
Mehr Datenschutz
aufs Smartphone

Mehr Datenschutz aufs Smartphone

Wichtig: Je nach Hersteller, Smartphonemodell und Betriebssystem gibt es in der Bedienung und den Optionen (und deren Namen) große Unterschiede. Nutze die oft verfügbare Suchfunktion in den Einstellungen deines Geräts, um etwas zu einem passenden Stichwort zu finden oder nutze eine Suchmaschine, um passende Infos zu deinem Gerät zu finden. Nimm dir bei Bedarf in Ruhe und ausreichend Zeit, dich mit deinem Gerät zu beschäftigen.

Inhalt

Tracking durch Werbe-ID unterbinden

Die Aktivitäten der Benutzer.innen können über die sogenannte Werbe-ID - einer eindeutigen Zeichenkette - über verschiedene Apps hinweg und langfristig zugeordnet und verfolgt werden. Glücklicherweise lässt sich diese Art Tracking einfach verhindern:

Android: Einstellungen → Google → Reiter “Alle Dienste” → Werbung → Werbe-ID löschen - Button “Werbe-ID löschen” tippen

iOS: Einstellungen → Datenschutz & Sicherheit → Tracking → “Apps erlauben, Tracking anzufordern” deaktivieren

Bebilderte Anleitung: https://www.kuketz-blog.de/android-und-ios-werbe-id-abschalten-und-damit-tracking-verringern/

Weitere Infos dazu:
- https://netzpolitik.org/2024/databroker-files-wie-datenhaendler-deutschlands-sicherheit-gefaehrden/
- https://netzpolitik.org/2024/databroker-files-so-stoppt-man-das-standort-tracking-am-handy/
- https://netzpolitik.org/2024/databroker-files-jetzt-testen-wurde-mein-handy-standort-verkauft/

Übergriffige Apps finden, Berechtigungen einschränken

iOS und Android steuern die Zugriffe auf bestimmte Systemschnittstellen heutzutage über strikte Berechtigungen. Häufig kann man Apps den Zugriff auf sensible Dinge wie Standort, Kontakte und den Speicher verbieten, während die App dennoch nutzbar bleibt.

Auf **Android** kann man mit dem Dienst **Exodus Privacy** für die meisten Apps aus dem Play Store überprüfen, wie viele Trackingdienste in den Apps stecken:
- https://reports.exodus-privacy.eu.org/de/

Ebenfalls testet das Projekt Mobilsicher im **AppChecker** Android-Apps auf ihre Datenschutzfreundlichkeit: https://appcheck.mobilsicher.de/appchecks/

Vielen Apps können App-Berechtigungen entzogen werden, ohne ihre grundlegende Funktionalität zu beeinträchtigen:

- **Android**: Einstellungen → Datenschutz & Sicherheit → Berechtigungsmanager
  Alternativ: Einstellungen → Apps (→ Alle Apps anzeigen) → App auswählen → Berechtigungen
- **iOS**: Einstellungen → Datenschutz → Berechtigung/Dienst auswählen
  Alternativ: Einstellungen → Apps → App auswählen → Gewünschte Berechtigung konfigurieren

Besonders sollte man sich sensible Berechtigungen wie Standort, Mikrofon, Kamera und den Zugriff auf Dateien anschauen. Apps, die als besonders übergriffig oder aufdringlich auffallen oder zu viel Werbung enthalten, können oft durch freie Apps ersetzt werden, bei Android z.B. aus dem freien App-Store F-Droid (siehe unten).

Eine Liste an empfehlenswerten freien Apps – auch für iOS – findet ihr auf unserer Website: https://datenpunks.de/freie-apps-smartphone/

Werbung & Tracking blockieren

Werbung lässt sich - neben individuell im Webbrowser - auf zwei Wegen systemweit und damit in den meisten Apps blockieren: per Filter-App oder per DNS-Server. Wichtig: Damit lässt sich nur ein Teil der unerwünschten Datenverbindungen, die zum Tracking und für Werbung genutzt werden, unterbinden. In einigen Apps (z.B. Videowerbung in YouTube) greifen diese Maßnahmen nicht.

ACHTUNG: Die gleichzeitige Nutzung eines verschlüsselten DNS-Servers und eine der empfohlenen Filter-Apps kann zu Problemen führen. Entscheide dich daher für eine Variante.

Systemweit per DNS-Server

Einen DNS Server im System konfigurieren, der Werbung und Tracker blockiert, z.B.

