Smartphone Sicherheitscheck

LANDESANSTALT FÜR MEDIEN NRW
Der Meinungsfreiheit verpflichtet.

Schaffst du alle Security-Level?

Hinweis: Insbesondere bei Android-Geräten können sich die Bezeichnungen einzelner Einstellungen zwischen unterschiedlichen Herstellern (z. B. Samsung, Huawei) unterscheiden. Tipp: Nach ähnlichen Bezeichnungen für Optionen in den Einstellungen schauen.

Ist eine einzelne Option auch so nicht zu finden, dann hilft die Suche-Funktion in den Einstellungen.

TUTORIAL > *GUT GESTARTET*

Passwort für SIM und Bildschirm	**Android:** In den Einstellungen unter Bildschirmsperre & Sicherheit eine SIM-Pin eingeben und Bildschirmsperre aktivieren. Außerdem im Punkt Sperrbildschirm Bildschirmsperre aktivieren. Tipp: In den Sicherheitseinstellungen Kennwörter sichtbar bzw. Passwörter sichtbar machen deaktivieren. **iOS:** In den Einstelllungen unter Mobiles Netz den SIM-Pin festlegen. Für die Bildschirmsperre unter Einstellungen Touch ID & Code oder Face ID & Code wählen und dort Code aktivieren.
Sichere Passwörter	So sollte dein sicheres Passwörter für die Bildschirmsperre gestaltet sein: • Mit Groß- und Kleinbuchstaben + Zahlen + Sonderzeichen • Möglichst lang (richtig sicher wird es ab 12 Zeichen) • Keine persönlichen Daten, z. B. Namen, Geburtsdatum Überprüfe es auf **www.CheckDeinPasswort.de**

LEVEL 1 SICHER GEGEN DIEBE

Gerät verschlüsseln	**Android:** In den Einstellungen unter Sicherheit bzw. Bildschirmsperre & Sicherheit SD-Karte und Gerät verschlüsseln. **iOS:** Die Daten sind standardmäßig auf dem internen Speicher verschlüsselt.
Find my device	**Android:** Mit „Find My Device“ (google.com/android/find) kann das Smartphone geortet, gesperrt und die Daten gelöscht werden. Hersteller wie Samsung bieten teils eigene Apps und Dienste an. **iOS:** Mit der App „Mein iPhone suchen“ und über icloud.com kann das Gerät geortet, gesperrt oder gelöscht werden. Unter Passwörter & Accounts und iCloud die Option Mein iPhone suchen aktivieren.
IMEI notieren	**Android & iOS:** In der Telefon-App mit der Tastenkombination *#06# die IMEI abrufen. Diese für jedes Gerät individuelle Nummer kann helfen das Smartphone bei Diebstahl zu identifizieren. Auch eine Sperrung ist damit bei einigen Netzbetreibern möglich.

LEVEL 2 DATEN SCHÜTZEN

Ortungsdienste regeln	**Android:** Mit dem Finger vom oberen Bildschirmrand herunterwischen. In der Übersicht können Dienste (z. B. Standort) deaktiviert werden. **iOS:** In den Einstellungen Datenschutz und Ortungsdienste wählen und pro App einstellen.
Ad- und App-Tracking	**Android:** In den Einstellungen den Menüpunkt Konten und dann Google auswählen. Auf Daten & Personalisierung tippen und dort Zu den Werbeeinstellungen wählen (beim Punkt „Personalisierte Werbung“). Dort personalisierte Werbung deaktivieren. **iOS:** In den Einstellungen bei Datenschutz unter Werbung das Ad-Tracking beschränken aktivieren.

