provides confidentiality and integrity of transmitted data
    - confidentiality means outsiders cannot learn any information about what you are sending and receiving
    - integrity means outsiders cannot modify transmitted data undetected
  - confidentiality is achieved by means of strong encryption
    - without the right decryption key, a ciphertext looks like a sequence of random bits
    - the same message encrypted with the same key appears different every time
    - this means one cannot tell anything about encrypted content (besides the length)

Basic Definitions

- What does HTTPS mean?
  - parties monitoring your communication cannot see encrypted content
  - they are able to see unencrypted data
    - information needed to route the communication and establish a secure connection
  - the receiving server can obviously see everything

Web Tracking

- When you connect to a web server, the server can immediately observe the following information:
  - the client's IP address
  - HTTP headers (including the requested URL, HTTP version, etc.)
  - HTTP body if present
  - information exchanged if HTTPS is used
- Significantly more can be gathered

Fingerprinting

Browser fingerprinting refers to the process of collecting and using information about a remote computing device for the purpose of its identification

- Fingerprints can be used to fully or partially identify a device or individual users using the device
- Browser fingerprinting is a powerful method to collect information about clients without their knowledge
- This was enabled by recent changes in the HTML standard
- It is done by having a JavaScript run in your browser and collect information about your system

Fingerprinting

Information collected by fingerprinters includes:

- browser type and version
- operating system
- device model
- active plugins
- timezone
- language
- screen resolution
- fonts installed on your computer
- information about network connection
- other active settings

Fingerprint Uniqueness

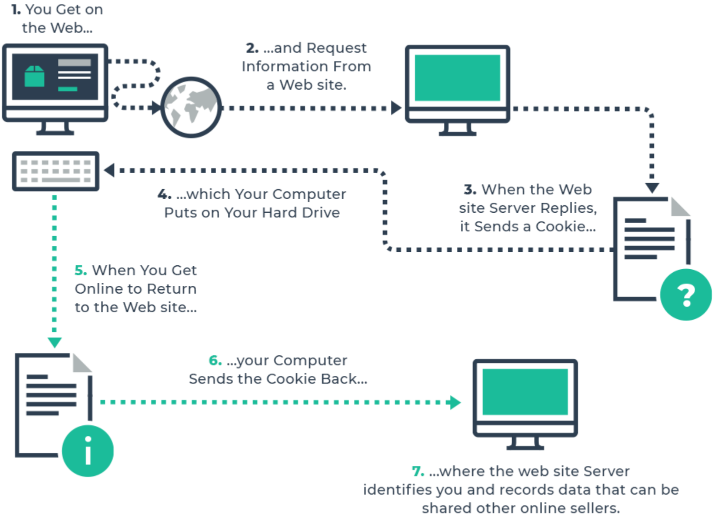
It appears that none of the information above is identifying

However, together various bits of information typically result in a unique profile

One can easily be unique among hundreds of thousands of users at any given time and among many millions long-term

- https://coveryourtracks.eff.org/static/browser-uniqueness.pdf describes a sample study

Cookies



1. You Get on the Web...

2. ...and Request Information From a Web site.

3. When the Web site Server Replies, it Sends a Cookie...

4. ...which Your Computer Puts on Your Hard Drive

5. When You Get Online to Return to the Web site...

6. ...your Computer Sends the Cookie Back...

7. ...where the web site Server identifies you and records data that can be shared other online sellers.

Image from pixelprivacy.com

Cross-Site Cookies

A cookie is a persistent piece of information stored on your computer

- it is loaded every time you visit a website
- it can store information about your prior activity, habits, interests, etc.

