WAP-Betrug mit teuren SMS ist wieder da

WAP-Abos sind teuer und total veraltet, Cyberkriminelle nutzen Sie aber noch, um Android-Nutzerinnen und -Nutzern heimlich das Geld aus der Tasche zu ziehen.

Erinnern Sie sich noch an Jamba-Klingeltöne und -Hintergrundbilder? Genau, das war, bevor es Smartphones und Apps gab. Und dafür gab es teure WAP-Abos. Solche Abos gibt es immer noch, die meisten Abonnenten und Abonnentinnen dürften von ihrem Abo aber gar nichts wissen. Apps auf dem Smartphone melden den Besitzer nämlich heimlich dazu an, warnt Microsoft.

WAP-Abos boten schon damals Möglichkeiten zum Betrug. In der Regel lockten die Anbieter die User in solche Abonnements, indem sie beispielsweise Klingeltöne als gratis bewarben und nur im Kleingedruckten auf das automatische, kostenpflichtige Abo hinwiesen. Die neue Masche ist raffinierter: Im Play Store tauchen Apps auf, die zu beliebten Themen Funktionen versprechen – und teilweise sogar wirklich bieten. So kommen die Apps in kurzer Zeit auf Millionen Downloads und durch die automatische Google-Prüfung. Der eigentliche Zweck der Anwendung ist aber das Anmelden zu teuren WAP-Abos sowie das Verschleiern der Anmeldung. Die Apps schicken nämlich nicht nur unbemerkt die Anmelde-SMS raus, sondern fangen auch Bestätigung- und Erinnerungs-SMS ab. Die Besitzerinnen und Besitzer der Geräte sehen davon also nichts. Nur auf der Rechnung des Mobilfunkanbieters tauchen die Kosten dann auf. Da die meisten aber Flatrates haben, setzen die Betrüger darauf, dass dort niemand so genau hinschaut.

Der einfachste und auch radikalste Weg, sich vor ungewollten WAP-Abos zu schützen, ist, diese beim Mobilfunkanbieter zu sperren. Dazu rufen Sie die Support-Hotline an und lassen eine solche Sperre einrichten. Je nach Anbieter heißt sie auch Drittanbieter-Sperre oder ähnlich. Mit so einer Sperre kann niemand ein WAP-Abo abschließen – Sie nicht und auch Hacker nicht! Zusätzlich erkennen Antivirus-Apps solche Abos und warnen Sie in der Regel davor.