Smartphonesicherheit

Hier erfährst du:

- Wo die Sicherheitslücken bei Smartphones liegen.
- Wie du deine Sicherheit bei der Nutzung erhöhen kannst.
- Wie du dein Smartphone verschlüsseln kannst.
- Wie du sichere Passworte und Backups erstellen kannst.
- Wie du deine Einstellungen überarbeiten kannst und die Preisgabe deiner Daten minimierst.

Da bei deinem Smartphone sehr viele Daten anfallen und es im Alltag kaum wegzudenken ist, haben wir hier einiges zum Thema Smartphonesicherheit zusammengefasst. Hier findest du neben Erklärungen und Anleitungen auch Empfehlungen und Tipps!

Smartphones sind Datensammelmaschinen

Deinen Laptop oder Desktop zu schützen ist super, aber was ist mit den Bedrohungen für deine Privatsphäre und Sicherheit wenn du telefonierst? Smartphones sind unglaublich begehrte Ziele, weil sie ganz konzentriert so viele Daten über dich beinhalten. Das GPS in deinem Handy kann deinen Aufenthaltsort über den Tag hinweg aufzeichnen. Vieles deiner Kommunikation mit Freunden, oft mit sensiblen Informationen oder Bildern ist in abrufbaren Textnachrichten gespeichert. Oft sind deine E-Mails, Bilder, Videos, Dateien und viele andere wichtige Daten in deinen Apps gespeichert.

Während Smartphones super praktisch und funktional sind, bedeutet das auch, dass du weniger Kontrolle über deinen digitalen Raum hast. Du musst deinen Apps vertrauen, dass sie deine Daten sicher verarbeiten. Du musst deinem Betriebssystem vertrauen, dass es nicht gehackt werden kann. Du musst deinem Mobilfunkanbieter vertrauen, dass er sich nicht in deine Daten oder Anrufe einmischt. Du musst hoffen, dass niemand mit böser Absicht Kontrolle über dein Handy erlangt.

Bevor wir richtig einsteigen, müssen wir festhalten, dass bei einem Smartphone oft viel mehr Daten anfallen als bei einem Computer. Smartphones haben wir meistens dabei und sind meist mit zusätzlichen Sensoren ausgestattet die zusätzliche Daten liefern. Obwohl es viele tolle Tools für Handysicherheit gibt, sind sie oft nicht leicht verständlich und werden Standort-tracking und Überwachung nicht gänzlich aufhalten.

Was kann ich tun, um meine digitale Autonomie zu stärken?

Schritt 1: **Verschlüssel dein Handy!**

Schritt 2: Verwende **Freie und Open-Source-Software** (Empfohlene Apps) und achte auf deine Einstellungen

Schritt 3: Mache Updates!

Schritt 4: Wähle **sichere Passworte**

Smartphones bieten nicht nur die Überwachungsmöglichkeiten des Computers, sondern besitzen auch noch zB Bewegungssensoren. Achte darauf Dinge wie Standort und Bluetooth nur eingeschalten zu haben, wenn du es auch gerade wirklich brauchst. → Das ist auch akkusparender 🙂

Habe außerdem nur die Apps installiert, die du auch brauchst, da jede zusätzliche App eine mögliche Sicherheitslücke darstellst. → **Mache regelmäßig Updates!**

Die weiteren Artikel zur Smartphone-Sicherheit sollen dir dabei helfen, etwas Kontrolle über deine Sicherheit zurückzubekommen!

Smartphones verschlüsseln

Wie Verschlüsselung grundsätzlich funktioniert haben wir in einem Artikel im Wiki geschrieben. Wie du deinen Computer oder deine Festplatte verschlüsseln kannst ist hier beschrieben.

