

4.

HINTERLASSE WENIGER SPUREN

Der Browser auf Deinem Handy speichert eine Menge Informationen über Dich – Deinen Standort, wonach Du suchst, Webseiten die Du besuchst – und verrät diese möglicherweise anderen. Auf Handys, Tablets und Computer sind üblicherweise Browser vorinstalliert, denen Deine Privatsphäre nicht sehr wichtig ist. An ihrer Stelle kannst du **einen Browser herunterladen und benutzen**, der Deine Aktivitäten im Netz **standardmäßig privat** hält und Dich vor Trackern schützt.

Und für eine zusätzliche Erhöhung Deiner Privatsphäre kannst Du Extras installieren, die „Add-ons und Erweiterungen“ heißen. (Dabei handelt es sich um Mini-Programme für Deinen Browser, die **Deine Online-Aktivitäten besser schützen können**).



Um neugierige Werbung und unsichtbare Tracker zu blockieren, kannst Du uBlock Origin (für Chrome, Safari und Firefox) oder Privacy Badger (für Chrome, Firefox und Opera) installieren.

Um sicherzustellen, dass Deine Verbindungen zu Webseiten wo möglich sicher sind, kannst Du HTTPS Everywhere installieren: Das ist eine Erweiterung für den Browser, die dafür sorgt, dass Deine Kommunikation mit vielen großen Webseiten verschlüsselt und bei der Übertragung geschützt wird. Wenn Du Safari benutzt und Dir diese Option gefällt, dann kannst Du deine Standard-Suchmaschine von Google zu einer anderen wie DuckDuckGo ändern, die dich automatisch zu verschlüsselten Verbindungen umleitet.

5.

ENTMARKIERE DICH SELBST UND ANDERE

Hast Du zur Datenmenge über Deine Freunde beigetragen, indem Du sie in der Vergangenheit in Fotos oder Beiträgen markiert hast? Mindere Ihre Datenlast (und erleichtere gleichzeitig auch Dein Gewissen), indem Du **sie entmarkierst** – in so vielen Fotos und Beiträgen wie möglich.

Sag es weiter! Sporne Deine Freunde, Verwandten und Kollegen dazu an, sich Dir bei der Kontrolle von diesen flüchtigen Daten anzuschließen. Wenn wir alle zusammenarbeiten, um die Kontrolle über unsere Datenspuren zu gewinnen, dann können wir uns gegenseitig beim Detox helfen.

Ein Produkt von

**TACTICAL
TECH**

Unterstützt durch



datadetoxkit.org
#datadetox



D A T A
D E T O X
K I T

KONTROLLIERE DEINE SMARTPHONE-DATEN

um Deine Online-Privatsphäre zu erhöhen

Wenn Du darüber nachdenkst, was Deine Daten anderen über Dich verraten, dann scheint es vielleicht keine große Sache zu sein: Wen interessiert es schon, ob Du gern Country-Musik hörst; dass Du mehr Schuhe kaufst, als Du tragen kannst; oder Deinen nächsten Urlaub schon ein Jahr im Voraus planst?

Das Problem ist, was mit Deinen Daten passiert. Über einen Zeitraum gesammelt kommen intime digitale Muster zum Vorschein: Deine Gewohnheiten, Bewegungen, Beziehungen, Vorlieben, Ansichten und Geheimnisse eröffnen sich denjenigen, die sie analysieren und von ihnen profitieren, wie Unternehmen und Datenbroker.

Im Verlauf dieses Daten-Detox erhältst Du einen Einblick, wie und warum all das passiert, und ergreifst praktische Maßnahmen, um Deine Datenspuren im Internet zu kontrollieren.

Legen wir los!

1.

ÄNDERE DEINEN GERÄTENAMEN

Irgendwann einmal hast du Deinem Handy vielleicht für WLAN oder Bluetooth einen „Namen gegeben“ – oder ein Name wurde automatisch während der Einrichtung festgelegt.

Das heißt, dass „Alex Jungs Telefon“ für den Besitzer des WLAN-Netzwerks sichtbar ist, und falls du Bluetooth aktiviert hast, sieht dies auch jeder in der Gegend, der sein Bluetooth ebenfalls aktiviert hat.

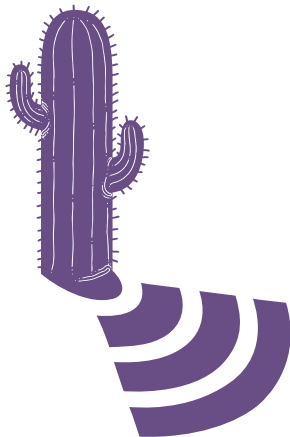
Du würdest Deinen Namen auch nicht verkünden, wenn Du ein Café, Restaurant oder den Flughafen betrittst – und Dein Handy sollte das auch nicht.

Du kannst **den Namen Deines Handys ändern**, in etwas, **das Dich nicht persönlich identifiziert**, aber immer noch eindeutig Du bist. So gehst Du dabei vor:



iPhone:
Einstellungen → Allgemein → Info → Ändere den Namen

Android:
**Gerätenamen für WLAN ändern:
Einstellungen → WLAN → Menü → Erweitert / Weitere Optionen → Wi-Fi Direct → Gerät umbenennen**
**Gerätenamen für Bluetooth ändern:
Einstellungen → Bluetooth → Aktiviere Bluetooth, wenn es deaktiviert ist → Menü → Telefon umbenennen → Deaktiviere Bluetooth**



2.

LÖSCHE DEINE STANDORT-FUSSABDRÜCKE

Es mag Dir so vorkommen, als wären Deine Standortdaten nur zusammenhanglose Brocken an Informationen. Betrachtet man sie aber im Ganzen, können sie **wichtige Details über Dich** und Deine Gewohnheiten enthüllen – beispielsweise wo Du wohnst, wo Du arbeitest und wo Du Dich gern mit Freunden triffst. Aus diesem Grund sind sie bei vielen Unternehmen und Datenbrokern heiß begehrt.

Du kannst **die Berechtigungen jeder einzelnen App** durchgehen und **die Standortdienste deaktivieren**. Halte Ausschau nach den Apps, für deren Dienste diese Angabe nicht nötig ist (Muss dieses Spiel wirklich wissen, wo Du gerade bist?), und bei denen Du nicht willst, dass sie sie bekommen.



Android:
Einstellungen → Apps → Verwalte den Standortzugriff auf App-Basis

iPhone:
Einstellungen → Datenschutz → Ortungsdienste → Verwalte den Standortzugriff auf App-Basis

Android:
Einstellungen → Apps → Wähle die App aus, die Du deinstallieren möchtest → Deinstallieren

iPhone:
Drücke auf eine App, bis alle beginnen zu wackeln und kleine Kreuze in der linken oberen Ecke jeder App auftauchen.
Tippe auf das kleine Kreuz einer App, um sie zu löschen.
Drücke auf den Home-Button, um zurückzukehren.

3.

RÄUME DEINE APPS AUF

Deine Social-Media-Apps, Spiele und Wetter-Apps sind an Deinen Daten interessiert ... Und sie sammeln ziemlich viele davon.

Diese beliebigen Apps die Du nicht benutzt auf Deinem Handy loszuwerden, kann ein großer Schritt zum Detox Deines digitalen Selbst sein.

Dazu kommt, dass das Aufräumen auch neuen Speicherplatz auf Deinem Telefon freigibt, die Datennutzung verringert und die Akkulaufzeit erhöht. Je nach App kann sich dadurch sogar die Leistung allgemein verbessern.