

Was ist ein sicherer Browser

Kurz gesagt: Die Suchmaschine (Ecosia, Startpage, DuckDuckGo ...) und der Browser (Chrome, Firefox, Brave ...) sind zwei getrennte Dinge – eine „sichere“ Suchmaschine macht einen eher „neugierigen“ Browser nicht automatisch privat, und umgekehrt.

Unterschied: Browser vs. Suchmaschine

- Der **Browser** (Chrome, Firefox, Brave, Edge, Safari, Tor usw.) bestimmt, wie stark Tracker, Cookies, Fingerprinting usw. blockiert werden – und er kann selbst Daten an den Hersteller senden.
- Die **Suchmaschine** (Google, Ecosia, Startpage, DuckDuckGo ...) entscheidet, was mit deinen Suchbegriffen, deiner IP-Adresse und Nutzungsdaten passiert.

Beispiel: Wenn du Chrome nutzt, aber Startpage als Suchmaschine, schützt Startpage deine Suchanfragen, aber Chrome kann dich trotzdem für andere Webseiten relativ gut tracken.

Wie „privat“ sind Ecosia und Startpage?

- **Ecosia**
 - Nutzt den Bing-Index, speichert Suchanfragen nicht dauerhaft personenbezogen und verkauft deine Daten nicht an Werbefirmen.
 - Verzichtet laut eigenen Angaben auf externe Tracking-Tools, anonymisiert Daten und respektiert „Do Not Track“.
 - Bietet teils erweiterten Tracking-Schutz in Apps/Browsern (Listen gegen Werbe-, Analyse- und Fingerprinting-Tracker).
- **Startpage**
 - Nutzt den Google-Index, schaltet sich aber als Proxy dazwischen: Google sieht nur Startpage, nicht dich.
 - Speicherverhalten ist stark reduziert, Suchanfragen werden nicht personalisiert, IP und persönliche Profile sollen nicht aufgebaut werden.
 - Mit „Anonyme Ansicht“/Proxy kannst du Seiten über Startpage aufrufen, sodass die Zielseite deine IP und Cookies nicht bekommt.

Beide sind im Vergleich zu klassischem Google-Suchen deutlich datenschutzfreundlicher, aber sie ersetzen keinen guten Browser-Schutz.

Woher kommt die Unsicherheit / Datenweitergabe?

Typische Quellen für **Unsicherheit** oder Datenabfluss:

- Der Browser selbst sendet Telemetrie, Nutzungsstatistiken, Absturzberichte etc. an den Hersteller (sehr ausgeprägt z.B. bei Chrome).
- Drittanbieter-Skripte (Werbung, Analytics, Social-Media-Buttons) auf Webseiten setzen Cookies und Fingerprinting, um dich seitenübergreifend wiederzuerkennen.

- Schwacher oder deaktivierter Tracking-Schutz (Standard bei vielen Mainstream-Browsern) lässt diese Skripte ungehindert durch.
- Erweiterungen/Add-ons können selbst Daten sammeln, wenn sie unseriös sind.

Deine Suchmaschine kann also sehr zurückhaltend sein – aber wenn der Browser alles andere durchlässt, bist du insgesamt nicht wirklich anonym.

Was kannst du praktisch tun?

- Einen Browser mit starkem Datenschutz nutzen, z.B. Firefox (mit strengem Tracking-Schutz), Brave, Mullvad, LibreWolf oder Tor Browser, statt z.B. Chrome mit minimalem Schutz.
- In den Einstellungen: strengen Tracking-Schutz, Cookie-Blockierung (Drittanbieter), Fingerprinting-Schutz aktivieren.
- Eine datensparsame Suchmaschine (Startpage, Ecosia, DuckDuckGo etc.) einstellen.
- Optional: Werbe-/Tracking-Blocker wie uBlock Origin einsetzen, wenn der Browser das nicht schon integriert hat.

Ein einfaches Setup wäre z.B.: Firefox mit strengem Tracking-Schutz + Startpage oder Ecosia als Standard-Suche.

Nachfolgend findest du detaillierte Einstellungen für ein starkes Setup mit **Firefox** (empfohlen: kostenlos, open source, sehr anpassbar) **oder Brave** (ähnlich stark, aber noch aggressiver out-of-the-box). Kombiniert mit Startpage/Ecosia und uBlock Origin maximierst du den Schutz vor Tracking, Fingerprinting und Datenweitergabe.

- **Firefox + Erweiterungen:** Flexibel, vielseitig, perfekt für detaillierte Anpassung.
- **Brave:** Weniger Einstellen nötig, integrierter Blocker, aber proprietäre Teile.

Firefox: Basis-Datenschutz maximieren

1. Öffne Einstellungen (Menü → Einstellungen).
2. Gehe zu **Datenschutz & Sicherheit** → **Verbesserter Schutz vor Aktivitätenverfolgung** → **Streng** wählen (blockt mehr Tracker, Cookies, Fingerprinting; bei Problemen Ausnahmen pro Seite setzen).
3. Unter **Cookies und Website-Daten: Angepasst** → Drittanbieter-Cookies blockieren, **Alle Cookies löschen beim Schließen von Firefox** aktivieren.
4. **HTTPS-Only-Modus** → **Aktiviert (streng)**.
5. **Geschichte: Benutzerdefinierte Einstellungen** → Cache nicht speichern, Telemetrie deaktivieren.

Firefox: Suchmaschine einrichten (Startpage oder Ecosia)

1. Einstellungen → **Suche** → **Standard-Suchmaschine** → **Startpage** oder **Ecosia** wählen (falls nicht da: Über add.startpage.com oder ecosia.org installieren).
2. **Suchvorschläge** deaktivieren (verhindert Abfragen an andere Server).
3. Für Ecosia: Optional ihre Erweiterung für extra Tracking-Schutz.

Firefox: ggf. Erweiterungen installieren & konfigurieren

Installiere aus Firefox Add-ons (addons.mozilla.org):

- **uBlock Origin** (Top-Blocker für Werbung/Tracker).
 - Dashboard öffnen (Icon → Zahnrad):
 - **Filterlisten** → Alle „EasyPrivacy“, „EasyList“, „Fanboy's Annoyance“ etc. aktivieren (Standard + zusätzliche für maximale Blockierung).
 - **Einstellungen** → „Ich bin ein fortgeschrittener Benutzer“ aktivieren, „1st-party CNAMEs deaktivieren“.
- Optional: **Privacy Badger** (lernt heuristisch Tracker blocken).
- **HTTPS Everywhere** oder integriert nutzen.

Brave: Schnelle Maximierung

1. Brave herunterladen (brave.com).
2. Einstellungen → **Shields** → **Aggressiv** für Tracker-/Werbeblockierung.
3. **HTTPS-Upgrades** → **Streng**.
4. **Datenschutz & Sicherheit** → Fingerprinting-Blocker **Streng**, Drittanbieter-Cookies blocken, „Vergiss mich bei Schließen“ aktivieren.
5. Suchmaschine → **Startpage** oder **Ecosia** setzen (ähnlich wie oben).