



Smartphones & Co: Alles über App und Nepp



Stark für Sie.

www.ak-vorarlberg.at



Im Internet surfen, Mails abrufen, die Benzinpreise der Umgebung checken, Musik hören, telefonieren, fotografieren und Bilder bearbeiten, Videos drehen, Zeitung lesen, Spiele spielen – das alles und noch viel mehr kann man mit Smartphones machen. Smartphones sind keine Handys, sondern mehr oder weniger vollwertige Computer, mit denen man auch telefonieren kann. Und die mobilen Fast-Alles-Köner sind aus den Sakkos, Hand- und Hosentaschen ihrer Besitzer nicht mehr wegzudenken, denn immer mehr Menschen wollen unterwegs mehr als nur telefonieren. Während aber jedem User klar ist, dass er für den PC zu Hause einen vernünftigen Virenschutz bzw. eine Firewall braucht, liegen Smartphones meist vollkommen ungeschützt herum. Offen für Angriffe jeder Art: für Phishing-Attacken, bei denen geheime Passwörter ausspioniert werden ebenso wie für Schadsoftware oder Viren.

Ebenfalls wichtig: Smartphones sind KEIN Kinderspielzeug! Kinder klicken oft unbewusst auf Werbelinks und tätigen dabei vor allem so genannte „In-App“-Käufe. Diese Broschüre will in kurzer Form aufzeigen, welche Sicherheitslücken und Kostenfallen im Umgang mit Smartphones auf die Benutzer lauern. Worauf zu achten ist, wenn es um passende Tarifmodelle geht, wie sich der Transfer von Daten einschränken lässt, was man über Apps wissen sollte und worauf Eltern schauen sollten, wenn der Nachwuchs ein Smartphone in Gebrauch hat.

Was ist ein Smartphone?

Ein Smartphone ist ein multifunktionales Handy. Es lässt sich als Telefon, Terminkalender, Adressbuch, Kamera oder auch als MP3-Player einsetzen und ermöglicht zudem die Nutzung des Internets. Mit kleinen Programmen, so genannten Apps, lässt es sich individuell mit unzähligen Funktionen ausstatten. Gegenüber normalen Handys haben Smartphones meist größere Displays, höhere Rechenleistung für die Apps und mehr Speicherkapazität. Außerdem unterstützen sie Technologien wie UMTS, GPS oder WLAN. Die Technik ist aber noch lange nicht am Ende angelangt. In Österreich wird gerade die 4. Generation des Mobilfunknetzes errichtet. Das LTE-Netz soll eine besonders schnelle Datenübertragung (v.a. Internet) ermöglichen.

Vor dem Kauf

Das Angebot der Netzbetreiber ist so unübersichtlich, dass es meist schwierig ist, den optimalen Tarif zu finden. Entscheidend für die Auswahl ist, zunächst einmal das eigene Nutzerverhalten zu analysieren. Je nach der Art der Nutzung sollten Sie überlegen, ob der Abschluss eines Vertrages oder ein Wertkartentarif sinnvoller ist.

Tip: Als Hilfestellung dient der Handytarif-Rechner der Arbeiterkammer www.ak-vorarlberg.at. Dieser Rechner schlägt – je nach Nutzungsverhalten – den günstigsten Tarif vor.

Vergleichen lohnt sich in jedem Fall!

Vergleichen Sie genau

Vor allem bei scheinbar besonders günstigen Angeboten ist Vorsicht geboten. Nicht selten sind zusätzliche Preisbestandteile wie etwa „Aktivierungsentgelt“, „Sim-Pauschale“ oder „Servicepauschale“ nicht auf den ersten Blick ersichtlich.

Ein auf den ersten Blick tolles Angebot kann bei genauem Nachrechnen dann doch recht teuer sein. Dies trifft beispielsweise auf Angebote für das neueste Smartphone um € 0,- zu, wenn bei langen Bindungsfristen (Mindestvertragsdauer) monatlich ein hohes Grundentgelt zu zahlen ist. Oft ist es günstiger, wenn Sie ein vertragsfreies Handy kaufen und dazu einen günstigen Tarif wählen, der Ihr spezielles Nutzungsverhalten abdeckt.

Stimmt die Qualität?

Bei der Wahl des Netzbetreibers ist abgesehen vom Preis natürlich auf die Qualität zu achten.

