APP-STORE: FÄLSCHUNGEN ERKENNEN

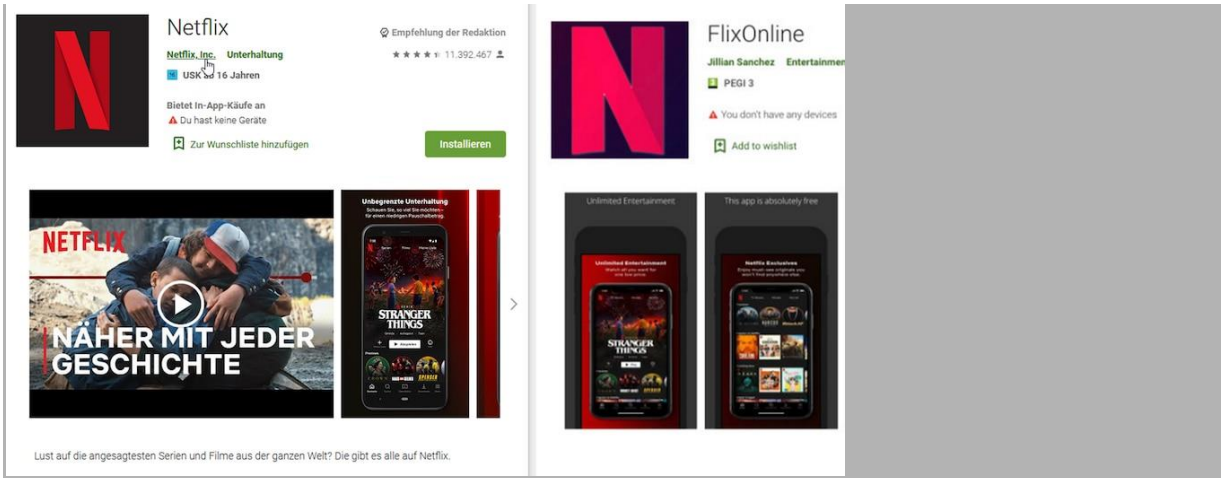
Eigentlich prüft Google Android-Apps, bevor sie im Store angeboten werden können. Aber immer mal wieder schlüpfen Fälschungen durchs Raster – darauf sollten Sie nicht hereinfallen.

Zwar ist Google Play an sich eine tolle Sache, um kostenlose Apps und Spiele zu entdecken, aber das System des Stores ist keinesfalls fehlerfrei. Immer wieder kommt es vor, dass Malware oder Fake-Apps dort frei zum Download verfügbar sind.
Darum sollten Sie sich vor der Installation einer Anwendung immer Zeit dafür nehmen, die angebotenen Informationen sorgfältig durchzulesen. Sonst kann es mit einmal Tippen auf den Installieren-Button schon zu spät sein.

So war beispielsweise eine App namens "FlixOnline" mit kopiertem Netflix-Logo auf über 500 Geräten gelandet. Diese Anwendung war dann in der Lage, Spam-Nachrichten mit schädlichen Links über WhatsApp an alle Kontakte zu senden.

Wir zeigen Ihnen hier Methoden, mit denen Sie sich effektiv vor solcher Malware und nutzlosen Fake-Apps schützen können – das erste Warnsignal sind zum Beispiel übertriebene Gratis-Versprechen.

Methode 1: Auf Herstellernamen achten



Original und die dreiste Kopie daneben – achten Sie darum immer auf den Herstellernamen.

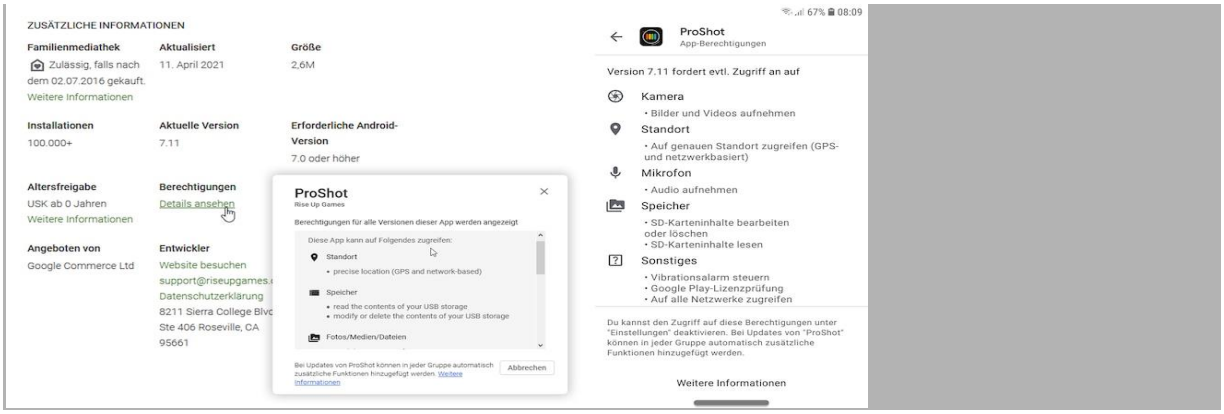
Bild: CHIP

Die Logos und Namen von Apps lassen sich bei Google Play teils relativ platt kopieren oder minimal abändern, dass manche Nutzer versehentlich die falsche Anwendung antippen und installieren.

