Mobilgeräte

Hinweis: Da Betriebssysteme für Mobilgeräte laufend weiterentwickelt und zudem von den Geräteherstellern stark angepasst werden, ist es möglich, dass bestimmte Einstellungen bei dir nicht auffindbar oder unter anderen Menüpunkten zu finden sind.

Für Anfänger.innen [Android & iOS]

Bildschirmsperre einrichten:

- Mobilgeräte gehen oft verloren oder werden geklaut. Damit Fremde nicht direkt auf dein Gerät zugreifen können, solltest du einen PIN-Code oder ein Passwort zum Entsperren des Geräts wählen. Insbesondere Wischgesten und Sperrmuster bieten oft keinen ausreichenden Schutz vor Fremdzugriff. Biometrische Merkmale wie Fingerabdrücke können von Dritten kopiert werden und sind im Gegensatz zu anderen Schutzmechanismen nicht einfach zu ändern.

Nicht genutzte Dienste deaktivieren:

- Aktiviertes WLAN, GPS und Bluetooth können deine Postion an Dritte verraten. Daher solltest du diese Schnittstellen nur dann aktivieren, falls du sie gerade tatsächlich benötigst.

Sprachassistenten deaktivieren

- Sowohl bei Android als auch bei iOS lauschen digitale Sprachassistenten immer mit. Glücklicherweise lassen sich der Google Assistant und Siri deaktivieren:
- Android: ***Google-App*** öffnen → unten rechts auf ***Mehr*** tippen → ***Einstellungen*** → ***Google Assistant*** → nach unten zur ***Liste der Assistant-Geräte*** scrollen → auf das ***Smartphone-Symbol*** tippen → den Assistant über den ***Regler oben*** deaktivieren.
- iOS: ***Einstellungen*** → ***Siri & Suchen*** folgende Optionen deaktivieren: ***Auf 'Hey Siri' achten***, ***Für Siri Seitentaste drücken*** und ***Siri im Sperrzustand erlauben***.

Synchronisation beschränken oder abschalten:

- Kalender, Kontakte und viele weitere Daten und Apps werden häufig standardmäßig mit den Servern von Google und Apple synchronisiert. Diese privaten Daten musst du nicht mit Datenkraken teilen.
  - Android: Unter ***Einstellungen*** → ***Konten*** entsprechende Konten deaktivieren.
  - iOS: Unter ***Einstellungen*** → ****dein Accountname**** iCloud-Apps von der Synchronisation ausschließen.

Zugriff auf Werbe-ID beschränken / Werbe-ID löschen:

- Viele Apps tracken dich über die Werbe-ID: eine lange, eindeutige Zeichenfolge, die dich eindeutig identifizierbar macht. Allerdings gibt es Gegenmaßnahmen:
- Android: Unter ***Einstellungen*** → ***Google*** → ***Anzeigen / Werbung*** die Option Personalisierte Werbung deaktivieren, außerdem kann hier je nach System auch die Werbe-ID zurückgesetzt oder gelöscht werden. Ersteres kann man regelmäßig wiederholen, letzteres ist ausdrücklich empfohlen.

- iOS: Unter ***Einstellungen*** → ***Datenschutz*** → ***Tracking*** die Option **Apps erlauben, Tracking anzufordern** deaktivieren. Apps bekommen anschließend grundsätzlich keinen Zugriff mehr auf die Werbe-ID.

Apps kritisch hinterfragen:

- Viele Apps verlangen deutlich mehr Rechte, als für ihre Funktion eigentlich notwendig sein sollte. Prüfe bei Neuinstallation oder dem Aktualisieren von Apps, welche Rechte angefordert werden. Eine Taschenlampen-App braucht z.B. keine Verbindung zum Internet, ein Mediaplayer keinen Zugriff auf deine Kontakte. Datenschutzfreundliche Alternativen sind oft verfügbar (siehe auch „Datenschutzfreundliche Apps & Dienste nutzen“).
- Apps spionieren ihren Nutzer.innen häufig umfassend hinterher – und das nicht nur, während die Anwendungen geöffnet sind. Versuche auf Apps zu verzichten, die du nicht zwingend brauchst oder deren Vertrauenswürdigkeit zweifelhaft ist, und nutze stattdessen lieber deinen Webbrowser. Ganz grundsätzlich gilt: Weniger ist meist mehr!
- Mit **Exodus Privacy** kannst du überprüfen, ob bestimmte Apps deine Privatsphäre gefährden: https://reports.exodus-privacy.eu.org/

  Unter Android gibt es Exodus Privacy auch als App in F-Droid und im Play Store, um installierte Apps auf Tracker zu prüfen.

