

## Using Browsers and Search Engines to Safeguard Your Digital Identity

Despite the growing adoption of new AI (Artificial Intelligence) tools, many of us still rely on traditional methods to navigate the internet. We start with a web browser, such as Chrome, Safari, or Microsoft Edge, which serves as the gateway to the online world. But once we're inside, the browser can't help us find anything on its own. That's where search engines such as Google, Bing, and Yahoo come in; they act like a guide or directory inside the building: you type what you're looking for, and it points you to the right rooms. We need both instruments working together — the browser to access the internet at all, and the search engine to make sense of the overwhelming amount of information once we're there.

Given the significant time we spend searching online, how we select and employ browsers and search engines is more crucial than ever. People tend to overlook safety settings because they're buried in complex menus that seem designed for experts rather than casual users. Additionally, technical jargon can be daunting, deterring many from adjusting settings for fear of creating issues.

### What Gets Lost in the Process?

Systems that collect and share data continue to operate quietly in the background, making the risks feel distant and hard to grasp. When you can't see what's being gathered or how it might be used, it's easy to overlook them.

## How Browsers and Search Engines Work Behind the Scenes

### → What a browser stores

**Cache** – a temporary folder that stores copies of images, scripts, and style files the first time you visit a site. If you were to return, the browser can pull these files from the cache instead of downloading them again, speeding up page load time.

**Cookies** – tiny text files that remember your login status, language choice, or items in a shopping cart. They let a site recognize you on later visits.

**Local storage** – a larger, more permanent storage option that web apps use to save settings, offline data, or game progress. This can take the form of “Save” and “Load” buttons. You can close the browser, come back later, and pick up your game right where you left off—no account or internet connection required.

### → What a search engine stores

**Search history** – a record of the queries you’ve typed and the results you’ve clicked. This helps the engine suggest completions and rank results that match your past interests.

**Location and device info** – approximate city, language, and whether you’re on a phone or a computer, later used to fetch locally relevant results (e.g., nearby restaurants) or to display a larger or smaller layout on the screen.

**Personalized settings** – include safe-search filters that block explicit results, “favorites” (items marked to revisit later, usually with a single “star” or “heart” button), and “collections” (saved items organized under a name or theme, such as “Decoration ideas” or “Healthy eating tips”). These follow you across devices you’re signed in to.

→ **How the two work together**

**Speed** – The browser’s cache reduces the amount of data transmitted over the internet, and the search engine’s giant, super-organized library catalog already knows the most popular pages, so both deliver content quickly.

**Continuity** – Cookies keep you logged in, and search engines store your query history. So long as you go from a search result to a site, the site already knows who you are, and the search engine knows what you were searching for.

**Personalization** – Consider a recipe website you visit regularly. If you choose a large font, the website saves that preference so every page appears in larger text the next time you return, making it feel the same every time you visit.

## Helpful Features Can Become Hidden Entry Points

Understanding how browsers and search engines maintain a smooth internet experience reveals a trade-off. The systems that enable quick, individualized browsing also create patterns—predictable activity signals and identity markers.

Although these traces aren’t necessarily harmful, they can become powerful if someone learns to track and follow them.

## ☞ From “Stay Signed In” to Session Hijacking

To keep you logged in, browsers store session tokens—digital “passes” that tell a website you’re already authenticated.

**Why is this convenient?** You don’t have to enter your password every time.

**Imagine this** – *You’ve logged in to a news site from the security of your home network and selected “Stay signed in.” The site then stores a small note (a cookie) on your computer that identifies you so you won’t have to re-enter your credentials on subsequent visits.*

**How it becomes a risk:** If malicious software, counterfeit sites, or an unsecured Wi-Fi network expose that token, an attacker can exploit it to impersonate you. They don’t need your password; they can reuse the token the browser initially saved for your convenience.

**Building on the previous example,** *the next day, you use a coffee shop’s Wi-Fi instead of your home network. Nearby malicious actors might intercept data exchanged between your device and the internet, including the tiny “note” (the cookie that shows you’re logged in). If they capture it, the attacker can insert this note into their browser, causing the website to believe it’s you. This gives them access to your preferences, private comments, and personal information—without added hassle.*

## What steps can prevent this?

### ➤ Skip “Stay Signed In”

When you don’t check the “Stay signed in” (or “Remember me”) box, the website doesn’t store a hidden login token on your device.

### ➤ Avoid Public Wi-Fi to Prevent Interception

Since no one can see your traffic, the risk of an attacker obtaining your login token or other data is significantly reduced.

