Dein Smartphone absichern – Schritt für Schritt

So schützt du deine Daten auf Android und iPhone

Warum Sicherheit auf dem Smartphone heute unverzichtbar ist

Das Smartphone ist für die meisten Menschen heute mehr als nur ein Telefon: Es ist ein Kalender, ein Fotoalbum, ein Briefkasten, eine Geldbörse, ein Navigationssystem und ein Schlüssel zu vielen persönlichen Informationen. Es enthält Nachrichten, E-Mails, Login-Daten, Bankverbindungen, Gesundheitsdaten und vieles mehr. Umso erstaunlicher ist es, wie oft Geräte **ohne Passwort**, **ohne Ortung** oder mit **viel zu großzügigen App-Berechtigungen** genutzt werden.

In dieser Anleitung lernst du, wie du dein Smartphone **sicherer und datenschutzfreundlicher** einrichtest – egal ob du Android oder iOS nutzt. Die einzelnen Maßnahmen sind leicht umzusetzen und erfordern kein Vorwissen.

1. Die richtige Bildschirmsperre einrichten

Die Bildschirmsperre ist die erste und wichtigste Verteidigungslinie deines Smartphones. Sie verhindert, dass jemand unbefugt auf dein Gerät zugreifen kann, wenn du es verlierst oder es gestohlen wird. Leider nutzen noch immer viele Menschen entweder **gar keine Sperre**, oder sie verwenden zu **einfache Muster oder PINs**.

Warum das wichtig ist:

Stell dir vor, dein Smartphone liegt verloren in der Bahn. Ohne Sperre hat jeder Zugriff auf deine Banking-App, deine E-Mails, deine Fotos, WhatsApp-

Nachrichten und mehr. Mit einer guten Sperre hat niemand eine Chance – selbst bei physischem Zugriff.

So richtest du die Sperre ein:

Auf Android:

1. Öffne die **Einstellungen** deines Geräts.
2. Gehe zu **Sicherheit** oder **Sperrbildschirm** (je nach Hersteller unterschiedlich).
3. Wähle eine **Sperrmethode**:
   a) **PIN** (mind. 6 Ziffern, nicht „123456“ oder Geburtsdatum!)
   b) **Passwort** (stark empfohlen, aber weniger bequem)
   c) **Muster** (nicht empfohlen, da oft leicht zu erraten)
   d) **Biometrisch**: **Fingerabdruck** oder **Gesichtserkennung**
4. Stelle ein, dass dein Gerät sich **nach kurzer Inaktivität sperrt** (z. B. nach 30 Sekunden).

Auf dem iPhone:

1. Öffne die **Einstellungen**.
2. Gehe zu **Face ID & Code** oder **Touch ID & Code**.
3. Wähle einen **individuellen Code** (nicht nur 4 Zahlen!).
4. Aktiviere die **biometrische Entsperrung** (Face ID oder Touch ID).
5. Stelle ein, dass der Bildschirm sich **automatisch sperrt**, z. B. nach 30 Sekunden.

2. Ortungsfunktionen und Diebstahlschutz aktivieren

Falls du dein Smartphone verlierst oder es gestohlen wird, zählt jede Minute. Mit aktivierter Ortungsfunktion kannst du dein Gerät **fernortung**, **sperren**, oder sogar **löschen**, bevor jemand auf deine Daten zugreifen kann.

Android: „Mein Gerät finden“ aktivieren

1. **Einstellungen → Google → Sicherheit → Mein Gerät finden**
2. Stelle sicher, dass diese Funktion **aktiviert** ist.
3. Der Standort muss eingeschaltet sein, damit das Gerät gefunden werden kann.
4. Melde dich im Notfall unter https://google.com/android/find an, um dein Gerät zu orten, zu sperren oder zu löschen.

Tipp: Du kannst dein Gerät klingeln lassen – sogar wenn es auf „Lautlos“ steht.

iPhone: „Wo ist?“ aktivieren

1. Öffne die **Einstellungen**.
2. Tippe oben auf deinen Namen → **Wo ist?**
3. Wähle **„Mein iPhone suchen“**.
4. Aktiviere:
    a) **„Mein iPhone suchen“**
    b) **„Letzten Standort senden“** (hilfreich bei leerem Akku)
5. Im Notfall öffne https://icloud.com/find

Falls dein iPhone gestohlen wird, kannst du es **aus der Ferne komplett sperren oder löschen** – niemand kann es danach benutzen.

