Fremdzugriff auf Handy erkennen und Spionage bekämpfen

In diesem Tipp erfahren Sie, wie Sie einen Fremdzugriff auf ihr Handy erkennen können und wie Sie Spionage bekämpfen können.

Ein versehentlich geklickter Link oder eine lustig anmutende Spiele-App, die ohne Nachzudenken einfach installiert wird: Es sind solche **Unachtsamkeiten, die Hackern und Malware auf Smartphones Tür und Tor öffnen**. Meist bemerken die Besitzer den fremden Besuch erst, wenn neben dem **Eingriff in die Privatsphäre** auch bereits ein (persönlicher oder finanzieller) Schaden entstanden ist. **Mit unseren Tipps können Sie einen Fremdzugriff auf Ihrem Handy erkennen** und diesem pro aktiv vorbeugen. Außerdem erfahren Sie, **was Sie tun können**, **wenn Sie schon Opfer von Spyware geworden sind**.

- ✔ Spionage Apps richten meist unauffällig und unbemerkt im Hintergrund Schaden an.
- ✔ Auch Apple-Geräte werden immer öfter zum Ziel von Hackern und Schadsoftware.
- ✔ Fremdeinwirkungen können auch nach einer vollständigen System-Bereinigung weiterhin bestehen bleiben.

Inhalt [Ausblenden]

1. Was sind verdächtige Anzeichen für Spionagesoftware auf dem Handy?
   1.1. Der Akku wird plötzlich sehr schnell leer
   1.2. Auf Ihrem Gerät befinden sich unbekannte oder unerwünschte Apps
   1.3. Sie bekommen seltsame Textnachrichten
   1.4. Der Datentraffic ist ungewöhnlich hoch
   1.5. Das Gerät ist wird sehr heiß
   1.6. Das Smartphone funktioniert nicht mehr korrekt
2. Welche Maßnahmen zur Vorbeugung und zum Datenschutz gibt es?
   2.1. Nutzen Sie die eingebauten Schutzmöglichkeiten Ihres Smartphones
3. Was können Sie tun, wenn Sie bereits Opfer eines Fremdzugriff auf dem Handy geworden sind?
   3.1. Bei Spionage-Apps ist oft schon der Name Programm
   Ähnliche Artikel:

1. Was sind verdächtige Anzeichen für Spionagesoftware auf dem Handy?

Es gibt eine ganze Reihe von Indizien, die darauf hinweisen, **dass sich Schadsoftware auf Ihrem Smartphone befindet**. Damit Sie diese auch richtig deuten können, ist es **wichtig, dass Sie die normalen Verhaltensweisen Ihres Endgerätes kennen**.

1.1. Der Akku wird plötzlich sehr schnell leer

Schadsoftware saugt den Akku Ihres Smartphones leer.

Unter normalen Umständen nutzen Sie Ihr Smartphone locker zwei Tage mit einer Akku-Ladung, **seit einigen Tagen ist der Saft aber schon nach ein paar Stunden komplett alle**. Die Ursache dafür ist möglicherweise eine Spionagesoftware, die im Hintergrund ständig aktiv ist und dabei Akku-Leistung verbraucht.

1.2. Auf Ihrem Gerät befinden sich unbekannte oder unerwünschte Apps

Wenn sich plötzlich **Apps oder Programme** auf Ihrem Gerät befinden, **die Sie weder kennen noch installiert haben**, ist in jedem Fall Vorsicht geboten. Es besteht die Gefahr, dass es sich dabei um eine Spy-App handelt, **die sich als harmlose App tarnt**.

1.3. Sie bekommen seltsame Textnachrichten

Spionage-Tools werden oftmals aus der Ferne gesteuert. Dafür verwenden die Hacker Textnachrichten, die nach einem wirren Durcheinander aussehen, in denen allerdings **Anweisungen für die Software enthalten** sind. Für gewöhnlich bekommen Sie diese Codes gar nicht zu Gesicht. Falls doch, ist das **nur einem Fehlverhalten der Spy-App zu verdanken und Sie sollten sofort reagieren.**

1.4. Der Datentraffic ist ungewöhnlich hoch

In den Einstellungen Ihres Handys können Sie die Datennutzung überprüfen.