App-Einstellungen anpassen bzw. einschränken:

- Android:
  - Unter ***Einstellungen*** → ***Apps & Benachrichtigungen*** (oder von dort ***Erweitert*** → ***Berechtigungsmanager***) App-Berechtigungen einschränken.
  - Unter ***Einstellungen*** → ***Google*** alles Unnötige deaktivieren.
- iOS: Unter ***Einstellungen*** → ***Datenschutz*** Zugriff von Apps beschränken.

Verschlüsselt chatten (Alternativen zu WhatsApp, Telegram und Co):

- Als mögliche Alternative zu WhatsApp und Co ist der Messenger **Signal** einen Blick wert. Er schützt Nachrichten und Anrufe durch Ende-zu-Ende-Verschlüsselung, lagert Chatverläufe nicht in eine Cloud aus und ist freie Software.
  - **Signal:** https://signal.org/, APK-Download (Android): https://signal.org/android/apk/

Webbrowser konfigurieren:

- Eine der meistgenutzten Apps ist der Browser. Umso wichtige ist es ihn gut zu konfigurieren:
  - Android: **Firefox** auf dem Play Store oder **Fennec** aus F-Droid installieren, dann App starten, unten rechts den „Drei-Punkte“-Menü-Button und auf **Einstellungen** tippen:

    Im Abschnitt ***Suchen*** andere Suchmaschine einstellen und **Suchvorschläge anzeigen** deaktivieren. Im Abschnitt ***Datenschutz und Sicherheit*** den **Nur-HTTPS-Modus** einschalten, **Verbesserter Schutz vor Aktivitätenverfolgung** auf „Streng“ stellen **Browser-Daten beim Beenden löschen** nach Bedarf konfigurieren. Zurück in **Einstellungen Add-ons** antippen und **uBlock Origin** installieren.
  - iOS**: Safari** ist vorinstalliert und kann besser konfiguriert werden. Im System auf **Einstellungen** und dann auf **Safari** tippen, dann:

Im Abschnitt ***Suchen*** evtl. auf **DuckDuckGo** wechseln, die Optionen **Suchmaschinenvorschläge**, **Safari-Vorschläge** und **Toptreffer vorab laden** deaktivieren. Im Abschnitt ***Datenschutz & Sicherheit*** die Optionen **Cross-Sitetracking verhindern** aktivieren, **IP-Adresse verbergen** auf „vor Trackern“ stellen, **Datenschutzwahrende Werbemessung** und **Apple Pay prüfen** deaktivieren.

Es empfiehlt sich sehr, **Firefox Klar** oder **AdGuard** als Inhaltsblocker zum Filtern von Werbung und Tracking einzurichten. Eine Anleitung zu Firefox Klar gibt es hier: https://mobilsicher.de/ratgeber/werbeblocker-bei-safari-einrichten-ios

Für Fortgeschrittene [Android & iOS]

Geräteverschlüsselung einrichten:

- Damit die Daten auf dem Gerät bei Diebstahl oder Verlust nicht ausgelesen werden können, solltest du das Dateisystem verschlüsseln.
  - In der Regel ist die Geräteverschlüsselung unter Android bereits aktiviert. Falls dem nicht so sein sollte, kannst du sie aktivieren:

    Android: ***Einstellungen → Sicherheit → Verschlüsselung und Anmeldedaten → Smartphone verschlüsseln***. Beim Start des Geräts musst du anschließend dein Gerät immer via PIN/Passwort/Wischgeste etc. Entsperren. Bei neueren Android-Geräten meist grundsätzlich aktiviert.

    Vorsicht: Insbesondere bei älteren Android-Versionen kannst du dein Passwort/PIN ohne Zurücksetzen deines Geräts nicht mehr ändern. Außerdem sind Passwort/PIN für Bildschirmsperre und Gerätestart häufig zwingend einheitlich.
  - iOS: Ab Version 8 grundsätzlich aktiviert.