Cross-site cookies unable a form of tracking where your browsing activities and interests are tracked at many websites

- they form a rich profile of your activities
- they are typically set by third parties such as advertisers and analytics companies

Social Media Trackers

Social networks use trackers to record what you do, see, and watch online

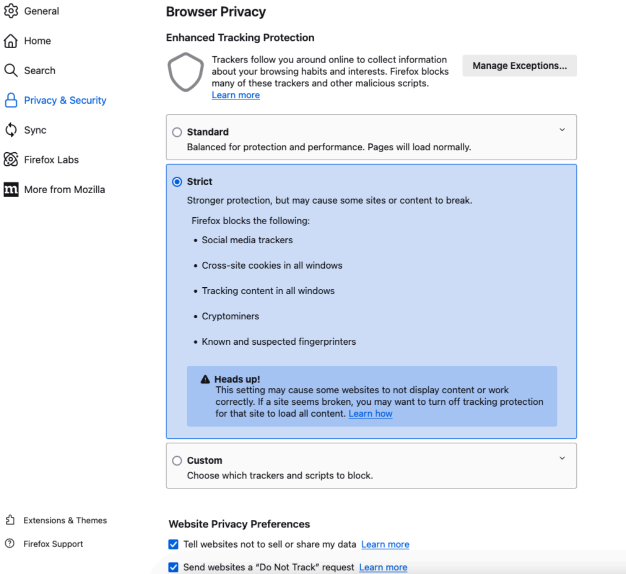
Together with the information already known about users, it allows for more effective ad targeting

Information can be collected even if you don't use social networks

What Can You Do?

- Step 1: Learn
  - Learn about, examine, and modify if desirable your web browser's security and privacy settings
  - Learn about what privacy protection mechanisms your and other browsers offer

Firefox Example



Browser Privacy

Enhanced Tracking Protection

Trackers follow you around online to collect information about your browsing habits and interests. Firefox blocks many of these trackers and other malicious scripts. Learn more

○ **Standard**
Balanced for protection and performance. Pages will load normally.

● **Strict**
Stronger protection, but may cause some sites or content to break.

Firefox blocks the following:

- Social media trackers
- Cross-site cookies in all windows
- Tracking content in all windows
- Cryptominers
- Known and suspected fingerprinters

Heads up!
This setting may cause some websites to not display content or work correctly. If a site seems broken, you may want to turn off tracking protection for that site to load all content. Learn how

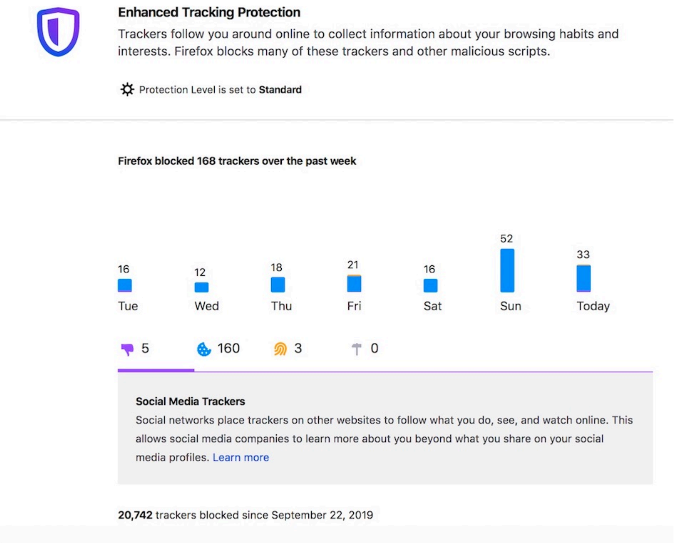
○ **Custom**
Choose which trackers and scripts to block.

Website Privacy Preferences

☑ Tell websites not to sell or share my data Learn more

☑ Send websites a "Do Not Track" request Learn more

Firefox Example



Enhanced Tracking Protection

Trackers follow you around online to collect information about your browsing habits and interests. Firefox blocks many of these trackers and other malicious scripts.