Auch **ein signifikanter Anstieg der Datennutzung sollte Sie in Alarmbereitschaft versetzen**. Greift jemand von außen auf Ihr Smartphone zu, werden automatisch auch Daten von Remote gesendet und empfangen.

In den Einstellungen Ihres Gerätes können Sie **die Peak-Zeiten des Anstiegs ermitteln**: Findet dieser beispielsweise vor allem nachts statt, müssen Sie **eine Malware als Verursacher in Betracht ziehen**.

1.5. Das Gerät ist wird sehr heiß

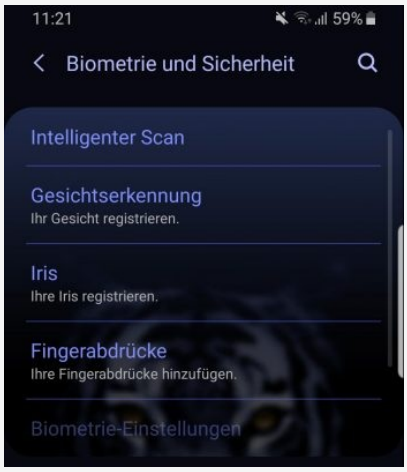
Ihr Smartphone wird so heiß, dass es Ihnen fast ein Loch in die Hosentasche brennt? Auch hier ist Vorsicht geboten, denn **Spionage Apps nutzen die GPS-Funktion**, **um den aktuellen Standort Ihres Gerätes zu ermitteln**. Die permanente Ortung kann im schlimmsten Fall sogar dazu führen, dass das Gerät überhitzt.

1.6. Das Smartphone funktioniert nicht mehr korrekt

Ganz klassische Anzeichen dafür, dass sich jemand Fremdes an Ihrem Telefon zu schaffen macht, sind **seltsame Verhaltensweisen und Fehlfunktionen**. Erhalten Sie bei Starten der Kamera lediglich eine Fehlermeldung oder flackert der Bildschirm kurzzeitig auf?

Gut möglich, dass Schadsoftware im Hintergrund auf Ihr Gerät zugreift. Auch **unerwartete Neustarts oder ein extrem langer Shutdown** können von Fremdzugriffen ausgehen.

2. Welche Maßnahmen zur Vorbeugung und zum Datenschutz gibt es?



Mittels PIN oder Biometrie-Scanner können Sie Ihr Smartphone gegen Fremdzugriffe schützen.

Oftmals reichen schon einige ganz einfache Maßnahmen, um Ihr Handy vor Schadsoftware oder Hackern zu schützen.

1. **Schalten Sie die Bildschirmsperre ein:** Sollten Sie Ihr Smartphone verlieren oder es gestohlen werden, verhindert die Bildschirmsperre im ersten Schritt unberechtigte Zugriffe. Für die Sicherung stehen drei Optionen zur Wahl:

- **PIN** (mindestens 6 Zeichen)
- **Biometrische Sicherung** (Fingerabdruck- oder Retina-Scanner)
- **Passwort** (Kombination aus Buchstaben, Zahlen und Sonderzeichen)

2. **Installieren Sie einen Virenschutz:** Ein Antivirusprogramm durchsucht Ihr Smartphone nach Malware (beispielsweise Viren, Trojaner, Ransomware oder Adware) und kann sogar **bestimmte Arten von betrügerischen Emails enttarnen**.

> **Gut zu wissen:** Für iOS gibt es nach derzeitigem Stand keine dedizierten Virenscanner. Mit speziellen Security-Paketen, wie beispielsweise der Avira iOS Security, können Sie Ihr Gerät aber trotzdem gegen Diebstahl schützen oder unseriöse Anrufe direkt blockieren.

