# Übersicht über Tools für einen kontrollierten digitalen Fußabdruck

Mithilfe einfacher Werkzeuge können Sie Ihre **Daten sichern und den Zugriff durch Fremde einschränken.** Im Folgenden werden wichtige Hilfsmittel dazu vorgestellt.

# Lightbeam

 https://addons.mozilla.org/de/firefox/addon/lightbeam-3-0/

|  |
| --- |
| **Lightbeam ist ein Add-on für Firefox, das mittels interaktiver Visualisierung die Erst- und Dritt-Websites zeigt, mit denen Sie im Internet interagieren.**  |
| <https://www.chip.de/downloads/Firefox-Lightbeam_65106174.html> | Mit unterschiedlichen Symbolen veranschaulicht Lightbeam, welche Seiten Sie besucht haben - und welche Verbindungen zu Drittanbietern daraus resultieren. Drei Ansichten stellt das Tool zur Verfügung: "Graph" ist eine Art interaktive Karte, "Clock" schlüsselt Aufrufe zeitlich auf, unter "List" finden Sie alle Einträge in einer sortierbaren Liste. |
| 1. Geben Sie https://www.mozilla.org/de/lightbeam/ in den Browser (Firefox) ein.
2. Klicken Sie auf:

 1. Klicken Sie auf:

 1. Das Lightbeam-Icon erscheint in der Toolbar:

 1. Klicken Sie auf das Icon – noch ist die Grafik leer:

 1. Surfen Sie im Netz und schauen Sie später nochmal nach!

 |

# Ghostery

|  |  |
| --- | --- |
| C:\Users\hellen.heisterkamp\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\5615D558.tmp | <https://addons.mozilla.org/de/firefox/addon/ghostery/> |
| * **Ghostery ist eine**[**Software**](https://de.wikipedia.org/wiki/Software)**, die den Anwender beim**[**Surfen**](https://de.wikipedia.org/wiki/Internetsurfen)**auf versteckte Dienste hinweist, die im Hintergrund private Daten an Seitenbetreiber übermitteln und diese auf Wunsch blockiert.**
 |
| Ghostery blockiert nicht alle Skripte kategorisch. Stattdessen werden nur diejenigen Skripte identifiziert, die die [Privatsphäre](https://de.wikipedia.org/wiki/Privatsph%C3%A4re) oder [Anonymität](https://de.wikipedia.org/wiki/Anonymit%C3%A4t_im_Internet) des Nutzers gefährden, und harmlose Skripte erlaubt. Neben Skripten werden auch weitere Verfahren identifiziert, die die Anonymität oder die Privatsphäre des Nutzers beeinträchtigen könnten (z. B. bestimmte [Cookies](https://de.wikipedia.org/wiki/Cookie), Bilder oder andere Webseiten-Elemente). Der Nutzer kann für jedes dieser potenziell gefährlichen Skripte oder Webseiten-Elemente entscheiden, welche er blockieren oder zulassen möchte. Außerdem kann er sich über deren [Urheber](https://de.wikipedia.org/wiki/Urheber) und [Datenschutz](https://de.wikipedia.org/wiki/Datenschutz)richtlinien informieren. |
| 1. Geben Sie www.ghostery.com in den Browser ein.
2. Klicken Sie auf:

 1. Klicken Sie auf:

1. Suchen Sie einen Browser aus, z.B. Firefox 🡪 Klicken Sie auf „ADD TO FIREFOX“
2. Rufen Sie ach der Installation eine Ihrer beliebtesten Seiten auf.
3. Klicken Sie auf das Geister-Zeichen in der Menüleiste:

1. Konfigurieren Sie die Einstellungen für die entdeckten Tracker (z.B. immer blockieren, temporär blockieren, immer erlauben…):

 |

# Flagfox

|  |  |
| --- | --- |
| Image result for flagfox logo |  <https://flagfox.net/> |
| **Flagfox ist eine**[**Firefox-Erweiterung**](https://de.wikipedia.org/wiki/Mozilla_Firefox#Erweiterungen)**, die durch das Anzeigen der jeweiligen Landesflagge hinter der**[**URL**](https://de.wikipedia.org/wiki/Uniform_Resource_Locator)**grafisch darstellt, in welchem Land sich der**[**Web-Server**](https://de.wikipedia.org/wiki/Webserver)**der geöffne-ten**[**Webseite**](https://de.wikipedia.org/wiki/Webseite)**befindet. Zusätzlich bietet das Tool eine Vielzahl an Werkzeugen, wie Website-Sicherheitsprüfungen, Whois, Übersetzung, ähnliche Seiten, Validierung, URL-Kürzung und mehr.** |
| Image result for flagfox  | Das Wissen über den Standort des Servers ermöglicht es dem Nutzer unter anderem, auf national geltende Rechtsprechung aufmerksam zu werden. Weitere Informationen über den Server, die Webseite oder die [Domain](https://de.wikipedia.org/wiki/Domain_%28Internet%29) können über eine Vielzahl externer Quellen bezogen werden. Ein Klick auf das Flaggensymbol lädt standardmäßig eine Webseite, welche eine detaillierte Karte mit der Stadt, in der sich der Server befindet, und andere nützliche Informationen wie die Ortszeit und den [ISP](https://de.wikipedia.org/wiki/Internetdienstanbieter) anzeigt. Ein Klick mit der mittleren Maustaste, in der Regel das Mausrad, startet in der Voreinstellung eine [Whois](https://de.wikipedia.org/wiki/Whois%22%20%5Co%20%22Whois)-Abfrage. Whois ([englisch](https://de.wikipedia.org/wiki/Englische_Sprache) „*who is“* = „wer ist“) ist ein [Protokoll](https://de.wikipedia.org/wiki/Netzwerkprotokoll), mit dem von einem verteilten [Datenbank-system](https://de.wikipedia.org/wiki/Datenbanksystem) Informationen zu Internet-Domains und [IP-Adres-sen](https://de.wikipedia.org/wiki/IP-Adresse) und deren Eigentümern abgefragt werden können. |
| 1. Geben Sie https://flagfox.net in den Browser ein.
2. Klicken Sie auf:

1. Akzeptieren Sie die Installationshinweise & Befehle des Browsers.
2. Rufen Sie nach der Installation eine Ihrer beliebtesten Seiten auf.
3. Überprüfen Sie die Seite anhand der Flagfox-Tools.
 |
|  | * Geotool zeigt u.a die Server-Lokation an
* Alexa zeigt an, wie beliebt die Seite ist (globales Ranking) und aus welcher Geographie die Nutzer der Seite kommen
* Site Advisor zeigt an, ob die jeweilige Seite sicher ist (Prüfung durch McAfee)
* Google Translate übersetzt die komplette Webseite
* My Info zeigt den Standort des Nutzers im Geotool an
* Virus Scan untersucht die aktuelle Website auf Viren
* Tiny URL verkleinert lange URLs für die Weitergabe
 |

# DuckDuckGo

|  |
| --- |
| Image result for logo duckduckgo <https://duckduckgo.com/>  |
| **DuckDuckGo ist eine Internet-Suchmaschine mit besonderem Fokus auf Schutz der Privatsphäre der Nutzer. Die Suchmaschine verspricht, keine IP-Adressen oder Suchverläufe zu sammeln und kein Tracking der Besucher durchzuführen.** |
|  | DuckDuckGo ist eine [Suchmaschine](https://de.wikipedia.org/wiki/Suchmaschine), die [keine persönli-chen Informationen](https://de.wikipedia.org/wiki/Datenschutz) sammeln soll. DuckDuckGo gibt an, sich von anderen Suchmaschinen zu unterscheiden, weil es seine Nutzer nicht profiliere und für alle Nutzer die gleichen Ergebnisse anzeige.Die Suchmaschine betont, dass statt der meist gesuchten, die besten Suchergebnisse angezeigt würden, wobei die Sucher-gebnisse aus über 400 individuellen Quellen wie Wikipedia, aber auch anderen Suchmaschinen wie Bing, [Yahoo](https://de.wikipedia.org/wiki/Yahoo) oder [Yandex](https://de.wikipedia.org/wiki/Yandex%22%20%5Co%20%22Yandex) entstammen. |
| 1. Geben Sie https://duckduckgo.com in den Browser (Firefox) ein.
2. Klicken Sie im Suchfeld in der Toolbar auf die Lupe.