Die Netzabdeckung in der Wohn- bzw. Arbeitsgegend spielt bei Handy und mobilem Internet eine wichtige Rolle. Die Rundfunk und Telekom Regulierungs-GmbH (RTR) stellt für mobiles Internet hierzu ein nützliches Tool zur Verfügung:

Unter www.netztest.at können Sie die Qualität von mobilem Internet testen. Es werden auch Hinweise gegeben, wie die Qualität des eigenen Anschlusses verbessert werden kann. Dieses Tool können Sie auch für die Wahl eines für sie geeigneten Betreibers nutzen.

Taktung

Die meisten Tarife werden nicht sekundengenau abgerechnet, sondern mit einer bestimmten „Taktung“. Die für Ihren Vertrag gültige Taktung finden Sie z.B. in den Entgeltbestimmungen.

Bei mobiler Telefonie ist heute sehr häufig die 60/60-Taktung zu finden (bei Festnetztelefonie oder bei der Nutzung teurer Mehrwertdienste werden noch niedrigere Taktungsintervalle angewandt). 60/60 bedeutet, dass für jede angefangene Minute die ganze Minute verrechnet wird. Günstiger wäre z.B. eine Taktung 60/30, wie sie früher sehr verbreitet war. Bei 60/30 wird für den Beginn eines Telefonates immer mindestens eine Minute verrechnet, wird länger als 1 Minute telefoniert, wird in 30-Sekundenschritten abgerechnet.

Gesprächsnachweis

Es ist wichtig, Rechnungen genau zu kontrollieren. Allen Kund/innen steht dafür ein kostenloser Einzelentgeltnachweis (EEN) zur Verfügung.

Im Einzelentgeltnachweis werden alle innerhalb einer Abrechnungsperiode geführten Telefonate bzw. Internetsitzungen getrennt und detailliert aufgelistet. Er informiert Nutzer/innen über Beginn und Ende eines entgeltlichen Gesprächs bzw. einer Internetnutzung, über die Dauer dieser einzelnen Verbindung sowie über dessen jeweilige Kosten.

Meist ist der EEN auf der Webseite des Telekombetreibers mit einem individuellen Code abrufbar. Er kann jedoch auch in Papierform verlangt werden, wofür nichts extra verrechnet werden darf.

Rechnung klassisch oder elektronisch?

Konsument/innen können zwischen einer Rechnung in Papierform und einer elektronischen Rechnung wählen. Für die Papierrechnung darf kein zusätzliches Entgelt verlangt werden.

Die Rechnung wird in der Regel monatlich versandt. Die Rechnung soll immer überprüft werden. Oft erfolgt die Bezahlung automatisch durch Abbuchung vom Bankkonto.

Geschäftsbedingungen und Entgeltbestimmungen

Sind die grundsätzlichen Entscheidungen getroffen und kommt es zum Vertragsabschluss, ist zu beachten, dass auch Allgemeine Geschäftsbedingungen (AGB) und Entgeltbestimmungen (EB) zum Vertragsinhalt werden. In diesen finden sich relevante Regelungen zur Kündigung, zu Einmalentgelten und vieles mehr.

Achtung: Lesen Sie die Geschäftsbedingungen und vor allem auch die Entgeltbestimmungen vor Vertragsabschluss in Ruhe durch. Verlangen Sie diese im Geschäft oder rufen Sie sie im Internet ab. Bewahren Sie die geltenden Bedingungen gemeinsam mit dem Vertrag auf.

Ich bekomme kein Telefon

Mitunter kann es vorkommen, dass ein Vertragsabschluss mangels ausreichender Bonität abgelehnt wird. Grundsätzlich sind Telekommunikationsbetreiber zu den Kriterien der veröffentlichten AGB verpflichtet, mit Ihnen einen Vertrag abzuschließen. Die Betreiberfirma muss es begründen, wenn ein Ablehnungsgrund, wie eben mangelnde Bonität, geltend gemacht wird.

Im Falle einer Verweigerung des Vertragsabschlusses aus diesem Grund haben Sie nach dem Datenschutzgesetz das Recht, beim Telekombetreiber zu erfahren, welche Daten für die Bonitätsprüfung verwendet wurden und woher sie stammen. Diese Auskunft muss vollständig und kostenlos erteilt werden.