Auf Smartphones werden viele Daten gespeichert und gerade Repressionsbehörden sind sehr erpicht darauf sie in die Hände zu bekommen. Ihr solltet deswegen unbedingt darauf achten, dass euer Smartphone verschlüsselt ist. **Wichtig zu wissen ist jedoch, dass deine Daten mittels der Verschlüsselung nur dann vor anderen Augen sicher ist, wenn dein Gerät ausgeschalten ist!** Ist dein Smartphone angeschalten oder sogar entsperrt, ist es leicht möglich auf dein Gerät zuzugreifen. Das heißt spätestens wenn du zu einer politischen Aktion, wie zB einer Demo gehst ist das Handy ausgeschalten! (Oder noch besser, es bleibt ausgeschalten zu Hause) Wird dein ausgeschaltenes und verschlüsseltes Handy beschlagnahmt, ist ein Zugriff schwer möglich.

Nachdem ein Zugriff auf eure Daten aber nicht ausgeschlossen werden kann, **überlegt euch grundsätzlich was ihr für Daten auf eurem Smartphone speichert** und wie ihr die Nutzung möglichst datensparsam gestalten könnt. Auch wenn es ein paar Möglichkeiten gibt Daten einzugrenzen, fallen bei eurem Telefon meist noch viel mehr Daten an als zum Beispiel bei eurem Computer.

Neuere Smartphones sind mittlerweile fast alle standardmäßig verschlüsselt, trotzdem solltest du das nochmal in den Einstellungen kontrollieren. Sonst lassen sich die meisten Smartphones sehr einfach über die systemeigenen Einstellungen verschlüsseln.

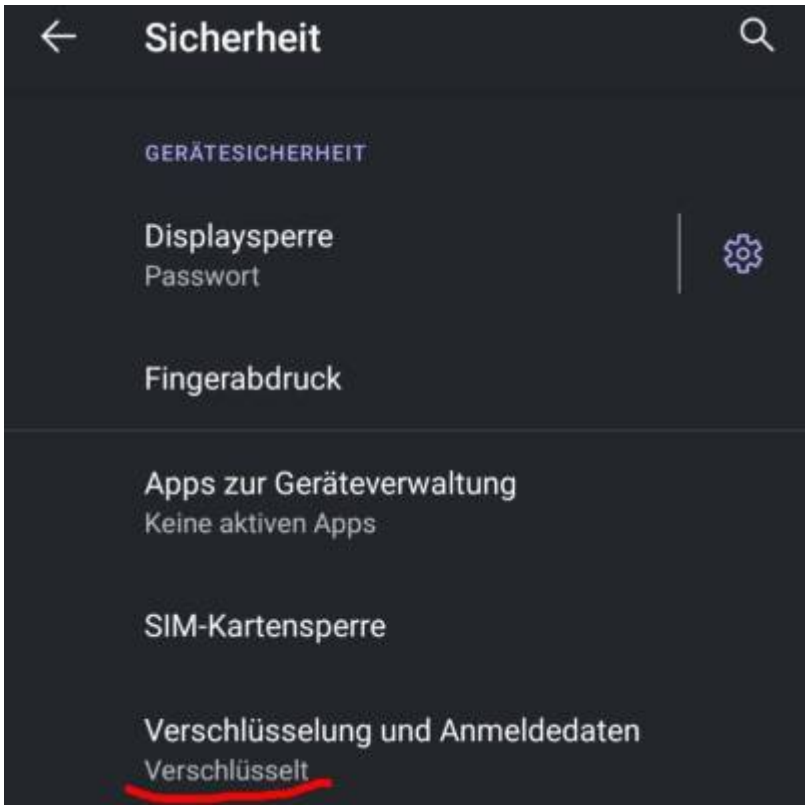
Vergesst nicht auch eure SD-Karte zu verschlüsseln!

Android verschlüsseln

Android bietet bei neueren Geräten eine Systemverschlüsselung meist beim ersten Einschalten des Gerätes an. Später lässt sich dies jederzeit einfach über Einstellungen nachholen. Je nach Hersteller oder Android-Version variieren die einzelnen Menüpunkte, jedoch ist der Vorgang meist sehr ähnlich: ***Einstellungen → Sicherheit***

Oft muss man das Gerät aufladen, wenn die Akkukapazität nicht ausreicht. Dies erkennt mensch daran, dass eine Fehlermeldung erscheint. Wenn das passiert einfach Smartphone anschließen.

