MEINKAUFSTADT Wien
meinkaufstadt.wien
Eine Initiative der Wirtschaftskammer Wien

Sicherer Surfen am Smartphone

Smartphones sind unsere täglichen Begleiter, auf die wir rund um die Uhr weder privat noch geschäftlich verzichten wollen. Tatsache ist jedoch, dass die Geräte nicht nur den Eigentümern zu Diensten sind.

02.10.2020, 9:33

© SENSAY/SHUTTERSTOCK

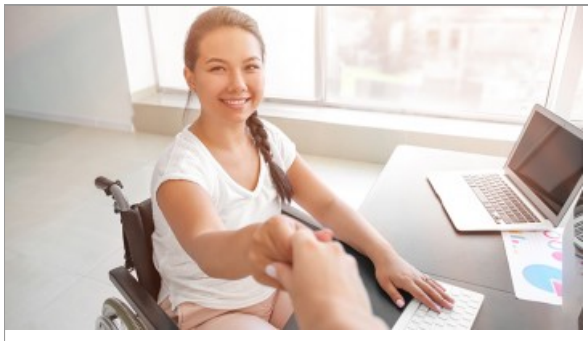
Ohne Zutun werden wir ausspioniert, belauscht und installierte Apps teilen persönliche Daten mit Dritten. „Ich habe ja nichts zu verbergen", lautet die Standardaussage vieler unbesorgter User. Ein Kardinalfehler weiß Martin Puaschitz, Fachgruppenobmann der **Wiener Unternehmensberatung, Buchhaltung und Informationstechnologie (UBIT)**: „Denn immer wenn ein Produkt, beispielsweise eine App, kostenlos angeboten wird, wird automatisch der User zum Produkt", erklärt der Experte. Diverse Anbieter verfolgen nämlich mit Nachdruck das Ziel, persönliche Profildaten so umfassend wie möglich zu erheben. Das beginnt beim Suchverlauf im Browser, geht über die Standortdaten und gipfelt im fortwährenden Mitschnitt jeglicher Konversation zum Beispiel via Sprachassistenten wie Alexa oder Siri.

„Es ist wichtig sich vor Augen zu führen, was mit den eigenen Daten geschieht. Dann kann man auch besser damit umgehen"

Hier ein kurzer Überblick, zu den Standard-Sicherheitsvorkehrungen, die man im Umgang mit Smartphones in jedem Fall beachten sollte und wie man Handys schon mit ein paar wenigen Handgriffen sicher machen kann - auch ohne sie in Alufolie zu wickeln oder permanent ausgeschaltet zu lassen.

1. **Nicht genutzte Apps deinstallieren**
   Je weniger ungenutzte Apps sich auf dem Smartphone befinden, desto besser. In regelmäßigen Abständen sollte daher überprüft werden, welcher unnötige Ballast sich angesammelt hat und wieder entfernt werden kann. Um weitere Risikofaktoren zu reduzieren, sollten Sie User-Anwendungen nur bei Bedarf öffnen und später auch wieder schließen, damit diese nicht permanent im Hintergrund laufen.
2. **Funktion GPS-Standort ausschalten**
   Wer nicht rund um die Uhr überwacht werden will, sollte bestimmten Apps - vor allem Google Maps - den Zugriff auf den eigenen Standort verweigern. Das lässt sich in den jeweiligen App-Einstellungen festlegen. Denn nur wenn das GPS-Modul des Smartphones deaktiviert ist, werden keine Daten über den Standort oder das entsprechende Bewegungsmuster mit Dritten geteilt.
3. **Cache, Cookie und Verlauf regelmäßig löschen**
   Cookies, temporäre Dateien und der mit der Zeit angesammelte Verlauf können nicht nur das Smartphone verlangsamen, sondern dokumentieren auch Details zum Nutzungs- und Surfverhalten der User. Wer diese Informationen regelmäßig löscht, erhöht damit die Sicherheit und den Schutz der eigenen Daten im Internet.
4. **Zugriffsrechte der Apps überprüfen**
   Ebenso lohnt sich ein genauer Blick auf die Zugriffsrechte bereits installierter Apps. Generell sollte auf jene Apps verzichtet werden, die sehr umfangreiche Zugriffsberechtigungen verlangen. „Meist finden sich dazu alternative Angebote. Eine Vielzahl an Apps verrichtet ihren Dienst auch dann zuverlässig oder fragt gezielt nach, wenn man ihnen etwaige Berechtigungen wieder entzieht", so Martin Puaschitz.
5. **Google-Einstellungen: Werbe-ID deaktivieren**
   Personalisierte Werbung ist eine tragende Säule im Geschäftsmodell von Google. Dafür werden verfügbare User-Daten genau analysiert, aufbereitet und werbenden Unternehmen als Datensatz zur passgenauen Zielgruppen-Ansprache zur Verfügung gestellt. Zu Gunsten einer höheren Datensicherheit können Nutzer auf dieses Angebot jedoch getrost verzichten und sollten die Funktion deaktivieren.
6. **Alternative Messenger-Apps verwenden**
   Über den Messengerdienst „WhatsApp" werden nicht nur persönliche Daten weitergegeben, sondern zum Beispiel auch Telefonnummern von gespeicherten Freunden. Das passiert in der Regel auch ohne dass die betroffenen Personen dem zugestimmt haben. Messenger-Programme wie beispielsweise „Signal" oder „Telegram" bieten hierzu eine Alternative und sorgen mit dezidierter Ende-zu-Ende-Verschlüsselung bei der Kommunikation für sehr hohe Sicherheit.
7. **Gleich mehrere Sicherheitsschranken setzen**
   Wer individuelle Passwörter, die Zwei-Faktor-Authentifizierung oder doppelte Sperrfunktionen - beispielsweise einen Fingerabdruck-Abgleich und eine PIN - nutzt, steigert zusätzlich die mobile Datensicherheit. „Wer sicherstellen möchte, dass seine privaten Fotos nicht ungewollt in den sozialen Netzwerken kursieren, versieht diese zudem am besten mit einem Wasserzeichen. Damit hat man im Fall der Fälle auch eine rechtliche Handhabe im Sinne des Urheberrechts", erklärt Puaschitz.

Das könnte Sie auch interessieren



Anlaufstelle für betriebliche Inklusion

Das NEBA Betriebsservice unterstützt und berät Unternehmen zum Thema Arbeit und Behinderung.

› mehr

StVO-Novelle: Was ab Oktober gilt

Mit 1. Oktober tritt die 33. StVO-Novelle in Kraft. Neben zwei neuen Verkehrszeichen, kommen Einschränkungen für Schrägparker und Erleichterungen für Radfahrer. › mehr

„Business Maniacs 2022“: Die Gründerszene weiter stärken

Das größte Wiener Info-Festival für Gründer, Startup-Interessierte und Jungunternehmergeht am 12. Oktober erstmals seit der Pandemie wieder „live“ über die Bühne. › mehr