Ergibt diese Auskunft, dass ein Wirtschaftsauskunftsdienst Daten über Sie gesammelt hat, ohne Sie darüber vorher informiert zu haben und ohne Ihnen Gelegenheit gegeben zu haben, der Datenverwendung zu widersprechen, dann liegt schon aus diesen Gründen eine unzulässige Datenverwendung vor (dies unabhängig davon, ob diese Daten richtig oder falsch sind).

Nach einer aktuellen Entscheidung der Datenschutzkommission haben Sie Anspruch darauf, dass diese Daten vom Auskunftsdienst nicht mehr verwendet und daher gelöscht werden. Sie müssen diesbezüglich einen Widerspruch formulieren (einen Musterbrief finden Sie unter www.argedaten.at). Wird die Datenlöschung trotz Widerspruchs verweigert, so können Sie sich an die Österreichische Datenschutzkommission wenden.

Bei unzulässiger oder unrichtiger Eintragung in eine Wirtschaftsdatenbank können unter Umständen Schadenersatzansprüche entstehen.

Rufnummernmitnahme

Sowohl Vertragskund/innen als auch Kund/innen mit Wertkarte haben die Möglichkeit, beim Wechsel ihres Telekombetreibers die bisherige Rufnummer beizubehalten. Das regelt eine „Verordnung betreffend die Übertragung von Nummern zwischen Mobil-Telefondienstbetreibern“ (Nummernübertragungsverordnung – NÜV 2012).

Die Rufnummernmitnahme läuft in drei Schritten ab. Zunächst ist die Einholung einer sogenannten Nummernübertragungsinformation notwendig, die Kund/innen Auskunft unter anderem über die verbleibende Vertragsdauer sowie über die Kosten, die mit der Portierung verbunden sind, gibt. Diese Information ist kostenpflichtig (max. EUR 4,- inkl. USt.) und ist sowohl bei der alten als auch bei der neuen Betreiberfirma erhältlich.

Als zweiter Schritt erfolgt der tatsächliche Antrag auf Rufnummernmitnahme. Dieser ist im Shop des neuen Mobilfunkbetreibers zu stellen, wobei ihm die Nummernübertragungsinformation vorzulegen ist, sofern diese nicht schon bei ihm eingeholt wurde. Der (alte) abgebende Mobilfunkbetreiber kann unter Umständen die Nummernmitnahme verweigern, etwa wenn die Rufnummer einem anderen Teilnehmer zugewiesen ist oder bereits ein Übertragungsprozess im Gange ist.

Steht dem Antrag nichts entgegen, kann als dritter Schritt die Rufnummer im neuen Netz aktiviert werden. Dabei sollte der Dienst nicht länger als einen Arbeitstag unterbrochen sein.

Achtung: Auch die gelungene Übertragung Ihrer Rufnummer bedeutet nicht, dass Ihr alter Vertrag automatisch gekündigt ist.

Unbedingt zu beachten sind daher Kündigungsfristen und Mindestlaufzeiten, um zu vermeiden, dass Kosten aus zwei Verträgen anfallen.

Für die Übertragung der Rufnummer dürfen max. EUR 15,- inkl. USt. Portierungsentgelt verrechnet werden. In Summe kann die Rufnummernmitnahme somit bis zu EUR 19,- inkl. USt. betragen.

Netzansagefunktion: In der Regel hat jeder Mobilfunkbetreiber eine eigene Vorwahl (z.B. 0660, 0699, 0664, etc.). Daraus kann im Allgemeinen abgeleitet werden, welchen Mobilfunkbetreiber der/ die Angerufene hat. Wurde die Rufnummer aber bei einem Wechsel des Mobilfunkbetreibers mitgenommen, stimmt das dann natürlich nicht mehr.

Dies spielt bei Tarifkomponenten, die in „in alle Netze“ gleich verrechnen, keine Rolle.

Es kann aber auch sein, dass bestimmte Telefonate/SMS je nachdem, in welches Netz Sie anrufen, unterschiedlich tarifiert werden. In diesem Fall können Sie nur dann die zu erwartenden Telefonkosten einschätzen, wenn Sie die „Netzansage“-Funktion aktiviert

haben. Diese Netzansage weist vor jedem Anruf zu einer übertragenen Rufnummer auf das Netz hin, in das Sie anrufen.

Auf Ihr Verlangen muss Ihr Mobilfunkbetreiber diese Ansage kostenlos freischalten, soweit Telefonate zu mitgenommenen Rufnummern tatsächlich anders verrechnet werden. Für SMS anportierte Nummern besteht allerdings keine derartige Pflicht.