1. Klicken Sie auf „Change Search Settings“ bzw. „Sucheinstellungen ändern“

1. Wählen Sie im Menü „Standardsuchmaschinen“ DuckDuckGo aus.

1. Stellen Sie weiter unten ein, welche anderen Suchmaschinen Sie mit einem Klick erreichen möchten.
 |

# Adblock Plus

*  <https://adblockplus.org/de/>

Blockiert Banner, Pop-ups und Videowerbung – sogar auf Facebook und You-Tube. Unaufdringliche Werbung kann von der Blockierung ausgenommen werden, um Webseiten zu unterstützen. Teilweise blockiert das Tool auch Inhalte, die direkt zu einer Seite gehören. Die Aktionen laufen im Hintergrund ab und sind nicht gut nachzuvollziehen



# Datenparty

 [www.datenparty.de](http://www.datenparty.de/)

Datenparty.de ist eine auf Jugendliche zugeschnittene Informationsplattform über Datenschutz und Persönlichkeitsrechte, die Hilfe bei ungewollter Datenveröffentlichung, Infos über Sicherheitslücken und Datenlecks in digitalen Medien sowie Sicherheitstipps für Smartphones & Social Media bietet.

# Facebook-Privatsphäre-Einstellungen

Über die Privatsphäre-Einstellungen können Sie die Sichtbarkeit Ihres Facebook-Profils einschränken. Sie können beispielsweise die Einsehbarkeit von verschiedenen Gruppen oder Posts anpassen (z.B. Freunde können mehr sehen als Unbekannte). Achten Sie darauf, welchen Seiten Sie ein „Gefällt mir“ geben. Machen Sie sich bewusst, dass alle Posts auch gelesen werden (Inhalte beachten, Facebook hat alle Rechte an den Inhalten!). Bei kritischen Inhalten sollten Sie vom „Recht auf Vergessenwerden“ Gebrauch machen. Das Recht auf Vergessenwerden (englisch: Right to be forgotten) soll sicherstellen, dass digitale Informationen mit einem Personenbezug nicht dauerhaft zur Verfügung stehen. Das Recht auf Vergessenwerden wird zuweilen verkürzt und unrichtig als „Recht auf Vergessen“ bezeichnet. Weil sich das Recht auf elektronisch gespeicherte Daten bezieht, spricht man auch vom „digitalen Radiergummi“. Es gibt von Google ein Formular online geschaltet, mit dem man das Recht in Gebrauch nehmen kann.

<https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=637187367654755986-1140070037&hl=de&rd=1>

Noch ein Tipp: Treten Sie bei Facebook eventuell nicht mit Ihrem richtigen Namen auf, dann ist Ihr Profil gar nicht erst auffindbar.



In der Publikumsauswahl können Sie ein bestimmtes Publikum auswählen, dass Ihre geteilten Inhalte sehen kann. Sie haben folgende Möglichkeiten:

**„Öffentlich“:** Wenn Sie einen Beitrag öffentlich teilen, kann jeder Internetnutzer den Beitrag sehen, egal ob Facebook-Mitglied oder nicht.

**„Freunde (+ Freunde von markierten Personen)“:** Mit dieser Option können Sie Inhalte mit Freunden auf Facebook teilen. Wenn andere Personen in einem Beitrag markiert wurden, dann umfasst die Zielgruppe dieses Beitrags auch die markierte Person und deren Freunde.

