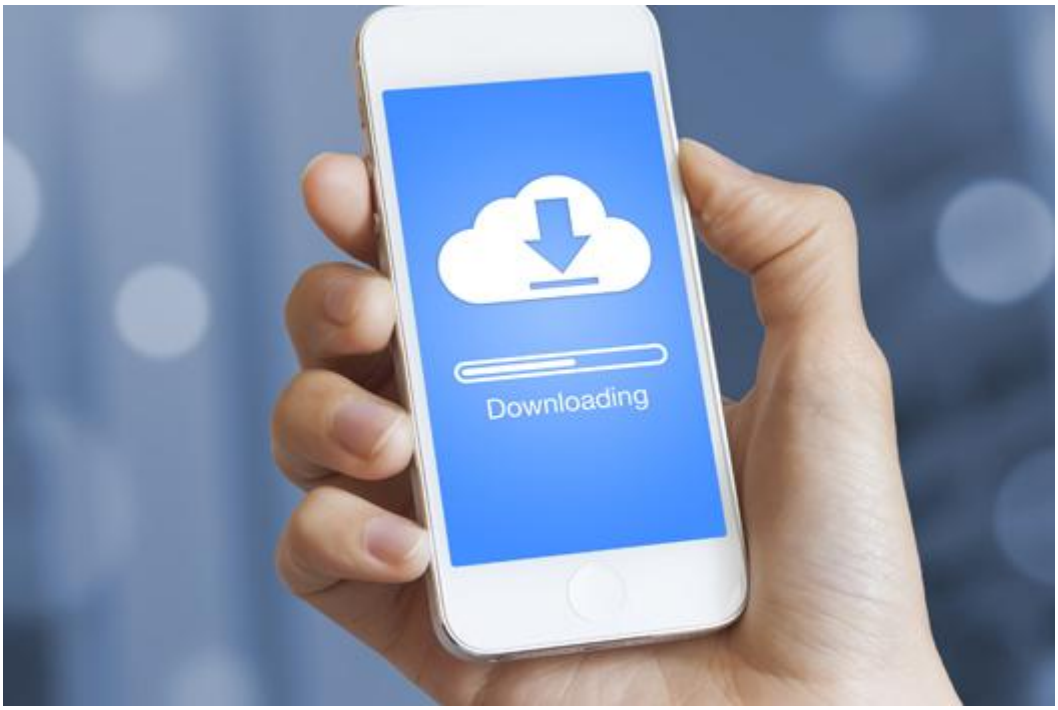
Hells Angels gegen Bandidos >
< Kritische Medienkompetenz entwickeln

Mobile Fraud: Vorsicht vor gefälschten Apps

„Was ich nicht kenne, installiere ich nicht“



Apps sollten nicht vorschnell installiert werden

Gefälschte Apps sind keine Seltenheit. Immer wieder schaffen es Betrüger, manipulierte oder betrügerische Apps in die offiziellen Stores zu schleusen. Worauf man beim App-Download achten sollte und wie man sich sonst vor App-Betrügern schützen kann, verrät Hans-Joachim Henschel vom Landeskriminalamt in Niedersachsen. Von den Fälschern wird häufig die Beliebtheit seriöser Apps ausgenutzt. Die gefälschten Apps sehen den echten dabei sehr ähnlich. „Die Betrüger hoffen, dass die Käufer den Betrug nicht bemerken und die App kaufen. Die gefälschten Apps haben dabei keine Funktion, stürzen ab oder verursachen sogar Schäden, indem sie zum Beispiel Schadsoftware einschleusen oder unerwünschte Werbung anzeigen“, erklärt Henschel. Eine weitere Betrugsmasche: Mit den Fake-Apps werden vermeintliche Zusatzfunktionen beworben, die die echte App nicht leistet. Hier wird zum Beispiel WhatsApp missbraucht, indem von den Betrügern etwa zusätzliche Emojis versprochen werden.

Passwörter und die richtigen Einstellungen

Generell sollten Apps immer nur aus den offiziellen Stores heruntergeladen werden und nicht von Webseiten. Bei Android gibt es etwa in den Einstellungen die Option „Unbekannte Quellen – Installation von Apps von anderen Quellen als Play Store erlauben“. Hier sollte kein Haken gesetzt sein, damit Apps nicht aus anderen Quellen automatisch installiert werden können. „Generell gilt bei jedem digitalen Endgerät, egal ob Computer, Tablet oder Smartphone: Was ich nicht kenne, installiere ich auch nicht.“ Teilweise werden für das Laden von Apps aus App-Stores auch eigene Passwörter vergeben. Dadurch

kann vermieden werden, dass man aus Versehen eine neue App aus einem App-Store lädt. Man muss dann bewusst ein Passwort zur Installation bzw. zum Kauf eingeben. Gleiches kann man teilweise auch für die sogenannten In-App-Käufe machen. In-App-Käufe sind die Käufe, mit denen man z. B. neue Funktionen innerhalb einer App gegen Bezahlung freischalten kann. Dies wird von Anbietern gern genutzt, um zunächst eine kostenfreie App zu ermöglichen. Wenn der Nutzer dann mehr haben möchte, muss er bezahlen. „In-App-Käufe können auch sehr hochpreisig sein. Es gibt betrügerische Apps, die dies ausnutzen oder aber auch auf die Masse von kleinen Zahlungen abzielen“, weiß Henschel.