Einseitige Vertragsänderung

§ 25 des Telekommunikationsgesetz 2003 (TKG 2003) gibt Telekommunikationsbetreibern die Möglichkeit, bei Einhaltung bestimmter Vorgaben einseitig Änderungen bei Verträgen oder den Entgeltbestimmungen vorzunehmen. Geplante Änderungen sind der Regulierungsbehörde anzuzeigen und entsprechend kundzumachen. Bei Änderungen, die für die Kund/innen nicht ausschließlich begünstigend sind, hat die Kundmachung und Anzeige zwei Monate vor dem geplanten Inkrafttreten zu erfolgen.

Außerdem ist der wesentliche Inhalt der geplanten Änderung den Kund/innen mindestens einen Monat vor Inkrafttreten der Änderung in schriftlicher Form mitzuteilen. Dies erfolgt häufig auf

der monatlichen Rechnung. Kann die Änderung für Sie Nachteile bedeuten, müssen Sie darauf hingewiesen werden, dass ein außerordentliches Kündigungsrecht besteht.

Der Vertrag kann dann bis zum Inkrafttreten der Änderung kostenlos gekündigt werden. Ein Anspruch darauf, den Vertrag zu den bisherigen Bedingungen weiterzuführen, besteht nicht.

Um die Verständlichkeit der Mitteilung über eine geplante Änderung zu erhöhen, hat die RTR die Mitteilungsverordnung erlassen (MitV). Sie regelt die Form, den Inhalt und den Detaillierungsgrad der gesetzlich vorgeschriebenen Mitteilung zur geplanten Vertragsänderung.

Sicherheitslücken/Gefahren

Bei der Nutzung von Smartphones ergeben sich zahlreiche – auch rechtliche – Probleme. Die Geräte sind für viele Konsumenten Hauptaufbewahrungsort von Daten. Gespeichert sind unter Umständen Kreditkarteninformationen, Bankdaten, Passwörter, Kontakte, Fotos und Videos. Anhand der eingetragenen Infos und vor allem über die Lokalisierungsfunktion lassen sich Verhaltensweisen ermitteln und Bewegungsprofile erstellen. Die Nutzer

können geortet und ihre Daten ausgelesen werden. Sicherheitslücken können aber auch dafür genutzt werden, gezielt Daten auf fremden Smartphones zu manipulieren. Und es ist oft nur schwer zu erkennen, wer für solche Pannen einzustehen hat und sie beheben muss: der Gerätehersteller, der Entwickler des Betriebssystems, der Entwickler der App, der Mobilfunkanbieter – oder am Ende gar der User?

Ein weiteres Problem ist, dass Smartphones zunehmend ins Visier krimineller Machenschaften geraten: Je mehr Menschen Smartphones nutzen, umso lohnenswerter ist es, Viren und andere Schadsoftware zu programmieren. Smartphones sollten daher ähnlich aufwendig abgesichert werden wie normale Computer.

► **Übermittlung bzw. Abfragen von Standortdaten**

Dass Standortdaten unter Apples iOS und Googles Android gespeichert werden, gilt als erwiesen. Was mit den gespeicherten Daten geschieht, ist allerdings umstritten. Einerseits können die Hersteller der Geräte diese Daten an Dritte weiterleiten (z. B. für die Erstellung von verschiedenen Profilen an die Werbewirtschaft). Aber auch eine fremde Person, welche das Gerät kurz in den Händen hat, kann sich leicht Zugang zu den Standortdaten verschaffen. Nutzer, die um ihre Privatsphäre besorgt sind, können fürwürgige Optionen teilweise deaktivieren.

► „Fake SMS“-Nachrichten

Mittels einfacher Programme lassen sich SMS versenden, bei denen der Name des Anrufers bzw. die angezeigte Rufnummer des Anrufers beliebig gefälscht werden kann. Dies bringt die Gefahr mit sich, dass dies missbräuchlich für Phishing-Angriffe genutzt werden kann. Dabei gibt der Absender beispielsweise an, dass die eingelangte SMS von der Hausbank stammt und man aufgrund eines Sicherheitsupdates die Zugangsdaten für die Onlinebanking-Funktion zurücksenden solle. Damit verschaffen sich Kriminelle Zugang zum Onlinebanking-Portal und können so erheblichen Schaden anrichten.