Sobald es genug Akku hat, einfach unten auf Gerät verschlüsseln klicken. Der Ladevorgang kann einige Zeit dauern, je nachdem wie viele Daten sich auf deinem Smartphone befinden.



Apple iOS verschlüsseln

Auch bei **iOS** ist bei neueren Geräten der Speicher standardmäßig verschlüsselt, Es muss nur ein Passcode eingestellt werden. Zu erreichen ist dies unter
general settings → Toch ID & Passcode.

Eine genauere Anleitung zu iOS-Verschlüsselung findest du hier:
https://ssd.eff.org/en/module/how-encrypt-your-iphone.

Verschlüsseln und sich den Gefahren trotzdem bewusst sein
Auch ein verschlüsseltes Handy kann viel über dich verraten: Einerseits besteht die Gefahr, dass dir dein Handy in entsperrtem Zustand weggenommen wird – dann können die darauf gespeicherten Daten (Fotos, Nachrichten, etc.) ausgelesen werden. Anderseits sendet ein Handy IMMER (auch wenn es verschlüsselt ist) bestimmte Daten an deinen Provider. Dabei handelt es sich vor allem um Standortdaten und klassische Telefonate. Diese Informationen fragt die Polizei auch in bestimmten Fällen bei dem Provider nach. Sollte man daher seinen Standort anonym behalten wollen, muss man das Handy zuhause lassen, ausschalten oder in den Flugzeugmodus versetzen. Es gibt auch Täschchen, die davor schützen.

Jede Verschlüsselung ist nur so sicher wie ihr Passwort.
Deine Geräteverschlüsselung wirkt nur dann, wenn dein Handy ausgeschalten ist!

Sichere Passwörter verwenden

Bekommt jemand Zugriff auf dein verschlüsseltes Gerät, benötigt die Person zuerst dein Passwort. **Überlegt euch ein gutes Passwort.** Wie du grundsätzlich sichere, aber dennoch leichtmerkbare Passwörter erstellen kannst, kannst du hier im wiki nachlesen.

Im Falle von Smartphones müssen Passwörter nicht ganz so lang sein, denn hier verhindert meist das System ein zu schnelles durchprobieren von Möglichkeiten. Trotzdem hat es Knack-Software bei PINs besonders leicht: Es stehen nur 10 Variablen zur Verfügung und oft werden 4-stellige PINs verwendet - das ist für die richtige Software eine Sache von Minuten bis der „Schutz“ geknackt ist. Außerdem könnte dieser Schutz aus unterschiedlichen Gründen eventuell ausgehebelt werden und dann ist wieder das Passwort die letzte Verteidigung.

Du solltest also darauf achten keine kurze PIN oder ein einfaches Swipe-Muster zu wählen, denn die sind zB über Spuren am Display oder Überwachungskameras leicht zu erkennen.

Pin-Länge: Gehe bei der Länge der PIN an deine absolute Schmerzgrenze der Praktibilität im Alltag! Besser wäre eine Passphrase.

Von der Verwendungs Biometrischer Daten raten wir ab, sie bieten in mehreren Hinsichten nur ungenügenden Schutz!

Sichere Backups erstellen

Auch die beste Verschlüsselung bringt euch nichts, wenn im Hintergrund ein unverschlüsseltes Backup gemacht wird. Achtet darauf Backups ebenfalls zu verschlüsseln, am besten ihr schaltet die automatischen Backups aber einfach aus und macht selbst hin und wieder ein Backup auf eure verschlüsselte Festplatte.

Einstellungen am Smartphone für mehr Sicherheit

Hier beziehen wir uns in den konkreten Einstellungsanleitungen auf Android-Geräte. Je nach Gerät, können die einzelnen Einstellungsschritte abweichen, sind aber in den meisten Fällen identisch.