### ↻ From Autofill Convenience to Autofill Exploitation

Autofill is designed to save time by remembering your name, address, phone number, and sometimes payment details, then automatically filling them in on online forms.

*Imagine this – you’re filling out a checkout page on a trusted shopping site. With Autofill enabled, your address and credit-card number appear instantly, and you can complete the purchase with just a click.*

### 🚩 How might it pose risks?

Suppose you’re shopping online and everything appears normal. The website’s layout resembles a store you’re familiar with, and the checkout page includes standard fields such as your name, address, email, and payment options. However, without your knowledge, a fraudster has secretly added hidden fields in the website's code that are invisible to the human eye. These hidden fields may include your full credit card number, security code, phone number, secondary email, and date of birth. While you can’t see them, your browser can.

## --> What happens next?

- You click into the first visible field.
- Autofill pops up, offering to “Fill in your information.”
- You accept—because that’s what you are used to doing.
- Your browser fills **every** field it detects, including the hidden ones.
- You click “Submit,” thinking you’re just completing a normal purchase.
- The attacker receives all the data Autofill inserted—including information you never saw, never typed, and never meant to share.

Autofill can input not only what you see on the screen but also anticipate what is being requested by sourcing it from its memory.

## What is your best defense?

### ➤ Turn Off Autofill for Sensitive Data

Disable the browser’s built-in address and payment-info autofill (or delete saved entries). Without autofill, concealed fields can’t capture confidential details.

### ➤ Open an Incognito Window for Untrusted Sites

In incognito or private mode, the browser acts like a clean slate. It doesn’t load any saved passwords, addresses, or other autofill information. As a result, the website or app you’re using sees only what you type at that moment; everything else, including autofill info normally stored in the back end, isn’t sent.

## 🕒 From Helpful Prompts to Permission Misuse

Modern browsers allow websites to request a range of permissions to perform various functions.

### 📍 Location Permission

#### Where you'll see the request

- Weather forecasts
- Local community calendars or events pages
- Pharmacy or medical-appointment finders
- Map or directions services


#### What a legitimate request looks like


A site that shows nearby events asks, “*Show activities near you?*” – That’s reasonable because it needs a general idea of your town or city to display relevant content.

Yet, if a website does not have your best interests at heart, it may:

- ✗ Keep your exact GPS location (your precise address) rather than only your town name.
- ✗ Sells that exact location to advertising companies, so you start seeing ads tailored to your very specific community.
- ✗ With a detailed address, the site can generate highly believable pop-up messages such as “Urgent notice for residents of [your street],” making phishing or scam alerts appear much more trustworthy.

**Pause for a moment...**

 **Can you restrict the permission to “this time only”?** Select that option whenever possible. This applies to other permissions your browser may request as well.

 **Do they need the exact address, or would a city name be better?** The “Precise location” feature provides exact addresses, such as 123 Main Street. Conversely, using “Non-precise or approximate location” authorizes a wider description, such as a radius of several miles or a general area.

## **Camera & Microphone Permission**

### **Where you’ll see the request**

- Telehealth appointments
- Online classes (e.g., exercise, technology, etc)
- Voice-controlled tools (“click to speak your question”)

### **What a legitimate request looks like**

When you join an online class you previously registered for, such as one hosted on Zoom, you will be asked to give your consent to use your camera (optional) and your microphone. This request is standard, as accessing a microphone is necessary for you to hear others and for them to hear you.

### **What will be a red-flag scenario?**

You're visiting a website that offers “free health tips.” At first, it seems like a reputable outlet, but while reading an article, you notice it ends with a button that says, “Live video chat with a doctor. Click here for instant help.” When you click the button, a message appears:

*“Allow this site to use your camera and microphone?”*

## What should you keep in mind?

✗ Unexpected request on a content-only page. The article didn't need video or audio; a simple comment box would have been sufficient. So what is the purpose of it?

✗ There is no clear explanation of why it is needed. The prompt merely states "Allow," without specifying what the doctor will observe or hear.

✓ Real medical portals usually have their own branded permission dialog or a clear "Start video call" button on the page, rather than the browser's generic "Allow" window.

✓ If you feel uneasy about a website's reliability, use incognito mode because it starts with no saved camera or microphone permissions. Any access is session-limited, meaning it is cleared when the window closes. This prevents lingering authorizations, even if a site tries to retain them.