Darum sollten Sie bei Google Play auch immer auf den Herstellernamen achten. Wenn bei einer vermeintlichen Netflix-App unter dem Namen als Hersteller nicht "Netflix" aufgeführt ist, sollten Sie stutzig werden.

Tippen Sie den Herstellernamen an, sehen Sie zudem andere Apps, die über diesen Account bereits veröffentlicht wurden. Sind dort mehrere Einträge mit sehr ähnlichem Logo und gleichen Funktionen zu finden, kann das ein Indiz für eine Spam-Masche sein. Selbst wenn sich dahinter keine Malware verbirgt, steht damit zumindest schon einmal der praktische Nutzen einer solchen App infrage.

Methode 2: Notwendige Berechtigungen hinterfragen



Die Berechtigungen lassen sich am PC sowie am Handy einsehen und prüfen.

Bild: CHIP

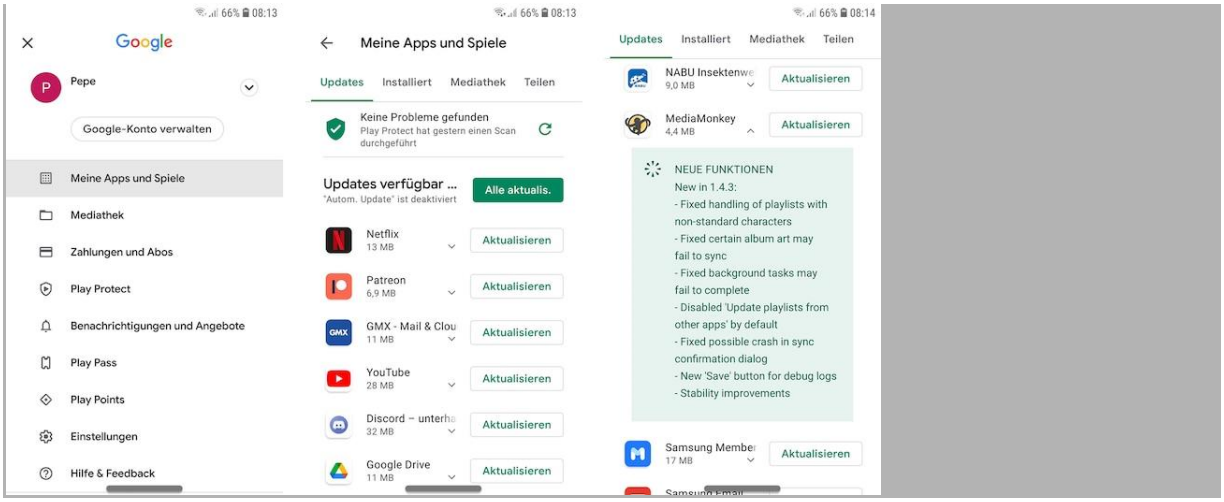
Viele Apps benötigen bestimmte Berechtigungen, um richtig funktionieren zu können. So braucht eine Kamera-App natürlich Zugriff auf Ihre Kamera und den Gerätespeicher, um die Fotos auch auf dem Handy sichern zu können. Eine Notiz-App wiederum muss hingegen wohl kaum Ihren Standort kennen.

Android-Malware versucht also, diese Berechtigungen geschickt auszunutzen, um Schaden anzurichten. Mit der Berechtigung "App kann über anderen Apps erscheinen" lassen sich etwa Pop-ups einblenden, die gefälschte Anmeldefenster erzeugen. Sollte so etwas unverhofft erscheinen, während Sie eine andere App nutzen, seien Sie skeptisch.

Um die erforderlichen Berechtigungen einzusehen, tippen Sie in Google Play auf "Über diese App" und scrollen bis ganz nach unten zur Schaltfläche "Weitere Informationen". Dort sind alle Zugriffe gelistet, inklusive einer kleinen Beschreibung.

Manche Berechtigungen sind auch optional und können weggelassen werden – ein Beispiel dafür wäre der Standortzugriff bei einer Foto-App. In diesem Fall kann der genaue Ort, wo ein Foto aufgenommen wurde, in den Metadaten des Bildes gespeichert werden.

Methode 3: App-Updates genau prüfen



Alle Apps auf einen Schlag zu aktualisieren kann ein ungeahntes Risiko beherbergen.