Berechtigungen einschränken

Smartphones speichern viele sensible Daten. Mit Hilfe bestimmter Android-Systemfunktionen können Apps solche Daten abrufen oder selbst generieren. Dafür benötigen sie Zugriffsrechte. Apps sind technisch auf das beschränkt, was ihnen per Berechtigung zugestanden wird. Hat eine App also

keinen Zugriff auf die Speicher-Funktion, kann sie von dort auch keine Fotos laden oder selbst welche ablegen.

Gewährt man einer App beim Einrichten Zugriffsrechte, kann die App anschließend bestimmte Dienste erbringen. In neueren Android-Versionen fordern Apps Rechte meist erst an, wenn sie sie auch wirklich benötigen. Der Zugriff auf die Kamera-Berechtigung wird in einer Banking-App beispielsweise erst abgefragt, wenn man seine Überweisung einscannen will.

Möchte man eine Berechtigung nachträglich wieder entziehen, kann man das über
Einstellungen → Apps → App-Name → Berechtigungen
tun. **Ab der Version 6** können App-Berechtigungen angezeigt und einzeln entfernt werden. **Ab Android 10** ist eine noch feinere Einstellung möglich: Man kann festlegen, dass Berechtigungen einer App nur während ihrer aktiven Nutzung gewährt sind. So wird etwa der Standort automatisch abgerufen, wenn die Navigations-App geöffnet wird, ansonsten aber nicht.

Datensammel-Apps: Manche Apps fordern wesentlich mehr Berechtigungen an, als für ihre Funktion notwendig wäre. Wenn etwa ein Taschenrechner Zugriff auf WLAN, Standort-Daten und Adressbuch haben möchte, bedeutet das wahrscheinlich, dass diese App vor allem dazu programmiert wurde, Nutzer:innendaten zu sammeln.
Wir empfehlen, den App-Store F-Droid (weiter unten im Artikel). Sonst jedoch vor der Installation einer App im Google Play-Store die Liste der möglichen Zugriffe anzeigen lassen. Ist die Liste unnötig lang, gibt es in der Regel eine bessere Alternative. **Apps, die deine Privatsphäre respektieren, empfehlen wir weiter unten im Artikel.**

Die geläufigste Art von App-Berechtigungen sind die so genannten „zustimmungspflichtigen Berechtigungen“. Dazu gehören beispielsweise Kamera, Mikrofon und Standort - eben alle Zugriffe, die häufig von Apps verlangt werden und über die du durch eine Abfrage informiert wirst.

Vertiefung:
Zur weiteren Auseinandersetzung mit App-Berechtigungen und Tipps dazu empfehlen wir 2 Artikel von mobilsicher.de.

Weitere Einstellungs-Tipps

o Sperre deine SIM Karte
Einstellungen → Sicherheit → SIM-Kartensperre

---

o Setze das Zeitlimit der automatischen Sperre des Displays möglichst kurz
Einstellungen → Sicherheit → Displaysperre (Einstellungen)

---

o Standortermittlung immer ausschalten, wenn es im Moment nicht benötigt wird
Einstellungen → Standort → Standort verwenden aus

---

o Wlan und Bluetooth immer ausschalten wenn es nicht benützt wird.

Einstellungen → Netzwerk & Internet → WLAN
und
Einstellungen → Verbundene Geräte → Verbindungseinstellungen → Bluetooth
und
Einstellungen → WLAN- und Bluetooth-Suche → beides deaktivieren

---

o NFC ausschalten
Einstellungen → Verbundene Geräte → Verbindungseinstellungen

Hier ist eine **Checkliste Handyeinstellungen** von mobilsicher.de was du bei den Handy-einstellungen beachten musst.

Android datensparsam nutzen

Wenn wir von mehr Datenschutz auf unseren Smartphones (hier Android) sprechen, dann geht es v.a. mal darum Google da einzuschränken wo es geht.

Datensparsamkeit: Wie du dein Google-Konto möglichst auf Datensparsamkeit einstellen kannst, kannst du bei mobilsicher.de nachlesen.