Protection Level is set to **Standard**

Firefox blocked 168 trackers over the past week

5 160 3 0

Social Media Trackers

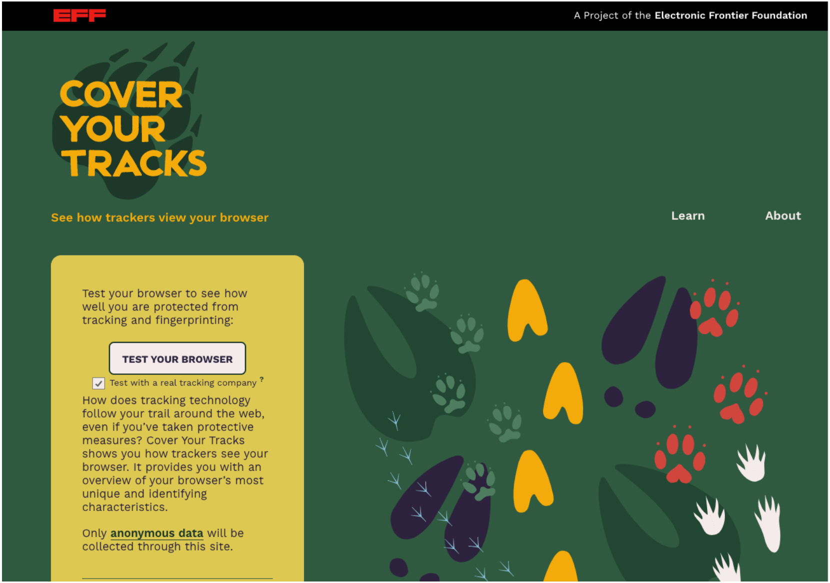
Social networks place trackers on other websites to follow what you do, see, and watch online. This allows social media companies to learn more about you beyond what you share on your social media profiles. Learn more

20,742 trackers blocked since September 22, 2019

What Can You Do?

- Step 1: Learn
  - Learn about, examine, and modify if desirable your web browser's security and privacy settings
  - Learn about what privacy protection mechanisms your and other browsers offer
- Step 2: Improve
  - Test how unique you are

Cover Your Tracks Test https://coveryourtracks.eff.org/


EFF
A Project of the Electronic Frontier Foundation
COVER YOUR TRACKS
See how trackers view your browser
Learn
About
TEST YOUR BROWSER

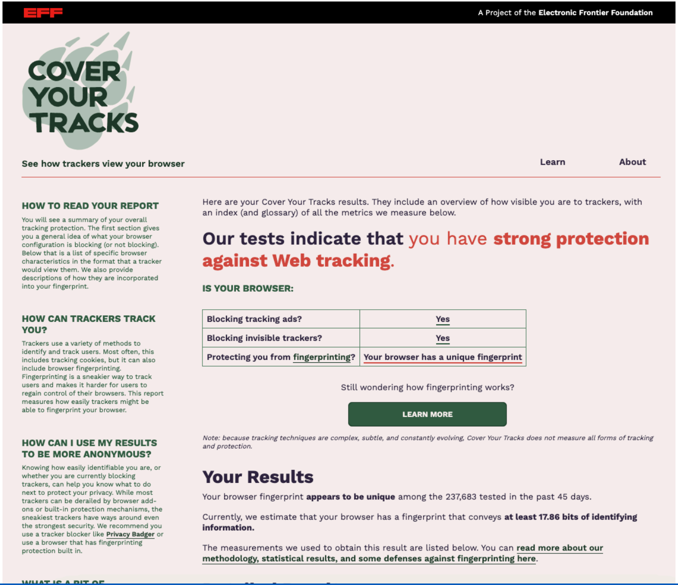
Test your browser to see how well you are protected from tracking and fingerprinting:

☑ Test with a real tracking company ?

How does tracking technology follow your trail around the web, even if you've taken protective measures? Cover Your Tracks shows you how trackers see your browser. It provides you with an overview of your browser's most unique and identifying characteristics.

Only anonymous data will be collected through this site.

Cover Your Tracks Test https://coveryourtracks.eff.org/



EFF

A Project of the **Electronic Frontier Foundation**

COVER YOUR TRACKS

See how trackers view your browser

Learn About

HOW TO READ YOUR REPORT

You will see a summary of your overall tracking protection. The first section gives you a general idea of what your browser configuration is blocking (or not blocking). Below that is a list of specific browser characteristics in the format that a tracker would view them. We also provide descriptions of how they are incorporated into your fingerprint.