## Notifications Permission

### Where you'll see the request

- News sites
- Social media updates from family
- Travel sites ("Your flight has changed")

What can start with you wanting to step on top of the news by accepting the site's request to send you "important updates" could progress to:

✗ Receiving more alerts than expected, cluttering the screen. The issue here isn't necessarily danger; it's just too much digital noise.


✗ Make alerts look similar to system messages, causing confusion.


Each major browser—Chrome, Edge, Firefox, and Safari—offers a central dashboard, with slight variations, to manage and revoke permissions for location, camera, microphone, and notifications. These options are typically found under:


👉 “Privacy & Security” → “Site Settings” or a similar menu...

Let's review the browser's “Settings” menu and its significance for everyday browsing.

### Delete Browsing Data

■  It disrupts the data flow, thereby complicating advertisers' ability to monitor user actions and deliver targeted ads.

■  When your browser saves items such as images and temporary files, this process is known as caching. Over time, cached data can accumulate and consume storage space, slowing page loading, especially on devices with limited storage capacity.

■  Caching can speed up browsing, but an oversized or outdated cache can slow it down. Therefore, clearing the cache should be part of your regular maintenance, not something you do every day.

## How to Clear Browsing Data

► **Open the browser's main menu** on either the three-dot or three-line icon in Chrome, Edge, or Firefox.

→ In the Safari app, locate “Preferences”.

► **Find the section for clearing data**

→ Look for labels such as “History” or “Clear or Delete browsing data.”

→ In Safari, go to the “Privacy” tab.

► **Decide how far back to clear**

This option can be seen in the “time range” or “timeframe” sections, with common choices—last hour, last day, last week, or all time.

► **Select what you want to delete**

→ Most browsers display categories—cached files, cookies, and history—along with their sizes or counts (e.g., “12 MB of cached images” or “45 cookies”). This shows what’s stored and helps you decide which items are worth clearing based on how much has accumulated.

→ In Safari, click “Manage Website Data...” to view individual site data, or click “Remove All Website Data” to delete everything at once.

► **Watch for sync/account notes**

When signed in to a Google, Microsoft, or Apple account, the dialog shows the account name and warns that clearing data may affect other synced devices (e.g., shared history or tabs).

## **Built-In Browser Security Features**

Once enabled, these protections update automatically, providing continuous security in the background.

### **How to Turn Them On**

▶ **Open the browser's main menu** on either the three-dot or three-line icon in Chrome, Edge, or Firefox.

→ In the Safari app, refer to the top menu bar.

▶ **Open the browser's settings**, located toward the bottom of the list, though they aren't always the very last item.

→ In Safari, go to *"Preferences."*

▶ **Go to the security/privacy area**

→ Under *"Privacy & Security"* or *"Privacy, search, and services."*

▶ **Find the built-in protection controls**

Each browser has its own way to activate protection, but they follow a similar pattern: you toggle a control, and the protection becomes active.

→ **Safe Browsing—Chrome**

There are three options: *"Enhanced," "Standard,"* and *"No protection."* Select one, and that choice becomes the toggle.

→ **SmartScreen—Edge**

It's literally one switch:

**ON** = protection active

**OFF** = protection disabled

→ **Enhanced Tracking Protection—Firefox**

Also uses levels. You can choose between “Standard” (default) and “Strict” (stronger protection).

→ **Fraudulent website warning—Safari**

Uses a single checkbox to enable or disable the warning system.

**What protections are provided by each built-in browser security feature?**

**\*\*Threat Warnings:\*\*** Displays a warning page before you access a site known for phishing or malware, preventing accidental exposure of personal information or the download of harmful software.

**\*\*Tracker Blocking:\*\*** Stops or limits hidden trackers that try to follow you across websites. This protects your privacy and reduces the amount of data advertisers can collect about you.

**\*\*HTTPS Enforcement:\*\*** Automatically implements the secure version of a website (HTTPS) if available. This is beneficial because encrypted connections help keep your data private, preventing eavesdropping on public Wi-Fi and other networks.

- Chrome, Edge, and Firefox let you enable this feature using an HTTPS-Only Mode switch.
- Safari has this setup by default, so no activation is needed.

**\*\*Password Breach Monitoring:\*\*** Checks saved passwords against leaked lists and alerts you if compromised, allowing you to change them before attackers exploit them.

## **Private or Incognito Mode**

It's helpful, but frequently misunderstood. These quick do's and don'ts clarify what private mode protects and what it doesn't.

### **Do's**

✓ Do use private browsing mode when you don't want your browsing history saved on your device. It's great for personal research, surprise gifts, or anything you'd rather not store locally.