Stecken wir jedoch das Ziel höher, sprich: Android (möglichst) **ohne** Google, müssen noch andere Komponenten miteinbezogen werden. Zu dieser Überlegung gehören mitunter:

- **Betriebssystem**: LineageOS, eine quelloffene Android-Betiebssystemvariante, steht für viele Smartphones zur Verfügung und enthält von Beginn an keine Google-Apps. Neben LineageOS gibt es noch weitere Betriebssysteme, welche den Anspruch haben, möglichst ohne Google auszukommen. Da die Software Android im Kern quelloffen (Open Source) ist, haben verschiedene Entwickler:innen und Communitys auf Android basierende freie Betriebssysteme entwickelt. Bedienen lassen sie sich ähnlich wie „normale“ Android – ohne dass Google viele Nutzungsdaten erhält. Dazu gehören neben LineageOS beispw. auch /e/ und GrapheneOS.
- **App-Store**: Es gibt neben dem Google Play Store noch andere Möglichkeiten, um Apps herunterzuladen und zu installieren. Im App-Store F-Droid (auch weiter unten in App-Empfehlung zu finden), werden nur freie und quelloffene Apps angeboten. Wenn du dort jedoch die gewünschte App nicht finden kannst, empfehlen wir die zusätzliche Nutzung vom Aurora-Store.
- **Apps, Dienste und Tools**: Überlege dir, welche Apps du wirklich benötigst und welche Berechtigungen Apps etc. von dir verlangen. Am besten du steigst schrittweise auf quelloffene Apps um und verabschiedest dich gleichzeitig von diversen Google E-Mail- oder Karten-Diensten.
- **Einstellungen**: Wie schon oft hier erwähnt, kommt es ebenfalls auf die Aktivierung der Geräteverschlüsselung, Passwort- bzw. PINwahl oder etwa der Deaktivierung (auch bei LineageOS!) der Telefonnummernsuche an.

Werde unbequem: Die eigene wohlbekannte Bequemlichkeit zu überwinden, ist natürlich einer der wesentlichsten Komponenten
Unser Lese-Tipp: lies dir den Artikel von digitalcourage.de mal durch
Persönlicher Sicherheitsplan Das ist unser Leitfaden wie du deine digitale Sicherheit ausbauen kannst. Du findest ganz konkret Tipps zu einem möglichen Vorgehen und empfohlene Programme.

Empfohlene Apps

Wir haben uns hier einige wenige Apps herausgepickt um sie zu empfehlen. Es gibt natürlich viele weitere wunderbare Apps :)

F-Droid

F-Droid ist der App Store für Freie Software. Wenn möglich, sollte Software aus diesem Store installiert werden. F-Droid muss einmalig manuell installiert werden. Dazu mit dem Browser des frisch installierten Android die F-Droid Seite aufrufen, »F-Droid herunterladen« auswählen und den Anweisungen folgen. Leider sind auch einige Open-Souce Apps nicht im F-Droid Store verfügbar. Darunter so wichtige Apps wie Firefox, Signal Messenger] und der VLC Media Player.

Aurora Store

Um auch Apps installieren zu können, die du nur über den Google Play Store beziehen kannst, kannst du dir Aurora installieren. Diese App bekommst du ebenfalls in F-Droid. Mit dem Aurora Store kannst du jede kostenlose App aus dem Google Play Store installieren. Mit dem Vorteil, dass du jetzt aber kein Google-Konto für dein Android-Handy/Google Play Store angeben musst. Aurora Store kann auch so konfiguriert werden, dass es auf Aktualisierungen für die installierten Apps hinweist.

Firefox-Browser

Wir empfehlen Firefox als Browser. Firefox wird von einer unabhängigen Stiftung entwickelt, die das Bedürfnis nach Privatsphäre zumindest einigermaßen ernst nimmt. Firefox ist nicht im F-Droid Store verfügbar, stattdessen kannst du Fennec F-Droid installieren. Das ist eine fast identischer Klon, aus dem einige unfreie Bestandteile entfernt wurden und der lediglich aus markenrechtlichen Gründen nicht Firefox heißt. Den klassischen Firefox kannst du sonst über den Aurora Store installieren.