Keine Zahlungsdaten hinterlegen

Beim Herunterladen von Apps kann Schadcode aufs Handy gelangen

Auch wer im App-Store Bank- oder Kreditkarteninformationen hinterlegt hat, kann schnell um sein Geld gebracht werden, wenn etwa unberechtigt Zahlungen durchgeführt werden. Besser ist es, das Kundenkonto mit einer Prepaid-Karte aufzuladen. Im Notfall kann dann nur der Betrag abgebucht werden, mit dem das Konto vorher aufgeladen wurde. Möchte man eine App installieren, sollte man außerdem einen Blick auf die Bewertungen im jeweiligen App-Store werfen. Aber Vorsicht: Auch Bewertungen können gefälscht sein. Henschel: „Fake-Bewertungen sind nicht immer sofort zu erkennen. Gegebenenfalls finde ich aber bereits doch irgendwo eine negative Bewertung, die einen Betrug vermuten lässt. Weitere Recherchen im Netz sind dann sinnvoll – oft findet man dann Hinweise, dass die App nicht in Ordnung ist. Im Zweifelsfall verzichtet man lieber auf eine Installation.“

Apps für das Online-Banking

Beim Online-Banking per Smartphone sollte man darauf achten, eine App zu nutzen, die von der Hausbank empfohlen wird – im Idealfall ist diese über die Webseite der Bank verlinkt. „Alternative Banking-Apps können gut sein, es kann sich aber auch um eine Falle handeln. Zudem sollte man vermeiden, bei mobilen TAN-Verfahren die TAN auf das gleiche Gerät geschickt zu bekommen, auf dem die App installiert ist. Ein altes Handy ist für den SMS-Empfang der TAN besser geeignet“, weiß Henschel.

Drittanbieter-Sperre setzen

Das Setzen der Drittanbieter-Sperre kann dafür sorgen, dass man bei seinen Telefonrechnungen großen Ärger und Stress vermeidet. Denn es gibt immer wieder Apps und Webseiten, die einen fiesen Trick verwenden: Für den Nutzer nahezu unsichtbar werden über Werbeanzeigen oder sonstige Buttons Schalter platziert. Klickt man dann auf die Werbung oder das „X“, das die Werbung schließen soll, kann es sein, dass man z. B. ein Abo für SMS-Dienste abgeschlossen hat. Hans-Joachim Henschel: „Dieses ungewollte Abo zu beenden, ist aufwändig und kostet Nerven. Auch ist es schwer, die Ursache zu finden und zu belegen. Aus diesem Grund sollte beim Provider für jeden Mobilfunk-Vertrag eine Drittanbieter-Sperre gesetzt werden.“

Aktuelles Betriebssystem und Antivirenschutz

Um sich vor Schaden durch gefälschte Apps zu schützen, kann man einige Sicherheitsmaßnahmen ergreifen. Zunächst einmal gilt, dass Nutzer dafür sorgen sollten, dass das verwendete Betriebssystem auf dem aktuellen Stand ist. Oft muss dazu in den jeweiligen Einstellungen des Smartphones gesucht und die Installation manuell gestartet werden. Henschel: „Je älter ein Smartphone ist, umso wahrscheinlicher ist es, dass der Hersteller das veraltete Gerät nicht mehr mit Updates unterstützt.“ Geräte mit veralteter Software sind dann möglicherweise nicht mehr so gut geschützt. Es kommt schließlich neben dem fehlenden Beseitigen von Sicherheitslücken auch nicht mehr dazu, dass neue Sicherheitsfeatures enthalten sind. Die Gefahr einer Infektion durch Schadsoftware oder betrügerische Apps steigt dann massiv an. Ein weiterer wichtiger Schutz für das Handy ist eine Antivirensoftware. „Auch hier bieten kostenpflichtige Versionen mehr Leistungsumfang. Eventuell muss bei kostenfreien Apps die Suche nach

Schadsoftware manuell angestoßen werden“, so Henschel.
SBa (25.05.2018)

Folgende Artikel könnten Sie auch interessieren:

- Cyber-Betrugsmasche „Jackpotting“
- Bestellt und nichts geliefert
- Vorsicht beim App-Download!
- Die Kommunikationswelt der Zukunft
- Bankgeschäfte und Einkaufen im Netz

Alle Artikel dieser Kategorie

Weitere Infos für Berater zum Thema Jugend

Ein Netzwerk gegen Rassismus und Diskriminierung

Aktiv werden und Courage zeigen

Der erste Schultag nach den Ferien: Bei vielen Schülern ist das ein...[mehr erfahren]

Ist das Zeigen der Aussage ACAB strafbar?

Gewalt beginnt bei der Beleidigung

A.C.A.B. steht für „All Cops Are Bastards“ („Alle Bullen sind...[mehr erfahren]

Die Ermittlungsarbeit beim Verdacht auf sexuellen Missbrauch

„Wir sind auf der Seite der Kinder“

Kriminalhauptkommissarin Cathrin Frost arbeitet bei der...[mehr erfahren]

So wirken Partydrogen auf deinen Körper

Das Drogen-Radar

Hat dir auf einer Party schon mal jemand Drogen angeboten? Hier...[mehr erfahren]

Härtere Strafen bringen nichts

Warnschussarrest für jugendliche Intensivtäter

Jugendliche Intensivtäter beginnen ihre kriminelle Karriere häufig...[mehr erfahren]