Verschlüsselte Chats via XMPP (Jabber):

- Dezentrale Chats über das Protokoll XMPP lassen sicvzns-h via OMEMO Ende-zu-Ende-verschlüsseln. Entsprechende Apps sind sowohl unter Android als auch iOS verfügbar:
  - Android: Conversations / blabber.im
    – https://conversations.im/ bzw. https://blabber.im/
  - iOS: ChatSecure / Monal / Siskin IM
    – https://chatsecure.org/ bzw. https://monal.im/ bzw. https://siskin.im/
- Mehr Infos zu XMPP findest du auf den folgenden Seiten:
  - https://www.freie-messenger.de/sys_xmpp/
  - https://www.kuketz-blog.de/empfehlungsecke/#messenger
    (Abschnitt „XMPP & Matrix: Android & iOS“)

Google-Apps deinstallieren/deaktivieren [Android]:

- Unter ***Einstellungen → Apps*** kannst du vorinstallierte Apps deinstallieren oder deaktivieren, sofern du sie nicht unbedingt nutzen willst. Insbesondere bei den Google-Apps musst du oft ausprobieren, wie stark das Deaktivieren bzw. Deinstallieren den Betrieb deines Systems einschränkt (z.B. sollte man die Google Play-Dienste zunächst aktiviert lassen, da viele Apps aus dem Play-Store von Ihnen abhängig sind). Fortgeschrittene können (auch andere) fest installierte Apps über die Android Debugging Bridge (ADB) deaktivieren: https://www.kuketz-blog.de/android-system-apps-ohne-root-loeschen/

Den freien App-Store F-Droid installieren und nutzen [Android]:

- F-Droid ist ein alternatives Verzeichnis für Apps („App Store“). Dort findet man ausschließlich freie Software, die häufig größeren Wert auf deine Privatsphäre legt als viele Apps im Play Store. Alternativ können sämtliche F-Droid-Apps auch als APKs zur manuellen Installation direkt von der Website heruntergeladen werden – allerdings gibt es ohne installiertes F-Droid keine automatischen Updates.
  - Offizielle Website: https://f-droid.org/
  - Anleitung: https://mobilsicher.de/ratgeber/so-installieren-sie-den-app-store-f-droid

Datenschutzfreundliche Apps & Dienste nutzen [Android]:

Zu vielen unfreien, kostenpflichtigen Apps und vorinstallierten Diensten von Google gibt es freie Alternativen, bei denen in der Regel mehr Wert auf deine Privatsphäre gelegt wird.

- **Aegis:** App zur Zwei-Faktor-Authentifizierung via TOTP.
- **AntennaPod:** Verwaltung, Download und Abspielen von Audiopodcasts.
- **Aurora Store:** Zugriff auf Google Play Store ohne eigenen Google-Account und Play-Dienste.
- **Blokada:** Werbung und Tracking via VPN-Schnittstelle systemweit unterbinden.
- **Bromite:** Auf Privatsphäre und Sicherheit optimierter Chromium-Browser. Zur Installation ein separates F-Droid-Repository hinzufügen: https://www.bromite.org/fdroid
- **Collabora Office:** Office-Suite auf Basis von LibreOffice. Zur Installation ein separates F-Droid-Repository hinzufügen: https://www.collaboraoffice.com/releases-en/collabora-office-on-mobiles-supporting-password-protected-documents-and-available-on-f-droid/
- **DAVx^5:** Kontakt-, Aufgaben und Kalendersynchronisation via CalDAV/CardDAV.
- **Editor:** Schlichter Texteditor.
- **Etar:** Alternative Kalender-App zum Google Kalender.
- **FairEmail:** Moderner E-Mail-Client mit vielen Funktionen (einige nur gegen Bezahlung).
- **Feeder** Verwalten und Lesen von Newsfeeds via RSS/Atom.
- **Fennec F-Droid:** Der bekannte Webbrowser Mozilla Firefox als F-Droid-Variante.
- **FitoTrack:** Eine privatsphärefreundliche Sport-Tracking-App.
- **Fritter:** Twitter-Inhalte ohne Account verfolgen.
- **ICSx^5:** Kalender via iCalendar/.ics-Dateien abonnieren.
- **Infinity:** Ein hübscher Client für Reddit, der auch Abos ohne Account ermöglicht.
- **K-9 Mail:** Umfangreicher E-Mail-Client.
- **KeePassDX:** Mit KeePassXC kompatible Passwortverwaltung.
- **Material Files:** Ein umfassender Dateimanager.
- **MuPDF viewer:** Betrachter für PDF-Dateien.
- **NetGuard:** Eine Firewall zur Regelung von ein- und ausgehenden Verbindungen via VPN-Schnittstelle (einige Funktionen nur gegen Bezahlung).
- **NewPipe:** Client für YouTube und andere Videodienste, der auch Downloads ermöglicht.
- **Open Camera:** Umfangreiche Kamera-App.
- **OpenBoard:** Eine Alternative zur vorinstallierten Hersteller-/Android-Tastatur.
- **OpenKeychain:** Tool zur Ver- und Entschlüsselung via OpenPGP inkl. Schlüsselverwaltung.