Für mehr Privatsphäre sollten zusätzlich folgende Firefox AddOns installiert werden:
- uBlock orgin als Werbe-Blocker
- Privacy Badger als Schutz vor Tracking
- HTTPS Everywhere um möglichst sichere Verbindungen zu Webseiten aufzubauen.

Tor-Browser

Falls es mal wichtig ist richtig anonym zu sein, kannst du den Tor-Browser verwenden. Die App kann über den Aurora Store, den Google Play Store oder F-Droid installiert werden. Bei F-Droid musst du in den Einstellungen die Paketquellen vom Guardian Project aktiviert haben. Zusätzliche Add-Ons können den Tor Browser deanonymisieren und sollten auf keinen Fall installiert werden!

Orbot

Auch andere Apps als der Tor Browser können mithilfe von Orbot über das Tor Netzwerk geleitet und anonymisiert werden. Du kannst auch den VPN-Modus verwenden, um deinen gesamten Internet-Verkehr über das Tor-Netzwerk zu tunneln. Bedenke aber, dass viele Apps nicht für Anonymität optimiert sind und womöglich deine Zeitzone, Geräte-Name oder andere, deanonymisierende Infos preisgeben könnten. Im Systemli-Wiki findest du eine Anleitung für die Benutzung von Orbot.

Osmand
Auch wenn wir das Internet nach dem Weg fragen, kommt die Antwort üblicherweise von Apple oder Google. Standardmäßig können diese Dienste unseren Standort permanent überprüfen und umfassende Bewegungsprofile erstellen. Ortungsdienste müssen manuell in den Programmeinstellungen deaktiviert werden. Ist die Ortungsfunktion auf dem Smartphone aktiviert, werden zudem sämtliche mit dem Telefon gemachten Fotos mit Informationen über Standort und Zeit der Aufnahme, sogenannten Metadaten, versehen. So können Dienste, die Zugriff auf Fotos haben, jederzeit rekonstruieren, wo und wann ein Foto gemacht wurde. Die Ortungsfunktion sollte also wenn immer möglich deaktiviert werden. Zur Navigation kann OsmAnd verwendet werden. Die App hat sehr umfangreiche Funktionen und ist zu Beginn etwas gewöhnungsbedürftig. Kartensätze müssen für die entsprechenden Regionen runtergeladen werden. Dafür funktioniert die Navigation anschließend auch ohne Internet-Verbindung. Also z. B. im Ausland oder wenn man Mobilfunk-Verbindung und WLAN ausschaltet. Da alle Routen-Berechnungen und das Darstellen der Karten auf dem Gerät passieren, ist die App etwas langsamer als man es vielleicht von Google Maps gewohnt ist. Dafür verrät man nicht jedes mal an einen großen Konzern (und potentiell anderen Mithorchenden), wo man gerade ist, wo man hin will und was man unterwegs macht. OsmAnd lässt sich aus dem F-Droid Store installieren. Die Version dort hat mehr Features als die kostenlose Version im Google Play Store.

Messenger Signal
Signal ist eine App über die du verschlüsselt Nachrichten austauschen und verschlüsselt telefonieren kannst. Du kannst sie einfach im Aurora-Store(oder einfach über den Play Store) runterladen. Signal ist besonders gut als Standard-SMS App für den Alltag geeignet. Mehr zu Signal findest du hier im Wiki.

Messenger Briar
Der Messenger Briar setzt verstärkt auf Sicherheit und Anonymität. Briar eignet sich als gut für Kommunikation bei der noch höhere Sicherheitsmaßnahmen getroffen werden sollten, für die Alltagskommunikation ist sie leider nicht angenehm zu verwenden und deswegen nicht geeignet. Mehr zu Briar findest du hier im Wiki.

Zum Weiterlesen: Empfohlene Guides und Anleitungen

Take back Control: Grundsätzlich empfehlen wir zum Thema Smartphonesicherheit eine Artikelreihe vom Kuketz-Blog.

- Grundlagen auf English findest du bei security in a box.
- mobilsicher.de gibt allgemein einen guten Überblick über Smartphonesicherheit.
- Hier findest du einige App-Empfehlungen.