Bild: CHIP

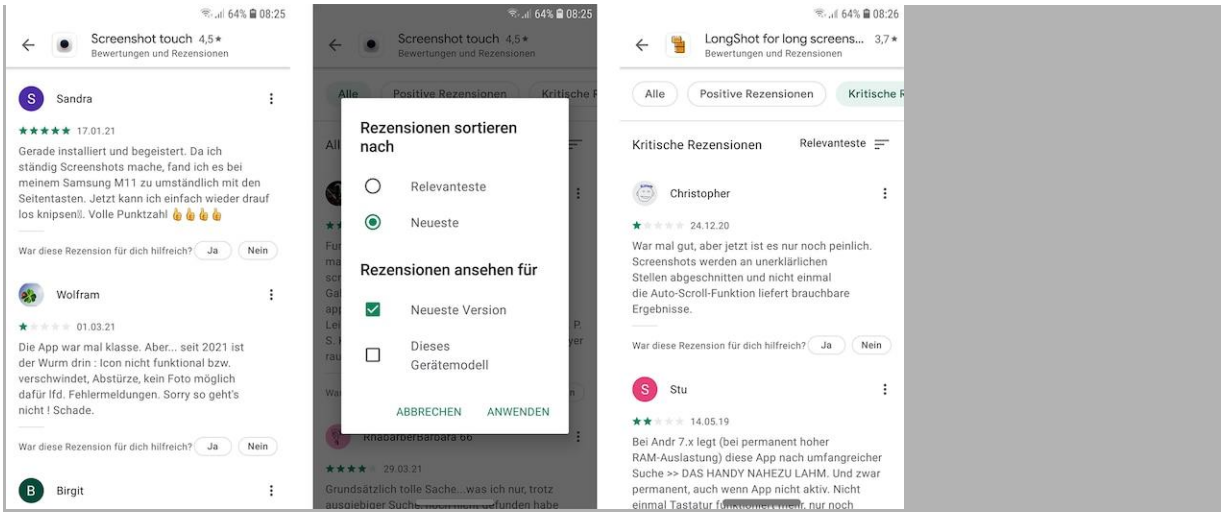
App-Updates sind wichtig, denn sie schließen oft kritische Sicherheitslücken. Gelegentlich kommt es aber vor, dass Anwendungen zunächst einen echten Mehrwert bieten und erst nach einem Update schädlichen Code ausführen.

Dadurch bauen die Entwickler zunächst eine große Nutzerbasis auf, um die Geräte anschließend zu infizieren. So war es etwa bei der App "Barcode Scanner", die nach einem App-Update überall im Android-System invasive Werbung zeigte und dann aus dem Store flog.

Bei Google Play gibt es unter "Meine Apps und Spiele | Updates" die Möglichkeit, alle Anwendungen auf einen Schlag zu aktualisieren. Genau durch solche Rundumschläge können sich aber auch ungewollte Änderungen ins System einschleichen. Bei Apps von großen offiziellen Anbietern müssen Sie sich weniger Sorgen machen, doch gerade bei kleinen Gadgets von kleineren Entwicklern besteht ein höheres Risiko.

Lesen Sie sich bei solchen Kandidaten also immer die neuen Funktionen durch und verzichten Sie lieber vorerst, wenn Ihnen etwas seltsam vorkommt. Prüfen Sie in diesem Zuge auch die aktuellsten Nutzerwertungen.

Methode 4: Nutzerbewertungen beachten



Wenn Sie nach den kritischen Bewertungen filtern, lassen sich Probleme schnell feststellen.

Bild: CHIP

Die Sternebewertung ist nicht nur beim Kauf von Produkten im Internet wichtig, sondern auch beim Download von Apps bei Google Play. Der Wert kann ein wichtiger Indikator sein, ob eine Anwendung brauchbar oder sogar gefährlich ist. Prüfen Sie dabei aber nicht nur die Gesamtwertung, sondern scrollen Sie auch nach unten, um die aktuellsten Nutzerwertungen zu prüfen.

Tippen Sie dazu auf "Alle Rezensionen anzeigen | Neueste" und setzen Sie optional noch den Haken bei "Neueste Version". Dadurch lässt sich schnell prüfen, ob andere Nutzer nach Installation eines Updates unzufrieden sind oder vor der App warnen.

In diesem Bereich lässt sich auch nach negativen Bewertungen filtern – so finden Sie schnell heraus, ob andere einfach mit dem Funktionsumfang unzufrieden sind oder eine tatsächliche Gefahr von der App ausgeht.

Wenn alle Stränge reißen: Antivirus installieren

Zwar lässt sich darüber streiten, ob man wirklich eine Antivirus-App auf dem Smartphone benötigt, dennoch kann eine gelungene Anwendung die Sicherheit des Gerätes durchaus erhöhen. Das Problem ist dabei oft, dass die Echtzeit-Überwachung relativ Performance-hungrig sein kann, was vor allem bei schwächeren Smartphones ins Gewicht fällt.