# EU: Verwaltung wird digitalisiert

Behördengänge künftig online erledigen

[Digitaler Binnenmarkt](http://europakonsument.at/de/rubriken/digitaler-binnenmarkt)

Die EU-Kommission hat ein Maßnahmenpaket verabschiedet, das den Binnenmarkt effizienter und digitaler machen soll. Einer von drei Punkten ist das so genannte zentrale digitale Zugangstor. Künftig soll es Konsumenten möglich sein, einfache Behördengänge online zu erledigen. Der Vorschlag umfasst unter anderem die Beantragung einer Geburtsurkunde, die Anmeldung eines Fahrzeugs oder die Änderung der Wohnadresse nach einem Umzug.

 Laut einer Aussendung der Kommission sind viele dieser Verfahren bisher nur für Staatsbürger eines Landes in der jeweiligen Landessprache zugänglich. Mit dem zentralen digitalen Zugangstor werden sie online und in zumindest zwei EU-Sprachen verfügbar sein.

Das neue System soll bis 2020 umgesetzt werden.

<http://europakonsument.at/de/news/eu-verwaltung-wird-digitalisiert>

# Mobiler Basis-Schutz: Die wichtigsten Sicherheitstipps für Smartphone und Co.

**Sie sind längst unsere ständigen Begleiter im Alltag: Die meisten von uns nutzen Smartphones und andere mobile Geräte, um auch von unterwegs E-Mails abzurufen, mal eben etwas im Internet nachzuschauen oder soziale Netzwerke zu pflegen. Aber wie schützt man das Handy oder Tablet gegen Viren, Hacker und Co? Wir geben ein paar Tipps.**

Auch wenn sie klein und handlich sind: Längst sind unsere Handys und andere mobile Geräte fast leistungsfähige kleine Computer – mit allen Vorteilen, aber auch allen Nachteilen. Und zu diesen gehört auch das Risiko, sich Viren, Trojaner und andere Schadprogramme einzufangen oder von außen gehackt zu werden.  Weil wir Smartphone und Co überall dabeihaben und uns mit ihnen auch im öffentlichen Raum bewegen, sind sie sogar noch stärker gefährdet als der heimische PC.

Was also tun, damit Handy und Co sicher sind? Hier die wichtigsten Tipps für den Basis-Schutz der mobilen Geräte.

### Gesunden Menschenverstan einschalten

Das vielleicht wichtigste Hilfsmittel gegen Viren, Hacker und Co ist unser gesunder Menschenverstand. Bewahren Sie sich eine gesunde Skepsis und folgen Sie nicht gleich jeder Empfehlung für einen Download oder eine App, die Sie irgendwo gelesen oder gehört haben. Klicken Sie nicht wahllos auf alle Links, die ihnen im Netz oder in E-Mails in die Quere kommen. Prüfen Sie zudem kritisch, welche Zugriffsrechte eine App wirklich zur Erfüllung ihrer Funktionalität benötigt.

### Apps nur aus vertrauenswürdigen Quellen laden

Als erste Hürde sollte in den Einstellungen das Laden von Apps aus "unbekannter Herkunft" ausgeschaltet sein. Während die offiziellen App-Stores meist gut überwacht und damit relativ sicher sind, birgt das Laden von Apps aus unbekannten Quelle ein ungleich höheres Risiko für eine Infektion. Sie sollten daher nur in begründeten Ausnahmefällen eine App aus einer Quelle außerhalb dieser offiziellen Quellen laden. Falls Ihnen der Anbieter einer App nicht bekannt ist, informieren Sie sich vor der Installation. Wenn Sie an der Integrität der App zweifeln, können Sie diese auch vor dem Laden online mit Virenscannern wie beispielsweise dem Dienst "VirusTotal" kostenlos überprüfen lassen.

Ähnliches gilt auch für Anrufe oder SMS von unbekannten Rufnummern: Rufen Sie Ihnen unbekannte Dienste-Rufnummern nicht zurück und klicken Sie auch die Links in der SMS nicht an. Meist stecken Anbieter dahinter, die Sie so zu Anrufen über teure 0900er oder andere hochpreisige Rufnummern verleiten wollen. Aktuell Informationen zu solchen Betrügerischen Nummern erhalten Sie unter anderem bei der [Bundesnetzagentur](http://www.bundesnetzagentur.de/cln_1422/DE/Sachgebiete/Telekommunikation/Verbraucher/Rufnummernmissbrauch/rufnummernmissbrauch-node.html).

## Sperrcodes aktivieren

Ebenfalls selbstverständlich sollte es sein, die Display-Sperre des Smartphones oder Tablets einzuschalten.  Diese kann über die Eingabe eines Pincodes, eines Musters oder eines Fingerabdrucks aufgehoben werden. Auch die PIN der SIM-Karte für den Mobilfunk sollte stets aktiviert sein. Halten Sie die Zugangsdaten dafür unter Verschluss. Geben Sie PIN und Codes nur unter Sichtschutz gegenüber Dritten ein.

Haben Sie ihr Handy verloren oder Grund zur Annahme, dass es gestohlen wurde, sollten Sie sofort ihre SIM-Karte sperren lassen. Zusätzlich bieten einige Hersteller die sogenannte Remote-Wipe-Funktion an, bei der das Gerät aus der Ferne zurückgesetzt und gesperrt werden kann. Dadurch sind Ihre persönlichen Daten auf dem Gerät gelöscht oder nicht aufzurufen.

[www.wissen.de/mobiler-basis-schutz-die-wichtigsten-sicherheitstipps-fuer-smartphone-und-co/](http://www.wissen.de/mobiler-basis-schutz-die-wichtigsten-sicherheitstipps-fuer-smartphone-und-co/)