2.1. Nutzen Sie die eingebauten Schutzmöglichkeiten Ihres Smartphones

3. **Richten Sie eine Verschlüsselung ein:** Alle aktuellen Smartphones besitzen eine Funktion, mit Sie den internen Gerätespeicher und die SD-Karte verschlüsseln können. Im Falle eines Diebstahls wird so **verhindert**, **dass Dritte Ihre Daten auslesen** können.

3. **Aktivieren Sie die Ortungs- und Fernwartungsfunktionen:** Mit Hilfe dieser Apps können Sie die genaue Position Ihres Handys ermitteln und es **bei Bedarf aus der Ferne sperren oder komplett löschen**. Per Remote-Zugriff auf die Kameras besteht zudem sogar die Möglichkeit, potenzielle Diebe „in flagranti“ zu fotografieren und an die Bilder an die Cloud zu senden.

> **Achtung:** Die Fernwartungsfunktionen sind nicht auf allen Versionen von Android verfügbar.

Sichern Sie Ihre Accounts bei WhatsApp, Google und Co. mit besonders starken Passwörtern.

5. **Richten Sie starke Passwörter ein:** Legen Sie sichere Passwörter für Konten bei Plattformen wie Facebook, Google oder WhatsApp fest ändern Sie diese möglichst regelmäßig. **Weisen Sie jedem Konto ein eigenes Kennwort zu**, so kann nicht gleich auf Ihre kompletten Daten zugegriffen werden, falls eins davon gehackt wird.

5. **Installieren Sie nur Apps und Programme aus bekannten Quellen:** Beugen Sie unbefugten Zugriffen vor, indem Sie nur Apps und Programme aus vertrauenswürdigen Stores und von seriösen Webseiten installieren. **Werden Sie hellhörig, falls eine App**

eine ungewöhnliche Berechtigung fordert (beispielsweise, wenn Spiele versuchen, auf Ihre SMS-Nachrichten zuzugreifen). Erteilen Sie entsprechende Berechtigungen nur Apps, die Sie kennen.

5. **Bleiben Sie immer auf dem neuesten Stand:** Die aktuellsten Security-Updates **schließen kritische Sicherheitslücken** und machen damit Hackern die Tür vor der Nase zu.

> **Tipp:** Über die Sicherheitseinstellungen Ihres Smartphones können Sie die die Berechtigung für die App-Installation aus unbekannten Quellen deaktivieren.

3. Was können Sie tun, wenn Sie bereits Opfer eines Fremdzugriff auf dem Handy geworden sind?

- **Überprüfen Sie, ob Ihr Android-Gerät gerootet wurde**. Suchen Sie dazu in den Apps nach klassischen Routing-Tools wie KingRoot oder SuperSu. Sollten Sie den Root nicht irgendwann selbst durchgeführt haben, ist die Option standardmäßig deaktiviert. Bei einem gerooteten Smartphone hilft in den meisten Fällen nur noch ein Rücksetzen auf die Werkseinstellungen.
- **iPhones müssen Sie hingegen auf die Anzeichen eines Jailbreaks** hin überprüfen: Sollten Sie nicht selbst Hand angelegt haben, kann zum Beispiel das **Vorhandensein der App „Cydia“ ein typisches Indiz** sein.
- Deaktivieren Sie die die Geräteadministratoren unbekannter Apps unter **„Sicherheit & Standort / Apps zur Geräteverwaltung“** und deinstallieren Sie die zugehörige Anwendung.

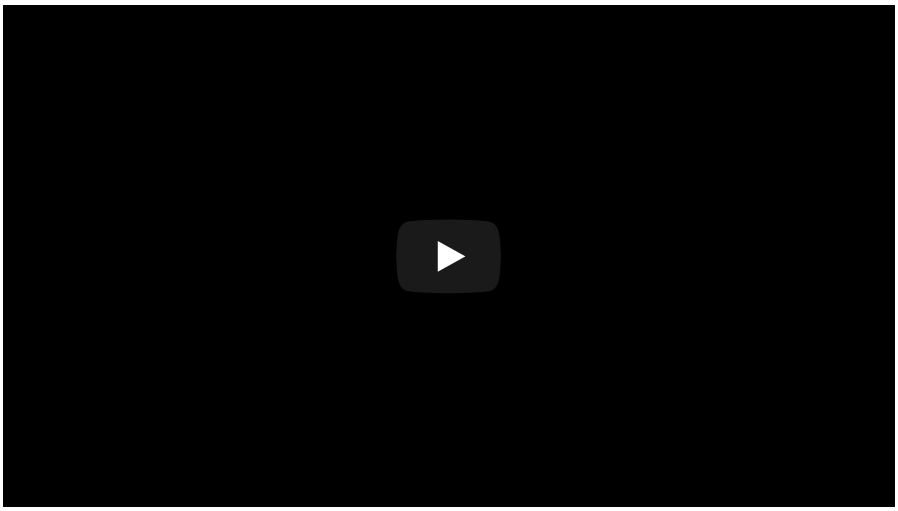
3.1. Bei Spionage-Apps ist oft schon der Name Programm

- **Prüfen Sie die Liste der installieren Apps auf unbekannte oder verdächtige Anwendungen** (z.B. deuten **Apps mit „Spy“ im Namen** für gewöhnlich bereits auf Ihre aushorchende Funktion hin) und deaktivieren oder entfernen Sie diese.

Bei Schadsoftware verheißt in der meisten Fällen schon der Name nichts Gutes.

- **Ändern Sie nach der Bereinigung Ihres Smartphones sämtliche Passwörter**, darunter auch die von Cloud-Diensten und Accounts (z.B. Google).

> **Achtung:** Bestimmte Messenger-Dienste wie WhatsApp oder Threema können Sie auch über den Browser nutzen. Einmal aktiviert, bleibt diese Option auch nach einer Bereinigung erhalten. Löschen Sie aus Sicherheitsgründen auch hier die Zugriffe, um Hackerangriffen zuvorzukommen.



- **Mit Anti-Spionage-Apps können Sie herausfinden, ob sich jemand an Ihrem Smartphone zu schaffen gemacht hat.** Sie

identifizieren Spionagesoftware anhand verschiedener Faktoren, wie beispielsweise unerlaubten Standort-Abfragen oder verdächtigen Berechtigungen. Snoop Snitch für Android warnt Sie beispielsweise vor SMS- und Standort-Spionage, während Looky-Looky für iOS neugierige Chefs oder schnüffelnde Partner auf frischer Tat bei Ihrer Überwachung ertappt.

- **Die drastischste Maßnahme**, um die Sicherheit Ihres Mobiltelefons wiederherzustellen, **ist natürlich das Rücksetzen auf Werkseinstellung**. Sichern Sie dafür vorab Ihre Daten und starten Sie den Reset über die Telefon-Einstellungen.

Ganz wichtig: Installieren Sie das Handy als neues Gerät, damit es sich nicht direkt aus dem Backup neu infiziert und **ändern Sie alle Passwörter erst nach dem Rücksetzen**. Sollte Ihr Smartphone nämlich mit einem Keylogger infiziert sein, erfährt dieser die neuen Passwörter noch vor dem Löschen.

37 Bewertungen

Ø 4,41

Ähnliche Artikel:

- Gebrochene Displays und Wasserschäden am Smartphone
- Laptop, Tablet und Co. richtig versichern
- Displayschutz – Auf diese Details kommt es an!
- Kindersicherung im Internet: So bewahren Eltern ihre…
- Malware durch E-Zigaretten? Durchaus!
- Keine Lücken in der Sicherheit – Penetration-Test

Weitere Rubriken:	Android, iOS, Mobil
Plattformen:	Android, iOS
Eingetragen am:	27.02.2019
Aktionen:	Aktionen