✓ Do use it to open multiple accounts at the same time. Helpful for people who manage both career and personal accounts and juggle different logins.

✓ Do use it to troubleshoot websites. Private mode loads pages without old cookies, which can fix *"why does this page look weird"* issues.

✓ Do close all private windows once you're done. Nothing clears until the window is fully closed.

### **Don'ts**

✗ Don't assume it erases everything. Downloads and bookmarks stay on your device unless you remove them.

✗ Don't assume websites can't identify you. If you log in, the site still knows who you are.

✗ Don't expect anonymity. Private mode does not hide your IP address or location.

## How do you open Private or Incognito Mode?

- 1 Open your browser.
- 2 Look for the main menu (three dots, three lines, or “File”).
- 3 Find “*New Incognito Window*” or “*New Private Window*.”
- 4 A new window opens featuring a darker theme or a “private browsing” title.

Evaluating the practicality of private mode requires considering its context—the browser—and how it shapes our interactions with the World Wide Web. This leads us to the next question.

## What is Your Default Browser or Search Engine?

Each operating system comes with a default browser. For instance, Android phones typically use Google Chrome, Windows devices usually feature Microsoft Edge, and iOS and Mac computers rely on Safari. The default browser is the program that opens automatically when we click a web link in an email, document, or other app. Regardless, users are not restricted to this default option; they can choose any other browser they prefer.

### Is it possible to switch between different browsers?

Yes, users can run multiple browsers on the same device without them interfering with each other. Each browser maintains its own settings, history, cookies, and privacy rules, so changes don’t “break” anything.

## To change your default browser,

👉 Open your system settings → Look for “Default apps” or “Default browser” → Select your preferred browser.

## Are search engines also configured by default?

Each web browser comes with a “pre-selected” search engine that it leverages immediately after a query is entered in the address bar or the search box.

- Because users are unlikely to adjust this setting, the browser automatically selects the most popular option. For example, Google Chrome defaults to Google Search, Microsoft Edge to Microsoft Bing, and Apple Safari to Google Search on macOS and iOS.
- Some users turn to a privacy-focused engine (e.g., Starpage) to avoid tracking.
- Certain engines deliver better local results (e.g., Baidu in China).

## To change your default search engine,

👉 Open your browser → Go to its Settings menu → Find “Search engine” → Select the one you want.

## Privacy-Focused Browsers...

...operate like a polite librarian who hands you the book you requested without intruding on your reading, whereas many mainstream browsers function more like a shopkeeper who monitors your choices and later recommends similar items.


## What are the goals of privacy-focused browsers?

- Reduce tracking
- Limit data collection
- Block or restrict ads

With that shared basis in mind, here are two browsers you can look into:


### ■ Brave

It blocks ads and trackers right away, making websites load faster and reducing how much companies can track your activity. Ideal for people who want strong privacy without revising any settings.

 **Potential Drawback:** includes an optional ad-reward system that enhances the user experience by allowing users to earn tokens for watching advertisements. Nonetheless, some users find this system confusing or unnecessary, as it adds complexity to their browsing experience.

### ■ DuckDuckGo

It delivers a clean, user-friendly design with a search engine that doesn't create user profiles. It quietly blocks trackers in the background, making privacy effortless.

 **Potential Drawback:** It has fewer features and customization options compared to Brave.



## DEFINITIONS

**\*Ad (short for advertisement)** is a paid message, such as a banner, video, or text, that promotes a product, service, or idea and is displayed on websites, apps, or other media to attract the attention of potential customers.

**\*Artificial Intelligence** is a computer program that can learn from information and make decisions or solve problems—much like a very smart assistant that helps you get answers, recognize pictures, or suggest actions without you having to tell it exactly how to do each step.

**\*Built-in** means something that is included as a standard part of a device, program, or system, rather than being added later as an extra component or plug-in. It's ready to use right out of the box.

**\*Counterfeit site** is a fraudulent website that pretends to be a legitimate service, brand, or retailer in order to trick visitors into sharing personal information, making payments, or downloading malicious content.

**\*Default apps** are the programs a device automatically uses to open a particular file type or perform a common task (e.g., the built-in email client for email links, the pre-installed browser for web URLs, or the photo viewer for images) unless you manually choose a different application.

**\*Encrypted** means the data has been transformed into a coded form that only someone with the correct key can decode and read, keeping the information private from anyone who intercepts it.

**\*GPS location** is the geographic location of a device determined through signals received from GPS satellites orbiting Earth.

