Datenschutz am Handy

- Standort-Tracking verhindern

Standort-Tracking verhindern

So schützt Du Dich vor dem Abgreifen heikler Daten.

> Artikel dient als Grundlage für verschiedene Betriebssysteme auf mobilen Endgeräten. Je nach Betriebssystem können die einzelnen Punkte etwas anders heissen oder es sind nicht alle Einstellungen 1:1 so umsetzbar.

In deinem Handy stecken viele kleine Spione. Tracker und Cookies in den Apps sammeln laufend Daten über Sie – und teilen sie mit Hunderten von Partnern. Diese Daten können auch in missbräuchliche Hände gelangen. Sobald die Daten ins Netz gelangen, haben Sie keine Kontrolle mehr darüber, was mit ihnen passiert.

Doch es gibt Möglichkeiten, sich und seine Daten vor dem Abgreifen zu schützen. Mit wenigen Einstellungen auf dem Smartphone bleiben die meisten Daten bei Ihnen. Folgende drei Schritte können Ihnen helfen, die Hoheit über Ihre Privatsphäre zu behalten – vom Anfänger bis zum Profi.

1. Keine Standortdaten teilen

Standortdaten sind die wertvollsten Daten, die Ihr Handy sammelt – aber auch die intimsten. Der wichtigste Schritt ist darum, Ihre Standortdaten nur dann zu teilen, wenn es unbedingt nötig ist.

Um Ihre Standortdaten nicht mehr zu teilen, gehen Sie zu den **Einstellungen** und klicken auf **Datenschutz & Sicherheit**. Klicken Sie nun auf **Ortungsdienste**. Hier können Sie die Ortungsdienste für alle Apps ausschalten, um keine Standortdaten mehr zu teilen. Sie können auch für jede App einzeln festlegen, wann Sie Ihren Standort teilen möchten

Keine Sorge: Die Apps werden Sie wieder anfragen, falls sie Ihre Standortdaten für eine bestimmte Funktion benötigen, beispielsweise die Fahrplansuche, oder um Sie auf einer Karte zu finden. Viele Apps funktionieren auch ohne Ihren genauen Standort einwandfrei. Sie können die neusten Nachrichten auch dann lesen, wenn die App nicht exakt weiss, wo sie das tun.

2. Entfernen Sie Ihre persönliche Werbe-ID

Ihre Daten werden dann besonders interessant, wenn sie aus verschiedenen Quellen stammen und kombiniert werden können. Das wird möglich gemacht mit einer eindeutigen ID für Werbung, die

alle Ihre Daten, die Sie auf unterschiedlichen Apps teilen, verbindet. Diese ID können Sie entfernen. So erschweren Sie das Verknüpfen Ihrer Daten.

Um Ihre Werbe-ID (IDFA) zu löschen, gehen Sie zu den **Einstellungen**, klicken auf **Datenschutz & Sicherheit** und dann auf **Tracking**. Hier können Sie das **Tracking durch Apps deaktivieren**.

3. Innehalten und alles ablehnen

Inzwischen fragen die meisten Apps und Webseiten, ob sie Ihre Daten sammeln dürfen – in der EU ist das sogar gesetzlich vorgeschrieben. Auch in der Schweiz fragen die meisten Apps und Webseiten, ob Sie Ihre Daten sammeln dürfen. Das geschieht über sogenannte Cookie-Banner, die beim ersten Besuch einer Webseite aufploppen – Sie kennen sie sicher.

Die Cookie-Banner sind oft so gestaltet, dass Sie intuitiv alles akzeptieren und so ständig Daten an die App oder Webseite – und potenziell an Hunderte Drittanbieter – senden, die diese eigentlich gar nicht brauchen. Wenn Sie in diesem Moment ein paar Sekunden investieren, können Sie grosse Wirkung erzielen: Bei den meisten Apps und Webseiten genügt in der Regel ein zusätzlicher Klick auf **Zwecke anzeigen** oder **Präferenzen verwalten**, um dann auf **Alle ablehnen** zu klicken und Tracking durch Drittanbieter zu verhindern.

Weitere Schritte

Mit den ersten drei Schritten haben Sie schon viel erreicht. Ein kompletter Schutz ist nicht möglich. Doch es gibt noch weitere Massnahmen, die Sie ergreifen können, um Ihre Daten zu schützen.

- **Berechtigungen überprüfen:** Neben den Standortdaten können Sie auch den Zugriff der Apps auf andere Daten einschränken – zum Beispiel auf Daten Ihrer körperlichen Aktivität. In Ihren **Einstellungen** klicken Sie dafür auf **Datenschutz & Sicherheit**. Hier können Sie die Berechtigung für verschiedene Kategorien anpassen.
- **Machen Sie den Google Privatsphärencheck:** Der Werbegigant Google verfügt über das mit Abstand grösste Tracker-Netzwerk – von Millionen von Webseiten fliessen Nutzerdaten an Google. Inzwischen bietet der Konzern die Möglichkeit, die eigenen Daten besser zu schützen. Mit dem Google Privatsphärecheck können Sie schnell und einfach überprüfen, welche Daten der Konzern von Ihnen speichert und mit Werbepartnern teilt – und die Weitergabe der Daten stoppen.
- **Regelmässig Cookies löschen:** Viele Werbetreibende greifen auf Ihre Cookies zu, um zu erfahren, welche Webseiten Sie besuchen und wofür Sie sich interessieren. Löschen Sie daher regelmässig Ihre Cookies über die Browsereinstellungen. Sie können Ihren Browser auch so einstellen, dass er nur minimal Cookies verwendet. Hier finden Sie eine Anleitung für Chrome, Safari, Edge und Firefox.
- **Ad-Blocker installieren:** In Ihrem Browser können Sie einen Ad-Blocker installieren, zum Beispiel uBlock Origin. Dieser blockiert Werbung auf den meisten Webseiten und verhindert, dass Tracker Ihre Daten sammeln.

- Wollen Sie noch mehr tun? Der Verein Digitale Gesellschaft Schweiz hat einen Ratgeber mit vielen Tipps und Software-Vorschlägen für mehr Datenschutz veröffentlicht.

Auf Telegram wirst du informiert sobald ein neuer Artikel veröffentlicht wird!
HIER ABONNIEREN:

https://t.me/anti_control_info