- dnsforge.de
- dns.adguard-dns.com
- fdns1.dismail.de
- fdns2.dismail.de
- adblock.dns.mullvad.net

Android: Einstellungen → Netzwerk & Internet → Privates DNS → "Hostname des Anbieters des privaten DNS" anwählen und dort einen der oben genannten Server angeben. Achtung: Nicht kompatibel mit Apps, die per VPN-Schnittstelle filtern.

iOS: Bei einigen Anbietern können die DNS-Server als "Profile" direkt ins System geladen werden:

- AdGuard: https://adguard-dns.io/de/public-dns.html
- DNSForge.de: https://dnsforge.de/

Wenn man den Link zur entsprechenden Datei antippt, sollte eine Meldung erscheinen, ob man das Laden des DNS-Profils zulassen möchte. Dies bestätigt man durch "Zulassen". Anschließend die "Einstellungen" von iOS öffnen und oben auf "Profil geladen" tippen. Anschließend tippst du oben rechts auf "Installieren" und dann auf "Fertig".

Alternativen:

- Dismail: https://dismail.de/info.html#dns
- Mullvad: https://github.com/mullvad/encrypted-dns-profiles

Die Installation der Profile ist hier etwas komplizierter. Hier ist eine Anleitung: https://mullvad.net/en/help/dns-over-https-and-dns-over-tls#ios

Man kann mit einem Aufruf von https://dnsleaktest.com/ (dort "Standard test" anklicken) im Browser prüfen, ob die DNS-Server auch tatsächlich genutzt werden.

Mehr Infos: https://www.kuketz-blog.de/fuer-anfaenger-bequeme-werbung-und-tracker-unter-ios-android-systemweit-verbannen/

Systemweit per App

Systemweit können Werbung und Tracker über eine App blockiert werden, die die VPN-Schnittstelle des Betriebssystems zum Filtern unerwünschter Verbindungen nutzt.

Vorteil: Anpassung der Filter möglich, Filterung geschieht "privat" auf dem eigenen Gerät

Nachteil: Erhöhter Akkuverbrauch, manchmal Probleme mit dem Internetzugriff (AdAway), andere VPN-Dienste parallel nicht nutzbar

Android:

- AdAway: https://adaway.org/
  1. Muss über F-Droid (siehe unten) oder als Installationspaket (APK) von GitHub (siehe AdAway-Website) heruntergeladen werden.
  2. Nach dem ersten Start wählt man den “VPN-basierten Webeblocker” aus und tippt auf “Weiter”.
  3. Im nächsten Fenster lässt man zu, dass AdAway Benachrichtigungen anzeigt, und tippt wieder auf “Weiter.”, anschließend nochmal auf “Fertig”.
  - ‣ Umfassende Anleitung: https://www.kuketz-blog.de/adaway-werbe-und-trackingfrei-im-android-universum/

iOS:

- AdGuard Pro (kostenpflichtig, ca. 10 US-Dollar): https://adguard.com/de/adguard-ios-pro/overview.html
  - ‣ Umfassende Anleitung: https://www.kuketz-blog.de/adguard-pro-tracking-und-werbung-unter-ios-unterbinden/

Den sicheren Messenger Signal installieren

Signal ist ein sicherer und vertrauenswürdiger Messenger, der sich genau so leicht wie WhatsApp bedienen lässt. Signals Quellcode ist offen, so dass Sicherheitsexpert.innen sich schon häufiger davon überzeugt haben, dass der Dienst sicher und datensparsam arbeitet. Eine Telefonnummer ist zur Nutzung Pflicht, muss aber nicht gegenüber anderen Chatpartner.innen offen gelegt werden.

Download:

https://signal.org/install (alternativ direkt in Play/App Store nach “Signal” suchen)
https://signal.org/android/apk/ (kein Play Store / APK für Android)

Android: Wenn Signal als APK außerhalb des Play Stores installiert wird, kann sich die App selbst aktualisieren und weist auf neue verfügbare Versionen hin.

Cloud-Dienste deaktivieren

Viele Dienste werden standardmäßig über das Google-, Apple- oder Hersteller-Konto synchronisiert. Nicht alle Daten möchte man aber mit den Großkonzernen teilen. Du

kannst auf deinem Gerät die Synchronisation bestimmter Apps und Daten deaktivieren:

- **Android**: Einstellungen → (Passwörter, Passkeys &) Konten → Konto/Dienst antippen → die jeweiligen Einstellungen deaktivieren
- **iOS**: Einstellungen → <Dein Accountname> → iCloud (→ Auf iCloud gesichert) → die gewünschten Dienste/Einstellungen deaktivieren

F-Droid installieren [nur Android]

Apps im Verzeichnis des freien "App-Stores" F-Droid sind in der Regel deutlich privatsphärefreundlicher, als die meisten Apps im Play Store. Außerdem sind dort einige Apps zu finden, die es im Play Store gar nicht erst gibt.

Anleitungen zur Installation von F-Droid:
- https://f-droid.org/de/docs/Get_F-Droid/
- https://mobilsicher.de/ratgeber/so-installieren-sie-den-app-store-f-droid

Download: