RheinlandPfalz
MINISTERIUM FÜR FAMILIE,
FRAUEN, JUGEND, INTEGRATION
UND VERBRAUCHERSCHUTZ

DER SPION IN DER HOSENTASCHE

Datenschutz auf dem Smartphone

VORWORT

Anne Spiegel

Ulrike von der Lühe

Prof. Dr. Dieter Kugelmann

Liebe Leserinnen und Leser,

Smartphones und Apps sind aus unserem Alltag nicht mehr wegzudenken. Wir können damit nicht nur kommunizieren, sondern auch Musik hören, fotografieren, einkaufen oder Bankgeschäfte erledigen. Die vielfältigen Möglichkeiten machen das Smartphone zum mobilen Alleskönner.

Aber aufgepasst: Smartphones und Apps sammeln auch eine Menge Daten über uns und unsere Kontakte. Wenn Sie nicht möchten, dass andere mit Ihren Daten persönliche Profile erstellen, deren Auswirkungen Sie nicht abschätzen können, sollten Sie die Einstellungen immer wieder anpassen.

Mit diesem Flyer möchten wir Ihnen Wege aufzeigen, wie Sie Ihr Smartphone oder Tablet vor dem unerwünschten Zugriff Dritter schützen können. Denn Sie allein müssen entscheiden können, wer Ihre Daten erhält.

Wir wünschen Ihnen eine informative Lektüre.

Anne Spiegel
Ministerin für Familie, Frauen, Jugend, Integration
und Verbraucherschutz in Rheinland-Pfalz

Ulrike von der Lühe
Vorstand der Verbraucherzentrale Rheinland-Pfalz e.V.

Prof. Dr. Dieter Kugelmann
Landesbeauftragter für den Datenschutz und die
Informationsfreiheit in Rheinland-Pfalz

WAS VERRÄT IHR SMARTPHONE ÜBER SIE?

Smartphones speichern eine Vielzahl **persönlicher Daten**, von denen Sie viele selber eingeben. Das gilt zum Beispiel für Kontakte, Fotos und Textnachrichten, aber auch für Bankverbindungen oder Passwörter. Andere Daten, etwa die von Ihnen **besuchten Internetseiten**, werden ohne Ihr Zutun erfasst. Darüber hinaus kann Ihr Smartphone über die **GPS-Daten** ebenso wie über die **WLAN-Ortung** verraten, wo Sie sich gerade aufhalten – vorausgesetzt, Sie haben die jeweiligen Funktionen aktiviert.

In der Standardeinstellung sind die Geräte mitunter sehr mitteilsam. Überprüfen Sie daher bereits bei Inbetriebnahme die Voreinstellungen auf ungewollte Datenübertragungen.

Überlegen Sie, welche Daten Sie Ihrem Smartphone anvertrauen. Bedenken Sie, dass es nicht nur um Ihre, sondern auch um die Ihrer Familie, Freunde oder Geschäftspartner geht.

Lesen Sie die Datenschutzbestimmungen einer App und beachten Sie, dass diese sich ebenso wie die Einstellungsoptionen jederzeit ändern können.

Schränken Sie die Rechte einer App so weit wie möglich ein. Prüfen Sie datenschutzfreundlichere Alternativangebote, selbst wenn sie kostenpflichtig sein mögen.

Vor allem **Apps** können Ihre Privatsphäre ausspionieren, indem sie gespeicherte Daten Ihres Smartphones auslesen und weiterverwenden. Ein solcher Zugriff ist nur mit Ihrer **Einwilligung** zulässig. Nicht immer wird Nutzerinnen und Nutzern bewusst, welche umfangreichen Rechte sie den Betreibern und möglichen Drittanbietern manchmal einräumen. Kostenlose Apps sind in der Regel besonders neugierig.

WER HAT INTERESSE AN IHREN DATEN?

Gerätehersteller, Provider oder Betreiber von Apps profitieren davon, dass Sie mit dem Smartphone online sind. Denn aus Ihren Daten und den Spuren, die Sie im Netz hinterlassen, können sogenannte **Nutzerprofile** gebildet werden. Ein Nutzerprofil beschreibt Verhaltensweisen oder Gemeinsamkeiten von Zielgruppen und ist daher bares Geld wert.

Mit den Informationen kann **Werbung** gezielt auf Ihre Bedürfnisse zugeschnitten werden. Das kann auch dazu führen, dass Sie bestimmte Angebote nicht mehr erhalten, wenn Sie für ein Unternehmen als Kundin oder Kunde unattraktiv geworden sind. Auch im Online-Shop angezeigte Preise können auf eine **Profilbildung** zurückgehen.

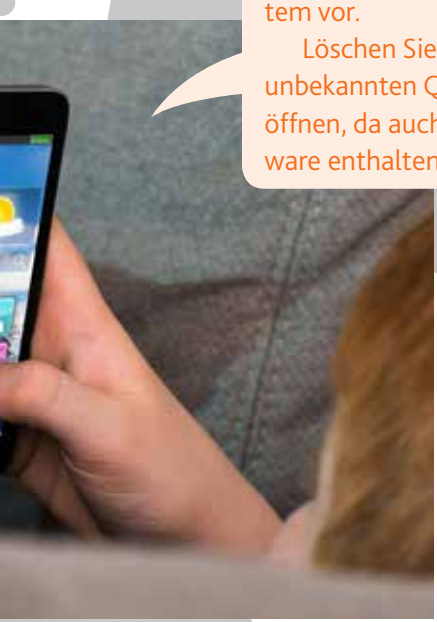
Der Profilbildung können Sie entgegenwirken, indem Sie zum Beispiel Tracking im Browser deaktivieren, die Browserdaten regelmäßig löschen sowie Cookies und die Standorterfassung nur bei Bedarf zulassen.

Bei manchen Apps können Sie interessenbezogene Werbung ablehnen.

Auch unseriöse Anbieter haben erkannt, dass das Smartphone der perfekte Spion in der Hosentasche ist. Sie locken zum Beispiel mit Gratis-Apps für Spiele, Bilder oder andere Angebote. Darin kann **Schadsoftware** verpackt sein, die Daten heimlich sammelt oder ungefragt weitersendet. Meistens ist nicht nachvollziehbar, was mit den Daten geschieht und wer sie erhält.

Nutzen Sie nur Apps aus vertrauenswürdigen Quellen, d. h. den Softwareportalen der Geräte- bzw. Betriebssystemhersteller. Nehmen Sie keine Eingriffe am Betriebssystem vor.

Löschen Sie Nachrichten aus unbekannten Quellen, ohne sie zu öffnen, da auch hier Schadsoftware enthalten sein kann.



WIE KÖNNEN SIE SICH NOCH SCHÜTZEN?

Smartphones sind heutzutage leistungsfähige Computer. Daher sollten ähnliche **Sicherheitsvorkehrungen** wie bei PC oder Laptop beachtet werden. Je besser Ihr Gerät und Ihre Daten gesichert sind, desto schwerer haben es Datendiebe, sich Zugriff zu verschaffen. Wir haben für Sie wichtige Schutzmaßnahmen zusammengestellt:

Halten Sie das Betriebssystem und installierte Anwendungen durch regelmäßige, am besten **automatische Updates** auf dem aktuellen Stand. Auch **Virenschutz** und **Firewall** sind beim Smartphone zu empfehlen.

Schützen Sie Ihre Daten durch **komplexe Passwörter** (mindestens acht, besser zwölf Zeichen, Groß- und Kleinbuchstaben, Ziffern, Sonderzeichen) und nutzen Sie **Verschlüsselungsmöglichkeiten**.

Sichern Sie insbesondere den Zugang zu **Banking-Apps** und **Apps mit Bezahlfunktion**. Reagieren Sie nicht auf Aufforderungen, PIN- oder TAN-Nummern offenzulegen. Vermeiden Sie das mobile TAN-Verfahren (mTAN, s. Glossar), wenn Sie das gleiche Gerät zum Online-Banking verwenden.

Aktivieren Sie die **Fernlöschfunktion** Ihres Smartphones. Löschen Sie Ihre Daten, bevor Sie das Smartphone zur Reparatur geben oder verkaufen.

Deaktivieren Sie **ungenutzte Funktionen** wie GPS, WLAN, Bluetooth oder NFC. Meiden Sie öffentlich zugängliche Internetzugänge wie **WLAN-Hotspots,** insbesondere bei vertraulichen Vorgängen.

IHR GUTES RECHT

Von Ihrem Anbieter können Sie **Auskunft** darüber verlangen, welche persönlichen Daten zu welchem Zweck gespeichert sind, an wen sie möglicherweise weitergegeben wurden und woher sie stammen. Falsche Daten sind auf Ihren Antrag hin zu berichtigen. Sollten Sie keine Einwilligung zur Datenspeicherung und -verwendung erteilt haben, können Sie die **Löschung** der Daten beantragen. Beachtet ein Anbieter Ihre Rechte nicht, wird er unter Umständen schadensersatzpflichtig. Außerdem haben Sie die Möglichkeit, der Verwendung Ihrer Daten zu Werbe- und Marktforschungszwecken zu **widersprechen**.

Mit einem einfachen Brief machen Sie Ihre Rechte gegenüber einem Anbieter geltend. Musterschreiben finden Sie auf unserer Homepage unter **http://s.rlp.de/smartphones**. Sollte der Anbieter Ihre Rechte ignorieren, wenden Sie sich an die für den Sitz des Anbieters zuständige Datenschutzaufsichtsbehörde. Auch der Landesdatenschutzbeauftragte und die Verbraucherzentrale Rheinland-Pfalz helfen Ihnen gerne weiter.

GLOSSAR

Cookies
sind kleine Dateien, die der Browser beim Surfen im Internet auf Ihrem Endgerät speichert. Sie enthalten z. B. Informationen über besuchte Seiten und persönliche Einstellungen.

GPS (Global Positioning System)
ist ein globales Satellitennavigationssystem zur Positionsbestimmung.

mTAN (Mobile Transaktionsnummer)
ist ein zeitlich limitierter Zahlencode zur Autorisierung von Online-Bankgeschäften, der per SMS auf das Mobiltelefon des Kunden geschickt wird und auf der Webseite der Bank eingegeben werden muss.

NFC (Near Field Communication)
ist ein Funkstandard zur drahtlosen Datenübertragung zwischen zwei NFC-fähigen Geräten. Er wird zum Beispiel für kontaktloses Bezahlen mit dem Smartphone genutzt.

Tracking
ist eine technische Möglichkeit, um Besucherströme, -verhalten und -aktionen auf Webseiten zu verfolgen. Ziel ist es, Nutzungs- und Verhaltensprofile zur Optimierung von Online-Marketingmaßnahmen zu erstellen.

WLAN-Ortung
ermöglicht die Standortberechnung anhand von WLAN-Signalen, die ein Smartphone von Hotspots, öffentlichen oder privaten Netzwerken empfängt.

KONTAKT

Ministerium für Familie, Frauen, Jugend, Integration und Verbraucherschutz
Kaiser-Friedrich-Straße 5a, 55116 Mainz
Telefon: +49 (0) 6131 16-0
poststelle@mffjiv.rlp.de | www.mffjiv.rlp.de

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz
Hintere Bleiche 34, 55116 Mainz
Telefon: +49 (0) 6131 208-2449
poststelle@datenschutz.rlp.de | www.datenschutz.rlp.de

Verbraucherzentrale Rheinland-Pfalz e.V.
Seppel-Glückert-Passage 10, 55116 Mainz
Telefon: +49 (0) 6131 2848-0
info@vz-rlp.de | www.verbraucherzentrale-rlp.de

Weitere Informationen
zu Datenschutz und Datensicherheit bei Smartphones und Apps finden Sie im Internet unter **http://s.rlp.de/smartphones** und **www.youngdata.de**.

Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

verbraucherzentrale
Rheinland-Pfalz

RheinlandPfalz
MINISTERIUM FÜR FAMILIE, FRAUEN, JUGEND, INTEGRATION UND VERBRAUCHERSCHUTZ

Impressum

Ministerium für Familie, Frauen, Jugend, Integration und Verbraucherschutz (Hrsg.)
Kaiser-Friedrich-Straße 5a, 55116 Mainz
✆ 06131 16-0 (zentraler Telefondienst), www.mffjiv.rlp.de

Redaktion
Patricia C. Krieger (Referat Reden und Öffentlichkeitsarbeit), Iris Nappe (Referat Digitales, Verbraucherbildung, Verbraucherdialog)

Design und Illustration: Sascha Jaeck
Bildnachweis Innenseite, v. l. n. r.:
© WavebreakMediaMicro, © Andrey Popov / fotolia.com
Außenseite, v. l. n. r.: © pictworks, © daviles / fotolia.com
Druck: Druckerei Zeidler, Mainz-Kastel
Erscheinungstermin: Oktober 2017