Grüne Erde

Handbuch für Internet-UserInnen

Die meisten Internetdienste, Social Media-Plattformen und Apps sind zwar kostenlos, aber nicht umsonst: Die Daten der Userinnen und User sind zur Währung geworden.
Um die Kontrolle über die eigenen, personenbezogenen Daten zu behalten, ist bei der Nutzung von Internet und Social Media kritische Aufmerksamkeit geboten.
Das Grüne Erde-Handbuch für Internet-UserInnen informiert und gibt Tipps, wie man selbstbestimmt, verantwortungsvoll und sicher mit dem Internet umgehen und seine persönlichen Daten schützen kann.
Grüne Erde hat für ihren eigenen Online-Auftritt eine eigene, klare und strenge Haltung entwickelt: Diese kann hier nachlesen werden.

www.grueneerde.com/socialmediahaltung-handbuch

ökologisch & fair
www.grueneerde.com

Inhaltsverzeichnis

1. Wieviel wissen Internet-anbieter über mich.

Wenn Sie sich im Internet bewegen, dann werden Daten über Ihre Person, Ihr Verhalten, Ihr soziales und privates Umfeld, Ihre Einkäufe, über Ihre Bewegungen im Internet, Ihren Standort sowie auch über Ihre Bewegungen im realen Leben, zum Beispiel mit wem Sie in Kontakt stehen, über Ihr Aussehen usw. gespeichert. Diese Daten werden miteinander zu Online-Profilen verknüpft.
Auch die Identität der Userin und des Users kann leicht festgestellt werden: Verknüpft mit Ihrem Social Media Konto sind alle Daten außerhalb der sozialen Plattform konkret Ihrer Person zuordenbar.
Ihre Interessen und Ihr Verhalten auf einer Website sind wichtig, weil es dem Unternehmen ermöglicht, angebotene Produkte sowie den Webauftritt zu verbessern und an Sie anzupassen. Das sind Daten, die zwischen Ihnen und dem Unternehmen, dessen Website Sie besucht haben, entstehen und die auch dort bleiben sollten.
Für viele Internetdienste stellt es ein Geschäftsmodell dar, Daten über Sie aus verschiedenen Quellen zu kombinieren und ein Profil daraus zu erstellen. Die Daten werden an dritte Unternehmen verkauft oder für kostenpflichtige Dienstleistungen verwendet, z. B. für personalisierte Werbung. Zu welchen Zwecken und wie Ihr Profil verwendet wird, ist unüberschaubar und unkontrollierbar.

2. Kontrolle über die eigenen Daten – seien Sie kritisch und werden Sie aktiv.

Zur Freiheit jedes Menschen gehört, darüber bestimmen zu können, vom wem und für welche Zwecke persönliche Daten erfasst und verwendet werden. Diese Freiheit fordern wir gemeinsam mit Ihnen ein! Mit diesem Handbuch möchten wir Ihnen zeigen, wie Sie sich im Internet aktiv vor Datensammlungen und Profilerstellungen schützen können.
Unsere Beispiele und Empfehlungen wurden vorab von uns geprüft. Wir können jedoch nicht garantieren, dass die Aussagen der Anbieter richtig sind. Die nachfolgenden Tipps können das Datensammeln zwar nicht komplett verhindern, aber zumindest reduzieren.

2.1. Webbrowser – das Tor zum Internet

Von vielen Menschen wird die Suchmaschine, z. B. Google, mit dem Browser gleichgesetzt. Das ist aber nicht korrekt: Browser sind Apps (Software) auf Ihrem Computer, die Sie benötigen, um Suchmaschinen oder andere Websites zu öffnen und im Internet zu surfen. Die bekanntesten Browser sind:

Chrome
(von Google)

Firefox
(von Mozilla)

Safari
(von Apple)

Internet Explorer
(von Microsoft)

Eine der wichtigsten Maßnahmen zum Schutz der Privatsphäre ist der Webbrowser. Hier gibt es folgende Möglichkeiten:

Probieren Sie alternative Browser aus, die Sie anonym surfen lassen oder die von sich aus schon verbesserte Privatsphäre-Einstellungen haben.

