



## **Gehe nur über den offiziellen Store. Gehe direkt dorthin. Lass dich nicht via WhatsApp und Facebook zu Schadsoftware locken.**

*Unsere Handys sind immer dabei. Telefonieren ist dabei schon fast die am wenigsten genutzte Funktion. Social Media Interaktion, E-Mails lesen, Spielen, Banking, Shoppen – wir nutzen unsere Smartphones universell. Das geht auch alles sorglos – wenn man zwei wesentliche Sicherheitstipps beachtet. Sophos klärt die wichtigsten Fragen.*

Früher galt mal: Apple-Nutzer sind vor Schadsoftware sicher. Mittlerweile wissen wir: kein Ökosystem ist perfekt, beide Betriebssysteme lassen sich mit Malware infizieren – wobei es bei Android Systemen oft einfacher ist als bei Apple.

Häufig gelangt Schadsoftware über Apps außerhalb der beiden offiziellen Stores von Android und Apple auf die Geräte, sogenanntes Sideloadung. Bei Apple gibt es zwei Methoden, die denen von Android-Missbrauch ähnlich sind, die Kriminelle für sich nutzen können, um eine Applikation zu laden.

1. Das Opfer wird dazu verleitet, ein Zertifikat zu installieren, das dem Angreifer erlaubt, Apps und andere Methoden herunterzuladen.
2. Die Betrüger nutzen die Apple TestFlight Option zur Überprüfung von Software, die noch nicht im offiziellen App Store akzeptiert wurde.

### **Wie lassen sich infizierte Anwendungen von virus-freien Apps unterscheiden?**

„Man sollte wirklich keine Applikation außerhalb der offiziellen Google- und App-Stores herunterladen. Zusätzlichen Schutz bietet auf Android-Geräten Sicherheits-Software, die Apps vor Inbetriebnahme nach verdächtigem Verhalten scannt, wie zum Beispiel Sophos Intercept X für Android. Vorsicht vor jeder Anwendung, die eine Zugangserlaubnis anfragt oder die die Möglichkeit hat, über den Bildschirm zu zeichnen – denn das sind alles Warnzeichen für Fernsteuerungsfunktionen“, empfiehlt Chester Wisniewski, Global Field CTO bei Sophos.

### **Die heruntergeladene App enthält einen Virus. Was nun?**

1. Schritt: Trennen des Geräts von sämtlichen verbundenen Netzwerken! Am schnellsten geht das mit dem Einschalten des Flugmodus.
2. Schritt: Backup der Daten erstellen, hier kann ein Experte helfen, damit danach ein Zurücksetzen auf die Werkseinstellungen möglich ist.

### **Was passiert mit meinen Daten, wenn mein Handy infiziert ist?**

Schadsoftware kann sehr variantenreich sein und sich auf die unterschiedlichsten Bereiche stürzen. Aber: generell sind Applikationen dazu in der Lage, Textnachrichten abzufangen, Tasteneingaben, Passwörter und PINs aufzuzeichnen, Kamera und Mikrophone zu aktivieren und sogar aufzunehmen, was auf dem Bildschirm ist. Was sie (noch) nicht können: Zugang zu biometrischen Informationen, denn diese sind nicht in der Form gespeichert, dass sie sich in einen Fingerabdruck oder eine Gesichtserkennung zurückverwandeln lassen.

### **Kann ich noch sicher online einkaufen?**



Ja. Auch mit dem Handy kann man komfortabel und weitgehend unbedenklich shoppen. Wisniewski sieht die Gefahr für Schadsoftware aber noch an anderer Stelle: „Der Schlüssel zur Sicherheit liegt in der Nutzung von Applikationen aus offiziellen Stores. Aber man sollte wachsam sein, wenn man über sekundäre Kommunikationswege angesprochen wird wie

WhatsApp. Die verschlüsselten Chat Apps sind wie dafür gemacht, Betrug und Schadsoftware zu verbreiten, denn sie entziehen sich der Kontrolle durch den Diensteanbieter. Die Köder werden auf Facebook gelegt, und dann wechselt man aber zu einer verschlüsselten Verbindung, damit gefährliche Links und Downloads nicht herausgefiltert werden können.“

Hier haben die Sophos-Forensiker frühere Angriffe auf Apple Nutzer analysiert:  
[Cryptorom bitcoin swindlers continue to target vulnerable iphone and android users.](#)

### **Social Media von Sophos für die Presse**

Wir haben speziell für Sie als Journalist\*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf  und 

LinkedIn: <https://www.linkedin.com/groups/9054356/>

Twitter: @sophos\_info

### **Pressekontakt:**

Sophos  
Jörg Schindler, PR-Manager Central & Eastern Europe  
[joerg.schindler@sophos.com](mailto:joerg.schindler@sophos.com), +49-721-25516-263

TC Communications  
Arno Lucht, +49-8081-954619  
Thilo Christ, +49-8081-954617  
Ulrike Masztalerz, +49-30-55248198  
Ariane Wendt +49-172-4536839  
[sophos@tc-communications.de](mailto:sophos@tc-communications.de)