

INFORMIEREN. AGIEREN. VORBEUGEN.



[Neuer Schutz für Medikamente >](#)
[< Seniorpartner in School](#)

Digitales Stalking

Die Täter sehen alles



Opfer von digitalem Stalking werden über das eigene Smartphone ausspioniert

© aijiro/stock.adobe.com

Eine unangenehme Vorstellung: Jemand verschafft sich heimlich Zugriff auf das eigene Smartphone. Jede Konversation wird mitgelesen, jedes Foto eingesehen, jedes Telefonat mitgehört. Beim so genannten „digitalen Stalking“ installiert der Täter dazu unbemerkt eine App auf dem Handy seines Opfers und spioniert es im Anschluss aus. Wie man sich davor schützen kann, erklärt Dr. Michael Littger von der Initiative „Deutschland sicher im Netz“ (DsiN).

Legale Software - illegale Nutzung

„Im Grunde hat ein Täter vollständigen Zugriff auf das Gerät – er kann alles machen, was ich selbst auch machen kann, Nachrichten lesen, die Kamera einschalten – oder sich Fotos und Videos auf ein eigenes Gerät kopieren“, erklärt Michael Littger. Dafür benötigt der Täter zunächst direkten Zugriff auf das Handy des Opfers. Im Anschluss installiert er dann eine Überwachungs-App. Diese Apps werden legal angeboten – oftmals mit vorgeschobenen Begründungen wie die Möglichkeit, seine Kinder damit besser schützen zu können. „Es ist grundsätzlich zwar nicht verboten, eine solche Software anzubieten – das Installieren auf einem fremden Handy und das anschließende Ausspionieren ist jedoch illegal. Damit macht man sich strafbar“, betont der Experte. Denn nach [Paragraf 202a](#) des Strafgesetzbuchs ist das Ausspähen von Daten verboten. Auch andere Persönlichkeitsrechte können dabei verletzt werden.



Hohe Dunkelziffer

Bei den Tätern handelt es sich häufig um (ehemalige) Partner, Affären, Bekanntschaften oder Familienangehörige. „Da die Apps in der Regel manuell auf dem Handy installiert werden müssen, besteht meist ein persönlicher Kontakt zwischen Täter und Opfer“, erklärt Littger. Wie verbreitet das digitale **Stalking** ist, lässt sich schwer erfassen, aber es wird davon ausgegangen, dass die **Dunkelziffer** hoch ist. „Wir haben Hinweise von Anbietern von Sicherheitssoftware, dass die Zahl der entdeckten Apps stetig zunimmt – allein in Deutschland im letzten Jahr um über 70 Prozent. Auch wenden sich immer mehr verunsicherte Verbraucher an uns.“ Schauen Sie sich zusätzlich die Download-Zahlen der Anbieter solcher Apps an, müssen Sie davon ausgehen, dass weltweit tatsächlich mehrere Millionen Menschen **Opfer** von digitalem **Stalking** sind. „Diese drei Faktoren weisen zumindest darauf hin, dass es sich nicht mehr nur um ein Randthema handelt“, betont Littger.



Wie merke ich, dass ich betroffen bin?

Es gibt einige Hinweise, die darauf schließen lassen, dass man eine Spionage-App auf seinem Smartphone hat. Misstrauisch sollte man etwa werden, wenn plötzlich der Datenverbrauch extrem ansteigt, also wenn man sein Datenvolumen schneller als sonst verbraucht. Auch wird das Handy langsamer und der Akku entleert sich in kürzerer Zeit als üblich, wenn eine solche App installiert ist. Hintergrundgeräusche beim Telefonieren könnten ein Zeichen dafür sein, dass jemand mithört. „Zudem sollte man auf sein Umfeld achten. Weiß eine Person plötzlich mehr, als sie eigentlich wissen kann? Weiß sie Details über Telefonate oder andere Privatangelegenheiten?“, ergänzt Michael Littger. Spätestens dann sollte man die App-Übersicht im Handy überprüfen. Taucht dort eine unbekannte App auf, die man nicht selbst installiert hat? Dies kann man dann zum Beispiel über eine Google-Recherche überprüfen. „Wichtig ist, dass man die App nicht einfach löscht, sondern zunächst einen Screenshot macht, um Beweise zu sichern. Zudem wird der Täter gewarnt, wenn die App gelöscht wird. Falls möglich, sollte man das Handy erst einmal nicht mehr benutzen, sondern auf ein Zweitgerät umsteigen“, rät der Experte. Sinnvoll ist es auch, sämtliche Passwörter zu ändern. Zudem sollte man sich Hilfe suchen, etwa beim Weißen Ring und Anzeige bei der **Polizei** erstatten. Hat man einen Verdacht, wer der Täter sein könnte, ist es nicht ratsam, diesen selbst darauf anzusprechen. „Die **Polizei** kann zum Beispiel eine so genannte Gefährderansprache durchführen. Diese kann in vielen Fällen zum Erfolg führen“, weiß Michael Littger.

Mehr Tipps zum Schutz vor Digitalem **Stalking** gibt es auf der Webseite von **Deutschland sicher im Netz**. Die DsiN-App „SiBa“ (SicherheitsBarometer) warnt zudem vor aktuellen Sicherheitslücken. Die Seite **No Stalk** des Weißen Rings bietet konkrete Hilfe und Tipps für **Opfer** von **Stalking**.

Schutz vor digitalem Stalking

Um gar nicht erst **Opfer** von digitalem **Stalking** oder digitalen Angriffen zu werden, sollte man einige Sicherheitshinweise beachten:

- ▶ Schützen Sie Ihr Handy vor fremdem Zugriff, am besten mit einer sicheren PIN. Teilen Sie diese niemandem mit. Wechseln Sie die PIN regelmäßig.
- ▶ Aktivieren Sie, wenn möglich, die Zwei-Faktor-Authentifizierung in den Sicherheitseinstellungen des

- ▶ Endgeräts.
- ▶ Blockieren Sie App-Installationen aus unbekanntem Quellen.
- ▶ Kontrollieren Sie regelmäßig die Apps auf Ihrem Handy. Halten Sie diese auf dem aktuellen Stand. Entfernen Sie Apps, die Sie nicht brauchen.
- ▶ Schränken Sie die Zugriffsrechte von Apps ein – eine Taschenlampen-App benötigt keinen Zugriff auf Ihre Kamera!
- ▶ Installieren Sie einen Antivirenschutz auf Ihrem Handy und installieren Sie regelmäßig Sicherheitsupdates für das Betriebssystem.
- ▶ Nutzen Sie grundsätzlich sichere Passwörter, die Sie regelmäßig wechseln.

SBa (24.04.2020)

Folgende Artikel könnten Sie auch interessieren:

-  [Sichere IT im Homeoffice](#)
-  [Cloud-Dienste – Pro und Contra](#)
-  [Erwachsene als Ziel von Cybermobbing](#)
-  [Unseriöse Model-Castings](#)

[Alle Artikel dieser Kategorie](#)

© Verlag Deutsche Polizeiliteratur

Cookie Einstellungen



- Statistiken
- Essentiell

Wir nutzen Cookies auf unserer Website, die in unserer [Datenschutzerklärung](#) beschrieben sind. Wir verwenden anonyme Statistiken, um unsere Website zu verbessern. Bitte unterstützen Sie unsere wichtige Präventionsarbeit und akzeptieren Sie alle Cookies. Vielen Dank!

[Ablehnen](#) [Alle akzeptieren](#)