Browser mit verbesserten Voreinstellungen:

Es gibt kostenlose Browser, die hinsichtlich der Privatsphäre verbesserte Voreinstellungen anbieten und die von sich aus Tracking und Werbung blockieren, ohne dass Sie selbst an den Einstellungen arbeiten müssen.
Beispielsweise www.brave.com und www.mozilla.org.

Es ist sehr einfach, diese Browser direkt von der Website oder im Appstore herunterzuladen.

Unterstützung wird in diesen Support-Links gegeben:

- Mozilla Firefox für PC:
  https://support.mozilla.org/de/kb/Firefox-unter-Windows-installieren
- Mozilla Firefox für Mac:
  https://support.mozilla.org/de/kb/installieren-firefox-mac
- Mozilla Firefox für Smartphone und Tablet:
  https://www.mozilla.org/de/firefox/mobile/
- Brave (für PC, Mac; Mobile):
  https://brave.com/de/download/

Tipp

Diese alternativen Browser verhindern, dass Userverhalten im Internet über sog. Tracker (z. B. bestimmte Cookies) nachverfolgt wird. Sollte eine Website ohne Tracker nicht korrekt funktionieren, kann eine „Ausnahme" erteilt werden – ein Pop-up Fenster informiert und fordert zur Erteilung einer Ausnahme auf.
Das bewirkt, dass diese Website Cookies und Tracker setzen kann und führt somit zu einem verbesserten Onlineerlebnis.

Browser zum anonymen Surfen:

Es ist auch möglich, komplett anonym zu surfen, solange Sie sich nicht auf einer Website einloggen. Dann ist eine Datensammlung über Sie nicht möglich. Dafür gibt es kostenlose Browser wie z. B. www.torproject.org. Wegen der Anonymisierung läuft der Browser jedoch teilweise langsamer und manche Funktionen, die dem Usererlebnis dienen, werden nicht unterstützt.

Sie können Ihren Browser auch selbst Privatsphäre-freundlicher einstellen. Das ist eine schwierigere Vorgehensweise, aber die einzige Möglichkeit, wenn Sie bei Browsern wie Internet Explorer oder Chrome bleiben und trotzdem Ihre Privatsphäre schützen möchten.

Ziel ist es, dass Cookies (Erklärung Punkt 4) verhindert und keine Suchverläufe gespeichert werden. Zudem kann ausgeschlossen werden, dass Werbung angezeigt wird. Anbieter der gängigen Browser bezeichnen die datenschutzrelevanten Einstellungen unterschiedlich.

Detaillierte Informationen, wie Sie diese Einstellungen vornehmen, finden Sie hier:
https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/Sicherheitscheck_Webbrowser.html;jsessionid=95EA3E22CE92B3D18DD16937BAC-69DAC.1_cid501

Der „Privat-Modus" oder „Inkognito-Modus" schützt nicht gegen Datensammlungen, sondern nur davor, dass Ihre Such- und Surfverläufe nachträglich von einer anderen Person auf Ihrem Computer abgefragt werden können.

Tipp

Sie können Datensammlung über Ihre Person zusätzlich erschweren, indem Sie verschiedene Internet-Browser verwenden:

- Einen Browser verwenden Sie für Tätigkeiten, für die Ihr echter Name erforderlich ist, zum Beispiel für Online-Shops oder Online-Banking.
- Einen anderen Browser nutzen Sie für anonyme Tätigkeiten, beim Surfen und bei Web-Recherchen.
- Trennen Sie grundsätzlich Browser für private und für berufliche Tätigkeiten.

Helfen Sie mit beim Umdenken! Wählen Sie Dienste und Anbieter, die Ihre Datenschutzrechte respektieren und datenschutzfreundliche Voreinstellungen von sich aus anbieten.

Tipp

2.2. Suchmaschinen – die Landkarte im Internet

Suchmaschinen sind Websites, die Ihnen helfen, das Internet nach Inhalten zu durchsuchen.

Google (von Google)

DuckDuckGO

Bing (von Microsoft)

Ecosia

Google und Bing gehören zu den Suchmaschinen, die Personen- und Verhaltensdaten sammeln. Dafür werden Tracking-Cookies und andere Techniken eingesetzt, um User-verhalten im Netz zu beobachten.