**\*HTTPS** stands for Hypertext Transfer Protocol Secure. is a secure way websites send and receive information, encrypting the data so that only you and the site can read it—like a private conversation that can't be overheard by others.

**\*Hijacking** is the unauthorized takeover of a system, account, or communication channel, such as a browser session, login, or network connection, by a malicious actor who redirects control, steals data, or manipulates the original user's activity.

**\*Identity marker** is any piece of information, such as a name, email address, username, device ID, or biometric data, that uniquely identifies you or distinguishes you from other users.

**\*IP address** is a unique series of numbers (e.g., 192.168.1.5) that identifies a device on a network, allowing it to send and receive data over the internet.

**\*iOS** is Apple's mobile operating system that runs on iPhones and iPads, providing the core interface, app management, security features, and services that let users interact with the device and run applications.

**\*Malicious software (malware)** is any program or code designed to damage, disrupt, steal from, or gain unauthorized access to a computer, device, or network.

**\*Online forms** are digital questionnaires or input fields on a website that let you enter information such as text, numbers, selections, or file uploads and submit it to the site's server for processing (e.g., sign-ups, surveys, purchases, or contact requests).

**\*Operating system (OS)** is the core software that manages a computer's hardware, such as memory, processors, storage, and input devices, and provides a platform for other programs to run, handling tasks like file organization, security, and user interaction.

**\*Page load** is the process that starts when you click a link or type a web address and finishes once the browser has retrieved all required files and displayed them on the screen, making the page fully visible and functional.

**\*Pharmacy or medical-appointment finders** are online tools or apps that let you search for nearby pharmacies, doctors, clinics, or appointment slots. By entering a location, specialty, or service, they return a list of options, often with hours, contact details, and the ability to book or request medication refills directly.

**\*Phishing** is a deceptive tactic in which attackers send fake emails, messages, or websites that appear to be from a trusted source, trying to trick you into revealing passwords, credit-card numbers, or other personal data.

**\*Pop-up messages** are small windows or overlays that appear automatically on top of a web page or app screen, usually to convey alerts, prompts, advertisements, or requests for input (e.g., “Allow notifications?”). They temporarily interrupt the current view until the user dismisses or interacts with them.

**\*Query history** is the list of search terms or questions you’ve entered into a search engine, website, or app, stored so you can revisit, reuse, or manage past queries. It records each request you make, often with timestamps, and may be used to suggest related results or to allow you to clear your past searches.

**\*Safety settings** are built-in controls that limit what a system can do or see, protecting you from harmful content, accidental data loss, or unwanted behavior.

**\*Shared history** is a log of browsing activities, including visited pages, searches, and form entries, that is synchronized or shared across multiple devices or accounts, enabling each device to access the same history.

**\*Signed in** means you have entered your username (or email) and password (or another verification method) so the service knows who you are, lets you access personalized features, and tracks your activity during that session.

**\*Style files** are the documents that tell the browser how a web page should look—fonts, colors, layout, spacing, and other visual details.

**\*System message** is a notification generated by the operating system or an application that informs the user about important events, status changes, or required actions, such as error alerts, updates, security warnings, or confirmations.

**\*Tab** is a separate, individual page within a web browser window that lets you view multiple websites at once. Each tab has its own address bar and content, and you can switch between them without opening new browser windows.

**\*Targeted ads** are promotional messages that are shown to you based on information about your interests, browsing history, location, or demographic profile. Advertisers use data they've collected about you to select ads they think are most relevant, increasing the chance you'll click or purchase.

**\*Toggle** is a control—usually a switch, button, or menu option that lets you turn a feature on or off with a single click or tap, switching between two opposite states.

**\*Unsecure Wi-Fi** is a wireless network that lacks proper encryption or authentication—often labeled “Open” or protected by weak passwords—so anyone nearby can intercept the data you send, see which sites you visit, or inject malicious traffic. It leaves your devices and personal information exposed to eavesdropping and attacks.

**\*Voice control tools** are features that enable hands-free control of devices through voice commands, converting speech into actions like opening apps, dictating text, or searching online.

**\*Window** is a rectangular area on your screen that displays the contents of an application or document, allowing you to view, interact with, and move that program while other windows remain visible in the background.

**\*World Wide Web** (or simply the web) is a system of linked documents and resources accessed via the internet, where each page is identified by a URL and can be viewed using a web browser.

- **URL (Uniform Resource Locator)** is the web address you type or click to reach a specific page or file on the internet, such as <https://example.com/page.html>. It tells the browser where to find the resource and how to retrieve it.