

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. Auch ändern sich die Apps von Entwicklern, sodass wir keine Aktualität garantieren können. Als Orientierung ist diese Handreichung aber durchaus gut geeignet.

Für Anfänger [Android & iOS]

Bildschirmsperre einrichten:

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

Nicht genutzte Dienste deaktivieren:

- Aktivierte Dienste WLAN, GPS und Bluetooth können deine Position an Dritte verraten. Daher solltest du diese Schnittstellen („Verbindungen“) nur dann aktivieren, WENN du sie gerade tatsächlich benötigst (d. h. Zu exakt diesem Zeitpunkt).

Synchronisation beschränken oder abschalten:

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

Apps kritisch hinterfragen:

- Viele Apps verlangen deutlich mehr Berechtigungen, als für Funktion der jeweiligen eigentlich notwendig sind. 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 ihre Nutzer:innen häufig umfassend hinterher – und das nicht nur, während die Anwendungen geöffnet sind. Versuche auf Apps zu verzichten, die du nicht zwingend brauchst/regelmäßig nutzt oder deren Vertrauenswürdigkeit zweifelhaft ist.
- Mit **Exodus Privacy** (englisch) kannst du überprüfen, ob bestimmte Apps deine Privatsphäre gefährden: <https://reports.exodus-privacy.eu.org/> (oder als App deine installierten Apps auf einen Blick prüfen).

App-Einstellungen anpassen bzw. einschränken:

- Android:
 - Datenschutzmodus standardmäßig aktivieren (**Einstellungen** → **Datenschutz**).
 - Unter **Einstellungen** → **Apps** App-Berechtigungen einschränken.
 - In der App **Google-Einstellungen** 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>
 - Eine weitere Alternative ist Wire. Statt einer Telefonnummer kann die App auch mit einer Mail-Adresse aktiviert werden (welche sich leichter/öfter wechseln lassen als Handynummern).
Wire: <https://wire.com/de>, APK Download (Android): <https://wire.com/de/download/>
-

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.
 - Android: **Einstellungen** → **Sicherheit** → **Smartphone verschlüsseln**. Beim Start des Geräts musst du anschließend dein Gerät immer via PIN/Passwort/Wischgeste etc. entsperren.
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 sich Ende-zu-Ende-verschlüsseln. Entsprechende Apps sind sowohl unter Android als auch iOS verfügbar:
 - Android: Conversations (Legacy) / Pix-Art Messenger
– <https://conversations.im/> bzw. <https://jabber.pix-art.de/>
 - iOS: ChatSecure / Monal
– <https://chatsecure.org/> bzw. <https://monal.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“)

E-Mails verschlüsseln [Android]:

- E-Mail-Verschlüsselung ist auch auf Smartphones möglich. Unter Android geht dies mit den E-Mail-Clients „K-9 Mail“ oder „FairEmail“ in Verbindung mit der OpenPGP-App „OpenKeychain“.

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 von Ihnen abhängig sind).
- Falls **Einstellungen** → **Apps** es Mal nicht zulässt: „adb uninstall –user=0 com.example.package_name“ macht sich dafür das Multi-User Feature zu Nutze.

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

- F-Droid ist ein alternatives Verzeichnis für Apps („App Store“ bzw. „Play Store“). Dort findet man ausschließlich freie Software, die häufig größeren Wert auf deine Privatsphäre legt als viele Apps im Play Store.

Ein toller Vorteil: viele kostenpflichtige Apps aus den Play Store werden hier kostenfrei angeboten.

Alternativ können sämtliche Apps auch als APKs zur händischen 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/schritt-fuer-schritt/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.

- **AdAway:** Nach X Fehl-Anmeldungen wird das Gerät heruntergefahren (root).
- **AFWall+:** Eine (root) Firewall, die mit IP-Tabellen arbeitet.
- **Amaze:** Ein Dateimanager mit vielen Funktionen.
- **andOTP:** App zur Zwei-Faktor-Authentifizierung.
- **AntennaPod:** Verwaltung, Download und Abspielen von Audiopodcasts.
- **AnySoftKeyboard:** Eine Alternative zur Hersteller-/Android-Tastatur.
- **Audio Recorder:** Diktiergerät.
- **Aurora Store:** Zugriff auf Google Play Store ohne eigenen Google Account und Play-Dienste (inkl. Prüfung durch Exodus Privacy).
- **BirthDayDroid:** Geburtstage aus dem Adressbuch erinnern.
- **Blokada:** Werbung und Tracking via VPN-Schnittstelle systemweit unterbinden.
- **Blade:** Musik-Wiedergabe.
- **Bromite:** Ein weiterer Browser mit Fokus auf Datenschutz.
- **DAVx⁵:** Kontakt-, Aufgaben- und Kalendersynchronisation via CalDAV/CardDAV.
- **Carnet:** Leistungsstarke Notiz-App.
- **ClassyShark3xodus:** Exodus Privacy auf Steroiden (untersucht auch Apps außerhalb des Play Stores).
- **Editor:** Schlichter Texteditor.
- **Etar:** Alternative Kalender-App zum Google-Kalender.
- **Exodus Privacy:** Überblick Tracker und Berechtigungen eigener Apps.
- **FairEmail:** Privatsphäre-freundlicher Mailclient; für Anfänger gut geeignet.
- **Fedilab:** Client für das Fediverse (Mastodon, PeerTube, Pixelfed,...)
- **Feeder & Flym:** Verwalten und Lesen von Newsfeeds via RSS/Atom (letzteres bietet Speichern von Favoriten).
- **Fennec F-Droid:** Der bekannte Webbrowser Mozilla Firefox als F-Droid-Variante.
- **Firefox Klar:** Auf Datenschutz getrimmte Variante von, bekanten Firefox-Internetbrowser.
- **ICSx⁵:** Kalender via iCalendar/.ics-Dateien abonnieren.
- **Joplin:** Notizen- /Todo-App mit Synchronisation zu Linux, Windows und MacOS
- **K-9 Mail:** Umfangreicher E-Mail-Client.
- **KeePassDroid:** Mit KeePassX kompatible Passwortverwaltung.
- **LibreOffice Viewer:** Betrachter für Office-Dateien.