Alternative Suchmaschinen

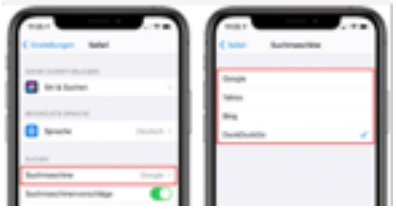
- Diese Suchmaschinen sammeln und speichern von vorneherein keine Userdaten. Beispielsweise www.Duckduckgo.com, www.startpage.de.

- Es gibt Suchmaschinen, die verbesserte Datenschutzeinstellungen versprechen, wie z. B. die ökologisch orientierte Suchmaschine www.ecosia.org.

So kann eine alternative Suchmaschine installiert werden:

- Die Suchmaschine kann direkt von der Website des Anbieters heruntergeladen werden: Auf der Website befinden sich Buttons für „Startpage/DuckDuckGo zu Chrome hinzufügen", „Startpage/DuckDuckGo zu Safari hinzufügen" usw.

- DuckDuckGo kann auf einem iPhone in den Einstellungen gewählt werden: Einstellungen > hinunterscrollen zu Safari > Suchmaschine klicken > DuckDuckGo auswählen.



- Die gewünschte Suchmaschine kann zudem über den App-/Webstore gesucht und installiert werden. Beispiele:

Mobile Chrome

DuckDuckgo installieren:
https://chrome.google.com/webstore/detail/duckduckgo-privacy-essent/bkdgflcldnnnapblkhphbgpggdiikppg

Startpage installieren:
https://chrome.google.com/webstore/detail/startpage-%E2%80%94-private-searc/fgmjlmbojbkmdpofahffgcpkhkngfpef

Ecosia installieren:
https://chrome.google.com/webstore/detail/ecosia-the-search-engine/eedlgdla-jadkbbjoobobefphmfkcchfk

Mobile Safari

DuckDuckgo installieren:
https://apps.apple.com/de/app/duckduckgo-privacy browser/id663592361

Startpage installieren:
https://apps.apple.com/de/app/startpage-suchmaschine/id632832982

Ecosia installieren:
https://apps.apple.com/de/app/ecosia/id670881887

Wenn die Suchmaschine nicht geändert werden soll, können auch die Datenschutz- und Privatsphäre-Einstellungen der Suchmaschine selbst verbessert werden.
Hier zwei Beispiele:
https://support.google.com/chrome/answer/114836?co=GENIE.Platform%3DAndro-id&hl=de
https://www.saferinternet.at/privatsphaere-leitfaeden/google/

2.3. Social Media – im Zentrum der Datensammlung

Social Media- und Content-Plattformen verdienen ihr Geld mit dem Sammeln von Daten der Userinnen und User. Diese Daten werden für Werbung von zahlenden Auftraggebern verwendet oder an dritte Unternehmen verkauft. Die Plattformen haben daher großes Interesse daran, Daten über Sie und Ihr Verhalten aus verschiedenen Quellen zu sammeln. Mitunter auch über andere Websites und Personen aus Ihrem Umfeld.
Sie können mit folgenden Maßnahmen Datensammlungen einschränken:

- Social Media-Konten können mit anderen Anwendungen und Websites verknüpft werden. Beispielsweise sind das Verknüpfungen des Facebook-Profils mit Instagram oder Anmeldungen auf Websites über das Facebook-Konto. Sie sollten Verknüpfungen dieser Art vermeiden, da Ihre Daten in diesem Fall unbeschränkt ausgetauscht werden.

- In den Kontoeinstellungen des jeweiligen Social Media-Dienstes können Sie die Nutzung und Weitergabe Ihrer Daten, zumindest für Werbung, einschränken. Loggen Sie sich dazu ein und öffnen Sie Ihr „Konto“ (Anleitung: siehe Link weiter unten).

- Seien Sie sparsam mit Informationen, die Sie aktiv über sich selbst oder andere Personen posten, z. B. Fotos oder Chat-Gespräche.

Respektieren Sie auch das Selbstbestimmungsrecht Ihrer Mitmenschen über deren persönliche Daten, indem Sie nur mit deren Erlaubnis Fotos und andere Informationen posten.