- **Organic Maps:** Hübsche Karten- und Navigationsapp auf Basis von OpenStreetMap. Allerdings weniger Features als...
- **OsmAnd+:** Mächtige Anwendung für Karten und Routenplanung auf Basis von OpenStreetMap, die auch offline funktioniert.
- **PCAPdroid:** Aufzeichnen des Datenverkehrs aller installierten Apps über die VPN-Schnittstelle.
- **QR Scanner (Privacy Friendly):** Ein QR-Code-Scanner und -Generator.
- **QuickDic:** Offline-Wörterbuch.
- **RadioDroid:** Verzeichnis und Player für Internetradio-Stationen.
- **Simple Gallery Pro:** Bild-/Medienbetrachter.
- **Tor Browser:** Webbrowser zum anonymen Surfen auf Basis vom Firefox. Braucht aktiviertes Guardian-Project-Repository in F-Droid.
- **Transportr:** Öffentliche Verkehrsverbindungen und Fahrpläne abrufen.
- **UntrackMe:** Leitet Seitenaufrufe auf datenschutzfreundliche Alternativdienste um.
- **Vanilla Music:** Ein schlanker Audioplayer.
- **VLC:** Bekannter Video- und Audioplayer, der mit vielen Formaten umgehen kann.
- **Wasserwaage:** Winkel und Neigungen mit dem Smartphone messen.
- **WiFi Automatic:** WLAN unter bestimmten Umständen automatisch (de-)aktivieren.
- **Zapp:** Zugriff auf die Mediatheken der deutschen öffentlich-rechtlichen Fernsehsender inkl. Downloadfunktion.

Weitere Alternativen zu unfreien Apps und Diensten findest du z.B. beim Gemeinschaftsprojekt Prism-Break und bei der digitalen Selbstverteidigung von Digitalcourage:

- https://prism-break.org/de/categories/android/
- https://digitalcourage.de/digitale-selbstverteidigung/freie-apps-fuer-das-befreite-smartphone

Datenschutzfreundliche Apps & Dienste nutzen [iOS]:

Unter iOS gibt es lediglich den hauseigenen App Store – alternative Quellen für Apps sind aufgrund des unfreien Systems und Apples Richtlinien nicht vorgesehen. Tracking ist auch trotz der vermeintlich strikten Richtlinien und Einschränkungen durch Apple ein großes Problem unter iOS: https://www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking/

Dennoch gibt es einige bemerkenswerte freie Apps:

- **AdGuard (Pro)**: Werbung und Tracking werden in der kostenlosen Version im Browser Safari unterbunden, in der kostenpflichtigen Pro-Version auch systemweit.
- **Collabora Office:** Office-Suite auf Basis von LibreOffice.
- **KeePassium:** Mit KeePassXC kompatible Passwortverwaltung.
- **Onion Browser:** Webbrowser zum anonymen Surfen durch das Tor-Netzwerk.
- **Organic Maps:** Hübsche Karten- und Navigationsapp auf Basis von OpenStreetMap. Allerdings weniger Features als...
- **OsmAnd Maps Travel & Navigate:** Anwendung für Karten und Routenplanung, die auch offline funktioniert.
- **PGPro:** Tool zur Ver- und Entschlüsselung via OpenPGP inkl. Schlüsselverwaltung.
- **Tofu:** App zur Zwei-Faktor-Authentifizierung via TOTP.

- **VLC for Mobile:** Bekannter Video- und Audioplayer, der mit vielen Formaten umgehen kann.

