



[Sicher auf dem Elektrofahrrad >](#)

[< Einbruchschutz - Tipps zum richtigen Verhalten](#)

Vorsicht beim App-Download!

Das Smartphone vor Schadsoftware schützen



Im **Internet** tauchen immer wieder Apps von unseriösen Anbietern auf

© georgejmclittle, Adobe Stock

Spannende Spiele, unterhaltsame Chatprogramme und clevere Anwendungen, die den Alltag einfacher machen: Mit einem Klick können sich Smartphone- und Tablet-Nutzer in App-Stores eine Vielzahl an Anwendungen herunterladen – viele davon auch kostenfrei. Beim Herunterladen von Apps sollte jedoch vorher immer geprüft werden, ob der Download auch risikofrei ist. Denn wer Apps von unseriösen Anbietern herunterlädt, läuft Gefahr, sich ungewollt Schadsoftware zu installieren, kostenpflichtige Abonnements abzuschließen oder von Spionage-Software überwacht zu werden.

Risiken beim App-Download

Die Gefahren beim sorglosen Herunterladen von Apps sind vielfältig. Neben der unfreiwilligen Installation von Schadsoftware, über die unseriöse Anbieter das Smartphone steuern und somit zweckentfremden können, ist auch der **Diebstahl** sensibler Daten ein Risiko. Dabei werden Daten, die auf dem Smartphone gespeichert sind, im Hintergrund an den Anbieter der App geschickt, der diese für **Spam** oder Werbeaktionen nutzen kann. Martin Müsgens, Referent bei der Landesanstalt für Medien NRW (LfM), warnt außerdem vor versteckten **Kostenfallen**: „In einigen unseriösen Apps schalten Anbieter Werbeanzeigen, die den Nutzer beim Anklicken zu Seiten weiterleiten, auf denen er seine persönlichen Daten eingeben muss und damit unwissend ein kostenpflichtiges Abonnement abschließt.“ Ähnliches gilt für In-App-Käufe. Das sind Apps, die zunächst kostenfrei heruntergeladen werden, aber durch Käufe innerhalb der App erweitert werden können. „Gerade bei jüngeren Handynutzern sollten In-App-Käufe mit

einem nur den Eltern bekannten **Passwort** abgesichert werden, damit hier keine unbeabsichtigten Kosten entstehen“, empfiehlt Müsgens.

Welche App ist sicher?

Oft sind unsichere Apps von sicheren kaum zu unterscheiden. Unseriöse Anbieter werben zum Beispiel damit, dass sie dem Nutzer neue Funktionen von bereits bekannten Apps versprechen, wie etwa die Möglichkeit, zu sehen, wer zuletzt das **Facebook**-Profil besucht hat oder V.I.P.-Funktionen für **WhatsApp**. „Gerade unseriöse Apps, die sich mit dem Namen bekannter Anbieter tarnen, werden vielfach von Nutzern bedenkenlos heruntergeladen“, kritisiert Müsgens. Daher empfiehlt er vor dem Download eine eingehende Überprüfung des App-Anbieters, beispielsweise, ob er eine seriöse Internetseite hat oder es eine Möglichkeit gibt, ihn zu kontaktieren. Auch der App-Store bietet bereits Anhaltspunkte dafür, ob eine App sicher ist oder nicht: „Bewertungen und Kommentare von anderen Nutzern können schon einen ersten Aufschluss darüber geben, ob die App sicher ist und das erfüllt, was sie verspricht. Kommentare können aber auch verfälschend sein. Dann sieht die Bewertung zwar sehr gut aus, die Zahl der Downloads ist aber relativ gering. Zudem können App-Bewertungen auch manipuliert werden. Dadurch kann ein falsches Bild entstehen“, warnt Martin Müsgens. Neben den Informationen aus dem App-Store gibt es auch Internetseiten, die regelmäßig Apps testen und ihre Ergebnisse veröffentlichen. Der Experte rät vor dem Kauf oder der Installation einer App auch dazu, Freunde und Bekannte zu fragen, welche Erfahrungen sie bereits mit der App gemacht haben.