- Auf manchen Plattformen kann man Personen, die man auf eigenen oder fremden Fotos erkennt, mit Namen identifizieren und markieren. Solche Funktionen sollen die automatische Gesichtserkennung und Identifizierung ermöglichen. Markieren Sie daher keine Personen auf Fotos.

Hier finden Sie einen Leitfaden, wie Sie Ihre Privatsphäre auf den gängigen Plattformen schützen können:
https://www.saferinternet.at/privatsphaere-leitfaeden/

2.4. Cookies und Social Plugins – Datenspione im Internet

Es gibt im Internet verschiedene technische Funktionen, die dazu dienen, Ihr Verhalten über das gesamte Internet hinweg zu beobachten und zu tracken, zu analysieren und ein Profil von Ihnen zu erstellen. Das können etwa bestimmte Cookies, Social Plugins, Bilder und Schriftarten sein. Manche Cookies sind technisch notwendig, um Websites als User nutzen zu können. Andere Cookies und Social Plugins dienen allein dem Zweck, Daten über Sie zu sammeln und weiterzuleiten, ohne dass Sie dies bemerken.

So gehen Sie mit den Tracking Cookies um:

- Tracking Cookies werden auf Ihrem Computer gespeichert, um Sie jederzeit und überall im Internet zu beobachten und Daten an denjenigen zu übermitteln, der das Cookie bei Ihnen gesetzt hat. In Ihrem Browser können Sie einstellen, ob Sie Tracking (Cookies) zulassen oder verhindern möchten (siehe Punkt Browser).

- Social Plugins sind Buttons wie z. B. „Gefällt mir“ oder „Teilen“, die auf verschiedenen Websites integriert werden. Social Plugins senden Daten über Sie an den jeweiligen Anbieter des Social Plugins (z. B. Facebook), sobald Sie eine Webseite besuchen, die solche Buttons anbietet. Wenn Sie dies nicht wünschen, vermeiden Sie Websites mit Social Plugins und nutzen Sie keine dieser Möglichkeiten.

- Gerade kostenlose Apps dienen dazu, Daten über Sie zu sammeln und an den Anbieter der App zu übermitteln. Installieren Sie daher nur jene Apps, die Sie als sinnvoll empfinden und tatsächlich benötigen. Lesen Sie vorher in den Nutzungsbedingungen nach, ob die in Frage kommende App Daten über Sie sammelt und weiterleitet.

Tipp

Wählen Sie Websites und Webshops aus, die keine Social Plugins einsetzen, sondern Ihnen eine Auswahl zum Thema Cookies ermöglichen bzw. keine Tracking Cookies einsetzen.
Auf unserer Website http://www.grueneerde.com/ verwenden wir keine Tracker und geben Ihre Nutzungs- und Verhaltensdaten nicht an Dritte, z. B. für personalisierte Werbung, weiter.

2.5. Alternative Messengerdienste

Der bekannteste aller Messengerdienste (whatsapp) hat vollen Zugriff auf alle Daten auf Ihrem Handy, und auch Zugriff auf Daten von als Kontakt eingespeicherten Personen (Name, Telefonnummer und andere gespeicherte Daten der Person), auch wenn Sie oder die Personen damit nicht einverstanden sind. Kommunikationsinhalte und andere übertragene Daten, wie z. B. Fotos und Videos, werden vom Anbieter des Messengerdienstes gespeichert und mit Partnerunternehmen ausgetauscht, sodass über Sie ein sehr detailliertes Personenprofil erstellt werden kann.
Alternative Messengerdienste sind z. B. Threema oder Signal. Die Dienste haben unterschiedliche Vor- und Nachteile hinsichtlich Userfreundlichkeit und Privatsphäre.

Tipp

Verwenden Sie alternative Messengerdienste und unterstützen Sie damit ein Umdenken zugunsten der Privatsphäre und der Kontrolle über die eigenen Daten.

3. Links

Weitere Informationen, wie Sie sich gegen Datensammlung, Identitätsdiebstahl __und Kriminalität im Internet schützen können, finden Sie unter:

https://www.sicher-im-netz.de/

https://www.saferinternet.at/