

> Sicherheits-Tipps für die fünf Arten von Smartphone-Besitzern (Sam Wordley – shutterstock.com)



Vom Profi

## Sicherheits-Tipps für Smartphone-Besitzer

Ein Sicherheitsexperte hat Smartphone-Besitzer in fünf Typen eingeteilt. Er gibt passende Sicherheits-Tipps für jede Benutzergruppe.

**1. Der Unwissende:** Sie benutzen ein Smartphone, da Ihr Chef oder Ihre Kinder Sie dazu gedrängt haben, wären aber besser mit einem traditionellen Handy dran: neu-deutsch auch als Feature Phone bezeichnet. HMD Global produziert beispielsweise unter dem bekannten Markennamen Nokia einige spannende Feature Phones alias Handys.

Aber Sie haben jetzt nun einmal ein Smartphone und kommen mit dessen Funktionen nicht klar und benutzen daher das Handy nur für Anrufe, SMS-Nachrichten und E-Mails. Und schliesslich laden Sie keine Apps herunter, es sei denn, Sie werden durch den Prozess geführt.

**2. Der Minimalist:** Sie sind zufrieden mit Ihrem Smartphone und benutzen es nur für grundlegende Dinge. Sie laden hin und wieder einmal Apps herunter, aber nur die nötigsten, wie z.B. WhatsApp, Instagram, Skype und Facebook. Sie behalten Ihr Smartphone bis es kaputt geht und für den Minimalist besteht kein Interesse an den neuesten Modellen – selbst dann, wenn der Hersteller keine Sicherheits-Updates mehr für Ihr Smartphone bereit stellt.

**Sicherheits-Tipp für diese beiden Gruppen:** „Sowohl der Unwissende und der Minimalist sollten besonders vorsichtig sein, wenn sie auf Links in Emails und

SMS-Nachrichten klicken, da sie nicht geschult sind, Malware zu erkennen“, glaubt Janus R. Nielsen, Sicherheitsexperte beim MYSecurityCenter. „Oft sind es diese beiden Gruppen, die keine Passwörter auf dem Handy haben, da sie meinen, es wäre zu kompliziert und sind bei Verlust des Handys somit anfälliger.“

**3. Der Enthusiast:** Sie finden das Leben schwierig ohne Ihr Smartphone. Ihre ganzen Fotos befinden sich darauf, ein Großteil Ihrer Kommunikationen läuft über das Smartphone und Sie sind neugierig, Apps herunterzuladen, um noch mehr aus Ihrem Smartphone heraus zu holen. Sie spielen verschiedene interaktive Spiele mit den Menschen um Sie herum und überweisen Geld mit Mobile-Banking.

**Sicherheits-Tipp:** Janus R. Nielsen rät dieser Benutzergruppe: „Sie müssen beim Herunterladen von Apps extra vorsichtig sein – lesen Sie vor der Installation immer die Bewertungen. Wenn es keine Kommentare oder Sterne gibt, stellen Sie weitere Forschungen der App im Internet an. Zuletzt, führen Sie kein Mobile-Banking in öffentlichen Orten mit WLAN aus.“

**4. Der Umfangreiche:** Ihr Smartphone ist eine Verlängerung Ihres Armes, sowohl zu Hause und am Arbeitsplatz. Sie benutzen es für alles und erforschen immer wieder neue Funktionen und Apps, um es noch effizienter zu nutzen. Sie verfügen über umfangreiche technische Kenntnisse, wie Ihr Telefon funktioniert und verlangen ein hohes Mass an Sicherheit.

**Sicherheits-Tipp:** „Diese Art von Smartphone-Nutzern installieren Virenschutz auf ihren Geräten, sodass sie erkennen, blockieren und absichern können, falls etwas passieren sollte. Natürlich sind auch diese Menschen potenziellen WiFi-Hotspot-Risiken ausgesetzt, Angriffe in öffentlichen Netzwerken sind zunehmend verbreitet. Hierbei kann ein Angreifer die Übertragung der Informationen von Ihrem Handy zum Netzwerk hin stören und manipulieren.“

**5. Der Zwanghafte:** Sie ersetzen häufiger Ihr Smartphone mit einem Neuen, um den neuesten Stand der Technik zu erhalten. Um das meiste aus Ihrem Handy zu erhalten, löschen Sie einige Standard-Programme des Handys, um es nach Ihren Wünschen zu organisieren.

**Sicherheits-Tipp:** „Benutzer sind sich nicht bewusst, dass Hacker den SSH-Port des Handys öffnen, was bedeutet, dass jeder sich möglicherweise mit Ihrem Smartphone verbinden und Daten stehlen oder zufügen kann“, sagt Janus R. Nielsen. Diese Benutzer installieren öfters nicht autorisierte Apps Dritter, welche kostenlos sind, die aber Schadprogramme leicht auf dem Handy zufügen können. „Der Zwanghafte könnte zum Beispiel von einem mobilen VPN-Service (Virtuelles Privates Netzwerk) profitieren, wo sie sich mit ihrem Heimnetzwerk verbinden können oder ausserhalb des Hauses über verschlüsselte Kanäle, sodass Fremde nicht in der Lage sind, das Online-Surfen zu verfolgen.“

## Sicherheits-Tipps für alle Smartphone-Nutzer

1. Erstellen Sie einen möglichst langen Zugangscode für Ihr Smartphone oder benutzen Sie den Fingerabdrucksensor.
2. Lesen Sie Bewertungen und Kommentare, bevor Sie eine App herunterladen. Wenn es keine gibt, verzichten Sie besser auf die App.
3. Lesen Sie die Bedingungen sorgfältig durch, bevor Sie akzeptieren und eine App herunterladen. Zum Beispiel braucht kein Puzzle-Spiel Zugang zu Ihren Nachrichten oder den Standort.
4. Überlegen Sie, ob Sie vielleicht von einem Antivirus-Programm mit Tracking-Funktion, Blockierung oder Datensicherung bei Verlust profitieren können. Das gilt für Besitzer eines Android-Smartphones.
5. Vorsicht bei öffentlichen WiFi-Hotspots.
6. Denken Sie daran, dass die Garantie nicht besteht bei ‚Jailbreak‘ (Ausschalten der Sicherheitsstruktur) des Smartphones.
7. Seien Sie vorsichtig mit Apps von nicht autorisierten App-Stores, da diese leicht Schadprogramme enthalten können. Laden Sie Apps am besten nur aus dem Apple App-Store und von Google Play herunter. Das gleiche gilt für Werbung in kostenlosen Apps.
8. Installieren Sie alle Sicherheits-Updates für Ihr mobiles Betriebssystem.

*Hans-Christian Dirscherl*

*Nach vielen Jahren als News-Schreiber spezialisierte sich Hans-Christian Dirscherl bei der PC-WELT auf Business-IT und baute den Bereich Auto & Technik auf, für den er Infotainmentsysteme testet. Außerdem befüllt er die Social-Media-Kanäle der PC-WELT.*