Nach dem Download

Ist eine App heruntergeladen worden, kann eine Anti-Virus-App helfen, den Download auf seine Sicherheit hin zu überprüfen. Anti-Viren-Programme scannen das System regelmäßig auf schadhafte Anwendungen und auch App-Stores führen regelmäßig einen Sicherheitsscan durch. „Trotzdem ist ein Download aus dem App-Store und eine Anti-Virus-App auf dem Handy keine Garantie dafür, dass die App sicher ist“, merkt Müsgens an. Er empfiehlt zusätzlich, über den Mobilfunkanbieter eine Drittanbietersperre auf dem Mobilgerät einzurichten, die vor Abfallen und unbeabsichtigten Kosten schützt. Zudem sollte das Betriebssystem aktuell gehalten werden. So werden Sicherheitslücken geschlossen. Ist das eigene Smartphone von einem Virus befallen, sollte die schadhafte App direkt gelöscht werden. Das heißt aber nicht, dass es danach wieder sicher ist. Martin Müsgens erläutert: „Weil Apps teilweise auch im Hintergrund andere Apps installieren können, die dann unbemerkt weiterlaufen, sollte man sein Handy auch nach dem Löschen der schädlichen App noch einmal mit einem Anti-Virus-Programm auf Schadsoftware prüfen.“

Klare Regeln und gemeinsame Überprüfung

Auch wenn in App-Stores immer wieder Apps von unseriösen Anbietern angeboten werden, ist die Installation über den App-Store sicherer als ein Download außerhalb des App-Stores. „Vor allem über das Android-Betriebssystem gibt es die Möglichkeit, Apps nicht über den App-Store, sondern über andere Internetseiten als Android-Package-Datei herunterzuladen. Das iOS-Betriebssystem ist hingegen geschlossener angelegt. Hier können Apps nur über den offiziellen App-Store von Apple heruntergeladen werden“, erklärt der Experte. Ein Thema, das dem Referenten der Landeszentrale für Medien auch am Herzen liegt, ist die **Medienkompetenz** von Kindern. Im Hinblick auf den sicheren App-Download rät er Eltern dazu, klare Regeln zu



Martin Müsgens





Referent bei der Landeszentrale für Medien
Nordrhein-Westfalen, © LfM

Weitere Informationsangebote:
klicksafe bietet Eltern und Jugendliche Infos rund um Apps und Smartphones.
Handysektor ist ein Informationsportal für Jugendliche. Das **Internet-ABC** gibt Eltern, Kindern und Lehrern Tipps zum Umgang mit dem Smartphone. Die **Broschüre „Smart mobil?!“** ist ein Angebot von klicksafe und

vereinbaren: „Apps sollten immer erst nach gemeinsamer Rücksprache installiert werden und der App-Store sollte kindersicher eingerichtet werden, damit nur bestimmte Apps, die dem Alter des Kindes entsprechen, heruntergeladen werden können. Zudem sollten sich Eltern die App vorab anschauen.“
FL (26.01.2018)

Handysektor und enthält einen App-Check zur Beurteilung von Apps. Mit dem Angebot www.mediennutzungsvertrag.de können Eltern und Kinder Regeln zur Mediennutzung vereinbaren.

Folgende Artikel könnten Sie auch interessieren:

-  [Kontaktloses Bezahlen](#)
-  [Mobile Fraud: Vorsicht vor gefälschten Apps](#)
-  [Bankgeschäfte und Einkaufen im Netz](#)
-  [Wer will an meine Daten?](#)

[Alle Artikel dieser Kategorie](#)

Weitere Infos für Senioren



Wie Sie sich schützen können **Tricks an der Haustür**

Bei den so genannten „Haustürtricks“ haben es Betrüger hauptsächlich...[\[mehr erfahren\]](#)



Gefahren und Datenschutz **Wer will an meine Daten?**

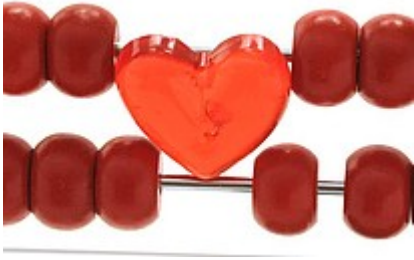
Wir hinterlassen Datenspuren, jeden Tag, auf verschiedene Weise: Im...[\[mehr erfahren\]](#)



Was Sie bei der Beförderung von Menschen mit Handicap beachten sollten

Menschen im Rollstuhl sicher ans Ziel bringen

Mobilität gehört zu den zentralen Bedürfnissen unserer Gesellschaft....[\[mehr erfahren\]](#)



Teures Flirten

Romance Scamming - der Liebesbetrug

Sie schien gefunden, die große Liebe: im Internet, bei einer...[\[mehr erfahren\]](#)



Fakeshops in der Hand von internationalen Täterbanden

Bestell und nichts geliefert

Die Polizei im Rhein-Sieg-Kreis nahm im Frühjahr 2018 vier Betrüger...[\[mehr erfahren\]](#)