LEVEL 3 MONEY MONEY MONEY

Passwort für In-App-Käufe	**Android:** Im Play Store die Menü-Taste tippen, um zu den Einstellungen zu gelangen. Dort unter Authentifizierung für Käufe erforderlich Für alle Käufe wählen und mit Passwort bestätigen. **iOS:** In den Einstellungen unter Bildschirmzeit den Punkt Beschränkungen auswählen. Im Bereich Käufe im iTunes & App Store die Option „Passwort immer erforderlich“ wählen.
Kostenfallen	Nicht auf SMS von fremden Nummern antworten und unbekannte Lockanrufe ignorieren. **Hinweis:** Mehr Tipps zu Kostenfallen gibt es bei **www.handysektor.de/abzocke**

LEVEL 4 ENDBOSS APPS

Nur Apps aus vertrauenswürdigen Quellen installieren	**Android:** Wir empfehlen nur Apps aus dem Google Play-Store zu installieren, in dem zumindest eine automatisierte App-Überprüfung stattfindet. Alternative Stores sind oft nicht vertrauenswürdig und daher nicht zu empfehlen. **iOS:** iOS erlaubt nur die Installation von Apps aus dem App Store.
App-Berechtigungen prüfen	**Android & iOS:** Beim ersten Öffnen einer App fragt diese einzeln Zugriffe auf Daten und Funktionen ab. **Android:** Bei bereits installierten Apps sind diese auch in den Einstellungen unter Anwendungen bzw. Apps einsehbar und für jede App anpassbar. **iOS:** Bei bereits installierten Apps sind diese auch in den Einstellungen unter Datenschutz einsehbar und für jede App anpassbar.
Einzelne Apps mit Passwort sichern	**Android:** Einzelne Anwendungen können mit einem Passwort gesichert werden. Dafür wird allerdings bei den meisten Geräten eine Hilfs-App benötigt, z. B. AppLock. **iOS:** iOS bietet keine entsprechende Option.

BONUSLEVEL ! WEITERMACHEN!

Updates für Apps und Betriebssystem	**Android:** App-Updates werden in der Regel vom Play Store gemeldet oder automatisch durchgeführt. Im Play Store im Menü unter Meine Apps und Spiele prüfen, ob Updates verfügbar sind. Ein Update für das Android-Betriebssystem wird ebenfalls automatisch gemeldet. Alternativ in den Einstellungen in den Geräteinformationen nachschauen, ob ein Software-Update verfügbar ist. **iOS:** App-Updates können automatisch durchgeführt werden. Dazu in den iTunes & App Store-Einstellungen die Automatischen Downloads für App-Updates aktivieren. Alternativ im App Store unter Updates Aktualisierungen suchen. Das Gerät meldet, wenn eine Aktualisierung für das Betriebssystem verfügbar ist. Manuell kann das in den Einstellungen unter Allgemein und Softwareupdate geprüft werden.
Nicht genutzte Apps löschen	**Android:** In den Einstellungen den Anwendungsmanager oder Apps aufrufen. In der Übersicht die App auswählen und über den Deinstallieren-Button entfernen. **iOS:** Die gewünschte App antippen und halten. Auf das erscheinende Kreuz tippen und deinstallieren. **Hinweis:** Manche System-Apps lassen sich nicht löschen, aber in den Einstellungen unter Bildschirmzeit, Beschränkungen und dort bei der Option Erlaubte Apps deaktivieren.
Backups machen	**Android:** Einige Hersteller bieten Backup-Tools zur Sicherung auf dem Computer an. **iOS:** Über iTunes kann ein Backup am Computer erstellt und Daten synchronisiert werden. **Alternative:** Cloud-Dienste (z. B. Dropbox, Google Drive, iCloud) helfen ebenfalls dabei, wichtige Dateien zu sichern und auf anderen Geräten verfügbar zu machen. Dieser Komfort kann jedoch zu Lasten des Datenschutzes gehen.
Hotspots vorsichtig nutzen	Manche Apps übertragen Daten nicht verschlüsselt. Ist ein Hotspot öffentlich können sie mitgelesen werden. Übertrage in öffentlichen Hotspot daher keine sensiblen Daten, z. B. deine Kontodaten oder andere persönliche Infos. Weiche dafür auf die mobile Datenverbindung aus!