3. App-Berechtigungen regelmäßig prüfen

Viele Apps fordern Zugriff auf Daten, die sie gar nicht brauchen: Taschenlampen-Apps, die deinen Standort möchten, Spiele, die deine Kontakte lesen – das ist unnötig und ein **Risiko für deine Privatsphäre**.

So überprüfst du die Berechtigungen:

Auf Android:

1. **Einstellungen** → **Apps** → gewünschte App → **Berechtigungen**
2. Entziehe unnötige Rechte wie:
    a) Standort
    b) Kamera
    c) Mikrofon
    d) Kontakte
    e) SMS
3. Für eine Übersicht über alle Apps:
    a) **Einstellungen** → **Datenschutz** → **Berechtigungsmanager**

Du siehst hier, welche Apps z. B. Zugriff auf dein Mikrofon haben

Auf dem iPhone:

1. **Einstellungen** → **Datenschutz & Sicherheit**
2. Wähle z. B. **Kamera**, **Mikrofon**, **Ortungsdienste** – dort werden alle Apps mit Zugriff gelistet
3. Oder: **Direkt bei der App** im unteren Teil der Einstellungen

Tipp: Nutze bei Ortung die Einstellung **„Nur beim Verwenden der App“** – nicht „Immer“!

4. Datenschutz-Einstellungen optimieren

Jedes Smartphone sendet standardmäßig Daten an den Hersteller (Google oder Apple), an App-Anbieter und andere Dienste. Viele dieser Übertragungen kannst du **einschränken oder deaktivieren**, um deine Privatsphäre zu schützen.

Android: Wichtige Datenschutz-Einstellungen

1. **Google-Aktivitäten**:
    a) **Einstellungen → Google → Datenschutz**
        i. Deaktiviere z. B.:
            1. „Web- und App-Aktivitäten“
            2. „Standortverlauf“
            3. „YouTube-Verlauf“

Oder verwalte sie unter myactivity.google.com

2. **Werbung personalisieren**:
    a) **Einstellungen → Google → Anzeigen**
    b) Deaktiviere: **Personalisierte Werbung**

3. **Sperrbildschirm**:
    a) Deaktiviere Inhalte von Nachrichten auf dem Sperrbildschirm:
        i. **Einstellungen → Benachrichtigungen → Sperrbildschirm**

iPhone: Wichtige Datenschutz-Einstellungen

1. **Analyse & Datenweitergabe**:
    a) **Einstellungen → Datenschutz & Sicherheit → Analyse & Verbesserungen**
        i. Deaktiviere alles (z. B. „Daten mit Apple teilen“)

2. **Ortungsdienste**:
    a) **Einstellungen → Datenschutz & Sicherheit → Ortungsdienste**
        i. Jede App einzeln prüfen – ideal ist: „Beim Verwenden der App“

3. **Siri & Spracheingabe**:
    a) Wenn du es nicht nutzt: Siri deaktivieren unter **Siri & Suchen**

4. **Werbung einschränken**:
    a) **Einstellungen → Datenschutz & Sicherheit → Apple Werbung**
        i. „Personalisierte Werbung“ deaktivieren

5. Weitere Sicherheitstipps für den Alltag

1. Nutze **ausschließlich offizielle App Stores** (Google Play / App Store).

2. Halte dein System **immer aktuell** – Updates enthalten wichtige Sicherheitsfixes.

3. Deaktiviere **Bluetooth** und **WLAN**, wenn du sie nicht brauchst.

4. Verzichte auf **automatische Verbindungen** zu offenen Netzwerken.

5. Nutze für sensible Apps (z. B. Banking) **zusätzliche App-Sperren**.

6. Erstelle regelmäßig ein **Backup** (Google-Konto / iCloud / lokal).

Fazit: Sicher in wenigen Minuten

Die meisten Menschen unterschätzen, wie viele persönliche Daten auf dem eigenen Smartphone gespeichert sind – und wie leicht Dritte darauf zugreifen könnten. Mit ein paar gezielten Einstellungen kannst du dein Gerät jedoch **sehr gut schützen** – ganz ohne Technikkenntnisse.

Wenn du dein Smartphone heute absicherst, schützt du nicht nur deine Daten – du schützt auch deine Identität, deine Kontakte, dein Geld und deine Privatsphäre.