- **Markor:** Notizen & mehr, Sync mit (eigener) Nextcloud
- **Memospiel:** Memory für Android.
- **MuPDF viewer:** Betrachter für PDF-Dateien.
- **Net Monitor:** Listet Netzwerkverbindungen aktiver Apps und Dienste auf.
- **NetGuard:** Eine (non-root) Firewall zur Regelung von ein- und ausgehenden Verbindungen.
- **NewPipe:** Client für YouTube, der auch Audio- und Videodownloads ermöglicht, das Abspielen bei ausgeschaltetem Bildschirm anbietet und keine Werbung vor/während Videos enthält.
- **ObscuraCam:** Fotos zensieren/verpixeln.
- **Odyssey:** Musik-Wiedergabe.
- **Offline Calendar:** Kalender ohne Online-Account/Synchronisation erstellen.
- **Öffi:** ÖPNV für Verbindungen und Fahrpläne weltweit abrufen.
- **Open Camera:** Umfangreiche Kamera-App.
- **OpenKeychain:** OpenPGP- und Schlüsselverwaltung unter Android.
- **OpenToDoList:** Notizen und Aufgaben verwalten.
- **Open Note Scanner:** Dokumente scannen.
- **OsmAnd~:** Anwendung für Karten und Routenplanung, die auch offline funktioniert.
- **Pen&PDF:** Betrachten und Bearbeiten von PDFs.
- **Pdf Viewer Plus:** Betrachter für PDF-Dateien.
- **PilferShush Jammer:** Mikrofon blockieren (aktiv und passiv).
- **QuickDic:** Offline-Wörterbuch.
- **RadioDroid:** Verzeichnis und Player für Internetradio-Stationen.
- **Scrambled Exif:** Fotos vor dem Versenden von Metadaten befreien (löschen).
- **SecScanQR:** Ein QR-Code-Generator und Scanner.
- **Shattered Pixel Dungeon:** Ein Rogue-like-Spiel.
- **Shelter:** Isolieren von Apps in Profilen.
- **Silence:** Verschlüsselte SMS versenden.
- **Slide:** Für Reddit-Nutzer.
- **Schlichte Galerie Pro:** Bild-/Medienbetrachter.
- **Snoopsnitch:** Überprüfen, welche Sicherheitsupdates installiert/Lücken geschlossen sind.
- **Tor Browser:** Webbrowser zum anonymen Surfen auf Basis vom Firefox.
- **Transportr:** Öffentliche Verkehrsverbindungen und Fahrpläne abrufen.
- **Vanilla Music:** Ein schlanker Audioplayer.
- **VLC:** Bekannter Video- und Audioplayer, der mit vielen Formaten umgehen kann.
- **Web Opac:** Stadt- & Universitätsbibliotheken durchsuchen und Benutzerkonto verwalten.
- **WiFi Automatic:** WLAN unter bestimmten Umständen automatisch (de-)aktivieren.
- **Wikipedia:** Die offizielle App der Online-Enzyklopädie Wikipedia.
- **Wrong PIN Shutdown:**

- **Zapp:** Zugriff auf die Mediatheken der deutschen öffentlich-rechtlichen Fernsehsender inkl. Download-Funktion.

Weitere Alternativen zu unfreien Apps und Diensten findest du z. B. Bei IzzyOnDroid, beim Gemeinschaftsprojekt PRISM Break und bei der digitalen Selbstverteidigung von Digitalcourage:

- <https://android.izzysoft.de/applists>
Tracker sind ausgewiesen, Quellen auch ("immer die Apps mit F-Droid Icon bzw. Gelbem Sternchen akaTrackerFrei bevorzugen")
- <https://prism-break.org/de/categories/android/>
- <https://digitalcourage.de/digitale-selbstverteidigung/freie-apps-fuer-das-befreite-smartphone>

Für die gängigen Google- oder Gerätehersteller-Apps gibt es Alternativen (Kalender, Kontakte, Kamera, Galerie, Rechner, Taschenlampe, Dateimanager,...). Mobilsicher erklärt in einem Video einzelne Schritte um ein Starter-Paket von „Simple Mobile Tools“ zu nutzen:

- <https://www.invidio.us/watch?v=MtpRqFW-gmE>

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/>
-

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 sind meist fest ins System integriert. Wer sich Google gänzlich entsagen will, sollte eine alternative Android-Variante auf seinem Gerät installieren. Das ist zwar häufig mit dem Verlust der Herstellergarantie verbunden, dafür wirst du aber 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/>

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:** Der Nachfolger zum einst beliebten CyanogenMod ist 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. <https://lineageos.org/>
- **Replicant:** Replicant will nicht nur einfach ein freies Betriebssystem sein, sondern setzt für die Hardwareunterstützung freie Gerätetreiber ein, die sonst von den Herstellern selbst oder von Google stammen. Wegen der aufwendigen Entwicklung ist es nur für sehr wenige ältere Geräte verfügbar. <https://replicant.us/>
- **OmniROM:** <https://www.omnirom.org/>
- **Sailfish OS:** <https://sailfishos.org/>
- **GrapheneOS (ehemals Copperhead):** <https://grapheneos.org/>
- **Paranoid Android:** https://de.wikipedia.org/wiki/Paranoid_Android