Weitere quelloffene Apps für iOS: https://open-source-ios-apps.netlify.app/ (nicht von uns gesichtet)

Für Profis [Android]

Alternatives Betriebssystem installieren:

Vorinstallierte Versionen von Android enthalten oft Änderungen des Herstellers, schnüffeln dir hinterher und schränken die Anpassbarkeit des Systems stark ein. Auch die Dienste und Apps von Google und anderer Konzerne sind meist fest ins System integriert. Wer Google gänzlich entsagen will, sollte eine alternative Android-Variante („Custom-ROM“) auf seinem Gerät installieren. Das ist zwar meistens mit dem Verlust der Herstellergarantie verbunden, dafür wirst du wieder laufend mit Systemupdates versorgt und hast auf deinem Gerät bei Bedarf Root-Zugriff (Stichwort Gerätehoheit), wodurch du jegliche Softwarekomponenten verändern kannst. Das Wiki von LineageOS (englisch) listet für viele Geräte die Schritte auf, mit denen man ein alternatives Betriebssystem installieren kann: https://wiki.lineageos.org/. Darüber hinaus sind zu den meisten Geräten ROMs und englischsprachige Hilfestellungen unter https://forum.xda-developers.com/ zu finden. Deutschsprachige Unterstützung gibt es auf https://www.android-hilfe.de/.

Auch aus Gründen der Nachhaltigkeit und des Umweltschutzes solltest du dir überlegen, ob du das Leben deines alten Smartphones durch ein Custom-ROM verlängern kannst: https://fsfe.org/activities/upcyclingandroid/upcyclingandroid.de.html

Warnung: Installation auf eigene Gefahr! Wir können dich im Rahmen dieser Veranstaltung leider nicht bei der Installation unterstützen und haften nicht für Datenverlust, Geräteschäden und ähnliches.

- **LineageOS** ist der Nachfolger zum einst beliebten CyanogenMod, eine modifizierte Variante von Android, und wird von einer großen Community fortlaufend weiterentwickelt. Viele Geräte werden offiziell unterstützt, für andere Geräte sind nicht selten inoffizielle Versionen verfügbar. Wer Ersatz für die Google-Dienste braucht, die für viele Apps im Play Store vorausgesetzt werden, kann auch LineageOS mit **microG**, einem freien Nachbau der Google-Dienste, installieren. https://lineageos.org/ bzw. https://lineage.microg.org/
- **/e/OS** ist ein gemeinschaftliches CustomROM-Projekt vom Mandrake-Linux-Schöpfer Gaël Duval, das auf LineageOS aufbaut, allerdings viele Ersatzdienste für die typischen Google-Apps enthält und auch einen eigenen Cloud-Dienst anbietet. Es ist für ähnlich viele Geräte wie LineageOS verfügbar; Smartphones wie z.B. das Fairphone 3/4 mit vorinstalliertem /e/OS können im hauseigenen Shop erworben werden. microG ist vorinstalliert. https://e.foundation/
- **GrapheneOS / CalyxOS** sind Android-Varianten, die ihr Augenmerk auf Sicherheit und Privatsphäre richten. GrapheneOS rückt dabei eher die Sicherheit in den Mittelpunkt, während sich CalyxOS an einem Mittelweg zwischen beiden Aspekten versucht und z.B. auch die Installation von microG anbietet. Im Gegensatz zu anderen Android-ROMs gibt es hier auch keinen entsperrten Bootloader, was als Sicherheitsproblem gilt, wenn jemand physischen Zugriff auf dein Gerät hat. Unterstützt werden fast nur Pixel-Smartphones von Google. https://grapheneos.org/ bzw. https://calyxos.org/

- **Replicant** will nicht nur einfach einfach ein freies Betriebssystem sein, sondern setzt für die Hardwareunterstützung freie Gerätetreiber ein, die sonst von den Herstellern selbst oder Google stammen. Wegen der aufwendigen Entwicklung ist es nur für sehr wenige ältere Geräte verfügbar. https://replicant.us/

Mike Kuketz hat in seinem Blog eine empfehlenswerte und äußerst detaillierte Artikelreihe veröffentlicht, in der Schritt für Schritt erläutert wird, wie du dein Android-Smartphone und deine Daten den neugierigen Blicken von Google und anderen Unternehmen entziehen kannst.

- Android ohne Google: Take back control! https://www.kuketz-blog.de/android-ohne-google-take-back-control-teil1/
- Your Phone Your Data (light) – Android unter Kontrolle: https://www.kuketz-blog.de/your-phone-your-data-light-android-unter-kontrolle/