**„Freunde von Freunden“:** Zur Zielgruppe gehören alle Ihre Freunde und deren Freunde.

**„Nur ich“:** Diese Option ermöglicht Ihnen das Posten von Inhalten in Ihrer Chronik, die nur für Sie selbst sichtbar sind. Beiträge mit dem Publikum „Nur ich“ erscheinen in Ihren Neuigkeiten, aber nicht in den Neuigkeiten Ihrer Freunde. Wenn Sie jemanden in einem „Nur ich“-Beitrag markieren, kann er/sie den Beitrag sehen.

**„Benutzerdefiniert“:** Wenn Sie „Benutzerdefiniert“ wählen, können Sie Inhalte mit bestimmten Personen teilen oder diese vor bestimmten Personen verbergen. Außerdem können Sie Beiträge mit bestimmten Freundeslisten, die Sie vorher festgelegt haben, teilen, wie z. B. Ihrer Familie oder Ihren besten Freunden. Sie können auch Beiträge für eine Liste bestimmter Personen verbergen. „Benutzerdefiniert“ ermöglicht es Ihnen auch, Beiträge mit Gruppen oder Netzwerken zu teilen, denen Sie angehören.

Überlegen Sie genau, wer Ihre Bilder/Alben, Freundeslisten, Kontaktinformationen (z.B. Adresse oder E-Mail) oder sonstige persönliche Informationen (z.B. Arbeit, Ausbildung, Familienangehörige, Beziehungen, etc.) sehen sollte.



Es ist sehr sinnvoll, Beiträge, in denen Sie erwähnt/getagged etc. wurden, vor Veröffentlichung zu überprüfen. So können Sie verhindern, dass jemand ein Foto von Ihnen in einer peinlichen Situation veröffentlicht oder Ihren Namen mit einem Kommentar verknüpft, der Ihnen Schwierigkeiten bereiten könnte. Stelle die Funktion der Chroniküberprüfung unbedingt auf „Ein“.

Wenn Sie sich nicht sicher sind, wie viel Sie auf Basis Ihrer Einstellungen an bestimmte Personen freigeben, können Sie sich Profil aus der Sicht von anderen Facebook-Nutzern anzeigen lassen. Entweder individualisiert als Name oder allgemein als Fremder. Wenn Sie dann bemerken, dass es dort Inhalte gibt, die die betreffende Person nicht sehen sollte, müssen Sie Ihre Privatsphäre-Einstellungen weiter detaillieren.



# Check-Liste Ihres Social-Media-Auftrittes für die Sicht eines Personalers bzw. zukünftigen Arbeitsgebers:

|  |  |  |
| --- | --- | --- |
|  | Das tue ich bereits: | Hier ist noch Anpassungs-bedarf: |
| Meine Privatsphäre-Einstellungen sind strikt gehalten. Nicht jeder kann meine Inhalte sehen oder mich kontaktieren. Außerdem kann ich nicht von jeder Person gefunden werden. |  |  |
| Die Einsehbarkeit meiner Posts ist nur verschiedenen Gruppen gewährt (z.B. Freunde können mehr sehen als Unbekannte). |  |  |
| Mir ist bewusst, dass alle Posts auch gelesen werden und Facebook alle Rechte an den Inhalten hat. |  |  |
| Mir ist bewusst, dass ich bei Veröffentlichung von kritischen Inhalten vom „Recht auf Vergessenwerden“ Gebrauch machen kann.  |  |  |
| Ich achte darauf, welche Seiten ich like und in welchem Ton ich Inhalte kommentiere. |  |  |
| Ich trete auf Facebook nicht mit meinem richtigen Namen auf (dann ist das Profil gar nicht auffindbar). |  |  |
| Mein Profilbild ist seriös und meine öffentlichen Bilder zeigen keine kritischen Inhalte.  |  |  |
| Ich habe einen Schulabschluss, meine aktuelle Ausbildungs- oder Arbeitsplatzsituation hinterlegt.  |  |  |
| Meine Posts haben keine Rechtschreibfehler. |  |  |