Android-Nutzer sollten sie kennen: Gängige Fehler, die Sie besser vermeiden

Android hat für Google einen enormen Stellenwert. Das Smartphone-Betriebssystem des Mega-Konzerns bietet für die User ein deutlich offeneres System als die Konkurrenz, was bei vielen auf großen Anklang stößt. Allein in Deutschland nutzen rund 65 Prozent aller Smartphone-User Android als OS ihres Gerätes. Und doch gibt es da draußen noch einige Nutzer, die ein paar Fehler bei Android begehen.

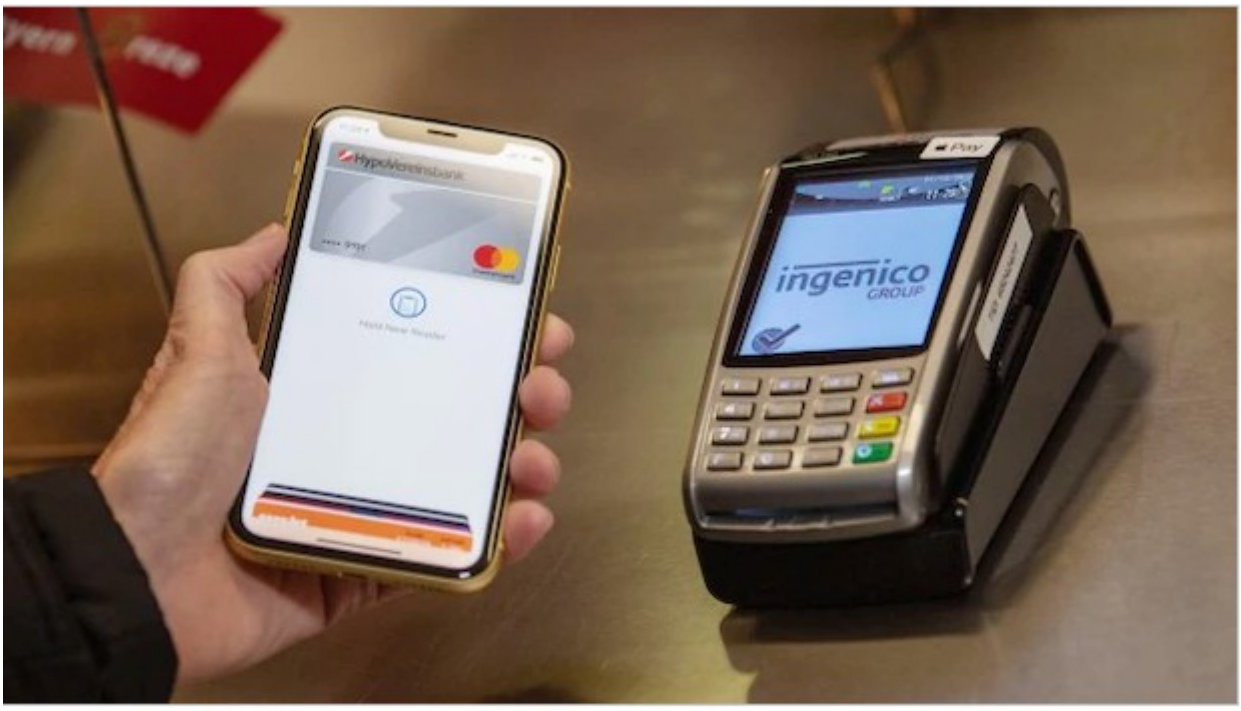
Einer der wichtigsten Tipps für das Android-Smartphone liegt beim System selbst. In regelmäßigen Abständen liefert Google Updates nach, damit das OS (Operating System) stabiler läuft, neue Funktionen an die User ausgerollt oder kritische Sicherheitslücken geschlossen werden. Dementsprechend ist es auch sehr wichtig, dass Android-User diese Updates wahrnehmen und aktivieren.

Schnell ist eine solche Meldung über ein verfügbares Update weggewischt und vergessen. Sollte eine neue Version von "Android" zur Verfügung stehen, zögern Sie dieses Update nicht unnötig heraus. Am Ende sind Sie dadurch auf einer deutlich sicheren und besseren Seite der Smartphone-Nutzung.

Keinen Virenscanner nutzen

Im Gegensatz zur Konkurrenz ist Android ein recht offenes System. Das Problem dabei: Um einige Dinge müssen sich die User selbst kümmern. So auch beim Schutz vor Angriffen auf das Smartphone und Virenscannern. Zwar gibt es Android-seitig einige Vorkehrungen, um solche Zugriffe zu vermeiden, doch ist der Griff zu einem waschechten Anti-Virenprogramm immer noch die bessere Alternative.

Bluetooth, NFC und weitere Dienste durchgängig aktiviert lassen



Beim mobilen Bezahlen ist NFC nützlich. Doch sollte die Schnittstelle nicht durchgängig aktiv sein.

Foto: Lino Mirgeler/dpa

Dienste wie Bluetooth und NFC sind auf vielen Android-Geräten durchgängig aktiviert. Sei es, weil vergessen wurde, sie abzuschalten oder sie aufgrund von Bequemlichkeiten - etwa bei der Verbindung mit Kopfhörern oder dem mobilen Bezahlen - ständig aktiv bleiben. Doch genau diese Verhaltensweise birgt Risiken. Bluetooth und NFC sind Schnittstellen zu Ihrem Smartphone.

So mancher Betrüger kann über diese Zugänge mit dem entsprechenden technischen Know-How Zugriff erhalten. Schalten Sie Bluetooth und NFC sowie sämtlichen anderen Schnittstellen immer aus, wenn sie gerade nicht gebraucht werden. In den Systemeinstellungen lassen sich auch bestimmte Zeitintervalle einstellen. Sollte kein Zugriff in dieser Zeit auf die Dienste erfolgen, schalten sie sich automatisch ab.

Ungenutzte Apps auf dem Smartphone lassen

Im Laufe der Lebenszeit eines Smartphones sammeln sich extrem viele Apps auf dem Gerät an. Das Problem: Durch den zugemüllten App-Drawer, in dem alle Anwendungen angezeigt werden, verlieren Sie nicht nur den Überblick, sondern auch wichtigen Speicherplatz und womöglich auch Geschwindigkeit bei Ihrem Smartphone. Deshalb lohnt es sich, in regelmäßigen Abständen die eigenen Apps zu durchforsten und etwaige Störenfriede zu löschen.

Die Apps lassen sich durch einen langen Druck auf das Icon und die anschließende Wahl der Option "Deinstallieren" oder "Entfernen" von Ihrem Android-Smartphone verjagen.

App-Berechtigungen nicht überprüfen

Bei der Installation von neuen Apps werden Sie häufig gefragt, ob Sie die ausgewählten Berechtigungen erteilen wollen. Die meisten User klicken leichtfertig auf "Akzeptieren", ohne sich die Regelungen und Erfordernisse für die App in Ruhe durchzulesen. Gerade bei vermeintlich kostenlosen Anwendungen können sich schnell Root-Berechtigungen einschleichen, die tief in das System eingreifen können.

So gelangen eventuell sensible Daten an die Hersteller der Android-Anwendungen. Stellen Sie also bei der Installation sicher, dass die App auch nur die Berechtigungen will, die Sie wirklich braucht. Fragt eine Wetter-App beispielsweise nach Zugriff auf die Kamera und Anrufe, sollten bei Ihnen die Alarmglocken läuten.