HOW CAN TRACKERS TRACK YOU?

Trackers use a variety of methods to identify and track users. Most often, this includes tracking cookies, but it can also include browser fingerprinting. Fingerprinting is a sneakier way to track users and makes it harder for users to regain control of their browsers. This report measures how easily trackers might be able to fingerprint your browser.

HOW CAN I USE MY RESULTS TO BE MORE ANONYMOUS?

Knowing how easily identifiable you are, or whether you are currently blocking trackers, can help you know what to do next to protect your privacy. While most trackers can be derailed by browser add-ons or built-in protection mechanisms, the sneakiest trackers have ways around even the strongest security. We recommend you use a tracker blocker like **Privacy Badger** or use a browser that has fingerprinting protection built in.

WHAT IS A BIT OF

Here are your Cover Your Tracks results. They include an overview of how visible you are to trackers, with an index (and glossary) of all the metrics we measure below.

Our tests indicate that you have **strong protection against Web tracking**.

IS YOUR BROWSER:

Blocking tracking ads?	Yes
Blocking invisible trackers?	Yes
Protecting you from fingerprinting?	Your browser has a unique fingerprint

Still wondering how fingerprinting works?

LEARN MORE

Note: because tracking techniques are complex, subtle, and constantly evolving, Cover Your Tracks does not measure all forms of tracking and protection.

Your Results

Your browser fingerprint **appears to be unique** among the 237,683 tested in the past 45 days.

Currently, we estimate that your browser has a fingerprint that conveys **at least 17.86 bits of identifying information.**

The measurements we used to obtain this result are listed below. You can **read more about our methodology, statistical results, and some defenses against fingerprinting here**.

Measuring Uncertainty

- Given a random variable X, self-information or surpisal of x is
$$I(X = x) = -\log_2 \Pr[X = x]$$
- Entropy H measures the amount of information (or amount of uncertainty) of a source
$$H(X) = -\sum_{x \in \mathcal{X}} \Pr[X = x] \log_2 \Pr[X = x]$$
  - it is the expected value of surprisal across all values
  - both surpisal and entropy are measured in bits

Measuring Uncertainty

- Think of entropy as the minimum number of bits required to encode all possible values
- If there are n choices and they are all equally probable, then

$$H(X) = -\sum_{i=1}^{n} \frac{1}{n} \log_2 \frac{1}{n} = -\log_2 \frac{1}{n} = \log_2 n$$

- Think of suprisal as the amount of information about objects with that value

Measuring Uncertainty

- Example:
    - there are 64 web users: 32 have Chrome, 16 Firefox, 8 Safari, 4 Edge, 2 Chromium, 2 Brave
    - what is the surpisal of a user with Firefox?
    - a Chromium user?
    - what is the entropy associated with this distribution?

Measuring Uncertainty

- When there are multiple variables/features, their surpisals and entropies can be added if they are independent

$$I = I(x) + I(y) \qquad H = H(X) + H(Y)$$

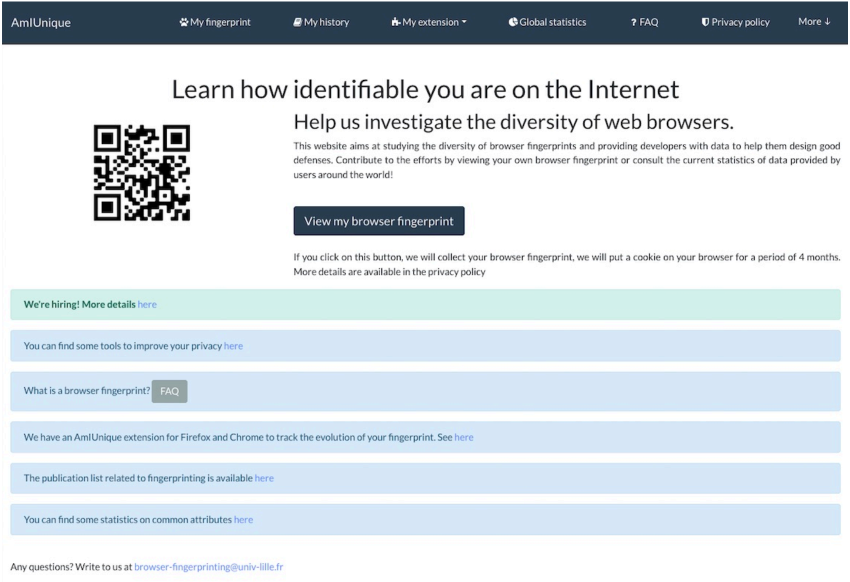
- Otherwise, conditional variants must be used:
  - conditional suprisal with two variables

$$I(x|y) = -\log_2 \Pr(X = x|Y = y) \qquad I = I(y) + I(x|y)$$

  - for each value y of Y, we get a conditional probability distribution on X, denoted by $X|y$

$$H(X|y) = -\sum_{x \in \mathcal{X}} \Pr[X = x|Y = y] \cdot \log_2 \Pr[X = x|Y = y]$$

AmIUnique Test https://amiunique.org



Learn how identifiable you are on the Internet

Help us investigate the diversity of web browsers.

This website aims at studying the diversity of browser fingerprints and providing developers with data to help them design good defenses. Contribute to the efforts by viewing your own browser fingerprint or consult the current statistics of data provided by users around the world!

If you click on this button, we will collect your browser fingerprint, we will put a cookie on your browser for a period of 4 months. More details are available in the privacy policy

We're hiring! More details here

You can find some tools to improve your privacy here

What is a browser fingerprint? FAQ

We have an AmIUnique extension for Firefox and Chrome to track the evolution of your fingerprint. See here

The publication list related to fingerprinting is available here

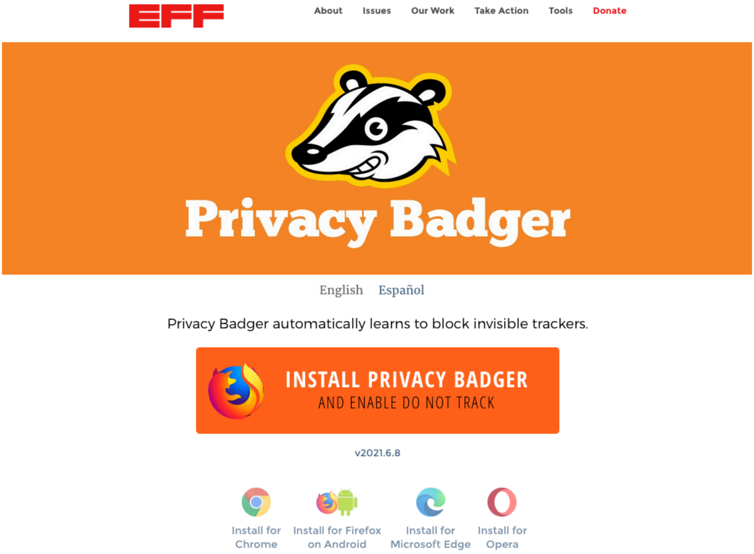
You can find some statistics on common attributes here

Any questions? Write to us at browser-fingerprinting@univ-lille.fr

What Can You Do?

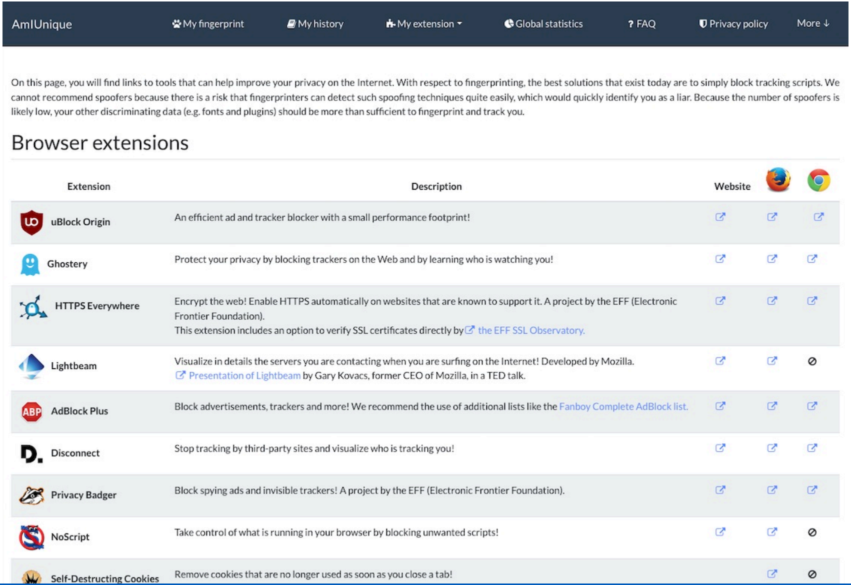
- Step 1: Learn
  - Learn about, examine, and modify if desirable your web browser's security and privacy settings
  - Learn about what privacy protection mechanisms your and other browsers offer
- Step 2: Improve
  - Test how unique you are
  - Install a privacy plugin

EFF Privacy Badger https://privacybadger.org



Privacy Badger automatically learns to block invisible trackers.

Additional Privacy Plugins https://amiunique.org/tools



On this page, you will find links to tools that can help improve your privacy on the Internet. With respect to fingerprinting, the best solutions that exist today are to simply block tracking scripts. We cannot recommend spoofers because there is a risk that fingerprinters can detect such spoofing techniques quite easily, which would quickly identify you as a liar. Because the number of spoofers is likely low, your other discriminating data (e.g. fonts and plugins) should be more than sufficient to fingerprint and track you.

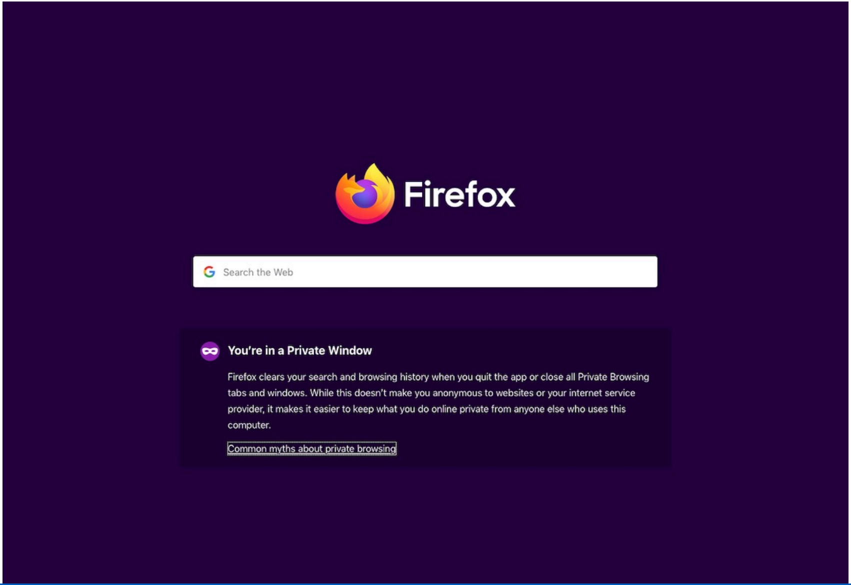
Browser extensions

Extension	Description	Website		
uBlock Origin	An efficient ad and tracker blocker with a small performance footprint!	↗	↗	↗
Ghostery	Protect your privacy by blocking trackers on the Web and by learning who is watching you!	↗	↗	↗
HTTPS Everywhere	Encrypt the web! Enable HTTPS automatically on websites that are known to support it. A project by the EFF (Electronic Frontier Foundation). This extension includes an option to verify SSL certificates directly by ↗ the EFF SSL Observatory.	↗	↗	↗
Lightbeam	Visualize in details the servers you are contacting when you are surfing on the Internet! Developed by Mozilla. ↗ Presentation of Lightbeam by Gary Kovacs, former CEO of Mozilla, in a TED talk.	↗	↗	⊘
AdBlock Plus	Block advertisements, trackers and more! We recommend the use of additional lists like the Fanboy Complete AdBlock list.	↗	↗	↗
Disconnect	Stop tracking by third-party sites and visualize who is tracking you!	↗	↗	↗
Privacy Badger	Block spying ads and invisible trackers! A project by the EFF (Electronic Frontier Foundation).	↗	↗	↗
NoScript	Take control of what is running in your browser by blocking unwanted scripts!	↗	↗	⊘
Self-Destructing Cookies	Remove cookies that are no longer used as soon as you close a tab!		↗	⊘

What Can You Do?

- Step 1: Learn
  - Learn about, examine, and modify if desirable your web browser's security and privacy settings
  - Learn about what privacy protection mechanisms your and other browsers offer
- Step 2: Improve
  - Test how unique you are
  - Install a privacy plugin
  - Use a private browsing mode

Private Browsing Mode



You're in a Private Window

Firefox clears your search and browsing history when you quit the app or close all Private Browsing tabs and windows. While this doesn't make you anonymous to websites or your internet service provider, it makes it easier to keep what you do online private from anyone else who uses this computer.

Common myths about private browsing

What Can You Do?

- Step 1: Learn
  - Learn about, examine, and modify if desirable your web browser's security and privacy settings
  - Learn about what privacy protection mechanisms your and other browsers offer
- Step 2: Improve
  - Test how unique you are
  - Install a privacy plugin
  - Use a private browsing mode
  - Disable Javascript and Flash

Disable JavaScript and Flash

Disabling JavaScript and Flash is an effective way of protecting privacy

- When JavaScript is disabled
  - fingerprinting capabilities are limited
  - certain types of cookies cannot be installed
  - user experience is impacted because some websites might not function properly
- When Flash is disabled
  - usability is typically not impacted because this is an outdated technology

What Can You Do?

- Step 1: Learn
  - Learn about, examine, and modify if desirable your web browser's security and privacy settings
  - Learn about what privacy protection mechanisms your and other browsers offer
- Step 2: Improve
  - Test how unique you are
  - Install a privacy plugin
  - Use a private browsing mode
  - Disable Javascript and Flash
  - Consider switching to a different browser

Consider a Different Browser

- Some browsers were built with privacy being their primary goal
- They address fingerprinting in their design
  - the browser can set parameters to default values to make your fingerprint less unique
  - the browser can make your fingerprint less consistent
- Notable examples are Brave and Tor Browser

https://brave.com

https://torproject.org

What Can You Do?

- Step 1: Learn
  - Learn about, examine, and modify if desirable your web browser's security and privacy settings
  - Learn about what privacy protection mechanisms your and other browsers offer
- Step 2: Improve
  - Test how unique you are
  - Install a privacy plugin
  - Use a private browsing mode
  - Disable Javascript and Flash
  - Consider switching to a different browser
  - Re-test

Privacy-Respecting Tools

There are ways to control your privacy beyond the browser

Think of sites that could collect a lot of information about you

Privacy-Respecting Tools

There are ways to control your privacy beyond the browser

Think of sites that could collect a lot of information about you

Privacy-respecting search engines and other tools:

- DuckDuckGo search engine & more
  - https://duckduckgo.com
  - displays ads based solely on your current search
- Additional resources can be found at https://amiunique.org/tools/

Summary

Web tracking presents a serious threat to user privacy

There is no universal solution, but steps can be taken to reduce tracking and uniqueness of your profile

Additional resources:

- https://coveryourtracks.eff.org/about
- https://amiunique.org/tools/
- https://pixelprivacy.com/resources/browser-fingerprinting/