► Fake ID-Call

Auch bei Anrufen ist das Verfälschen der Absendernummer oder des Absendernamens, welcher auf dem Display angezeigt wird, sehr leicht möglich. Potenzielle Opfer können hiermit ebenfalls zur Herausgabe von persönlichen Daten bewegt werden. Beispielsweise, indem der Anrufer sich als Mitglied einer Behörde, Bank oder sonstigen Institution ausgibt.

ACHTUNG: Weder Banken noch Behörden usw. erfragen solche sensible Daten mittels Telefon, SMS oder E-Mail! Hinterfragen Sie solche Kontakte und geben Sie keinesfalls persönliche Daten auf diesem Weg bekannt.

► Nutzung von Onlinediensten

Bei der Verwendung von Onlinediensten (Amazon, Ebay, Facebook, Webmail usw.), bei denen eine Anmeldung mittels Kennwort und Passwort zum Schutz des Konsumenten erforderlich ist, sollten Sie sehr penibel darauf achten, dass eine gesicherte Internetverbindung hergestellt wird. Erkennbar ist eine solche durch die Zeichenfolge `https://` im Internetbrowser des Smartphones. Mittlerweile sind Programme verfügbar, die es aufgrund vorhandener Sicherheitslücken ermöglichen, mit Hilfe eines anderen Smartphones direkt ungesicherte Verbindungen (`http://`) auszulesen. Dadurch kann der Angreifer, der sich in einer gewissen Nähe zum Nutzer aufhalten muss, das Kenn- bzw. Passwort problemlos ändern und den jeweiligen Account auf seinem Gerät übernehmen. Dadurch ist einem Identitätsdiebstahl (z. B. Facebook) oder einem Einkauf auf fremden Namen (Amazon, Ebay) Tür und Tor geöffnet.

► Fake WLAN Access Point

Vorsicht ist auch bei der Nutzung von vermeintlich öffentlichen WLAN-Hotspots dringend angebracht. Mittels eines Notebooks und einer entsprechenden Software ist es einem Angreifer möglich, einen öffentlich und gratis zugänglichen WLAN-Hotspot an belebten Plätzen wie z. B. einem Einkaufszentrum vorzutäuschen. Das Smartphone zeigt auf dem Display die Verfügbarkeit eines

solchen Zugangspunktes an, tatsächlich verbirgt sich dahinter lediglich der Versuch eines Hackers, sich Zugang zu den hergestellten Internetverbindungen der an diesem Standort eingewählten Smartphones zu verschaffen. Alle Daten, welche durch den Nutzer der Internetverbindung über diesen WLAN-Punkt fließen, können vom Angreifer auf seinem PC/Notebook mitgelesen werden.

Generell ist zu empfehlen, keine sensiblen Vorgänge (Online-banking, Internetshopping usw.) mittels eines öffentlichen WLAN-Zugangs durchzuführen, da sich Dritte recht einfach Zugang zum Datentransfer des Nutzers verschaffen können. Sollte man dennoch nicht darauf verzichten wollen oder können, ist es dringend zu empfehlen, solche Dienste nur durch eine gesicherte (https://-)Verbindung in Anspruch zu nehmen. Außerdem sollte die Funktion „automatisches Synchronisieren“ deaktiviert werden, da sonst die Gefahr besteht, dass sich das Smartphone möglicherweise automatisch mit einem vom Gerät vorgefundenen offenen WLAN verbindet.

Achtung: Die hier dargestellten Fallen/Gefahren/Sicherheitslücken erheben nicht den geringsten Anspruch auf Vollständigkeit. Sie stellen lediglich eine kurze Auflistung möglicher Gefahrenpotenziale dar. Durch die ständigen technischen Verbesserungen (höhere Datengeschwindigkeiten, neue Betriebssysteme, neue Verwendungsmöglichkeiten) ergeben sich auch laufend neue potenzielle Angriffsszenarien.

Alle hier dargestellten Formen der Zugangsbeschaffung zu persönlichen, sensiblen Daten dritter Personen dienen lediglich dem Zweck der Information und Warnung von Benutzern von Mobiltelefonen. Das Ausführen der beschriebenen Handlungen ist rechtlich selbstverständlich untersagt und kann strafrechtlich verfolgt werden. Von einer Nachahmung solcher Handlungen ist entschieden abzuraten.

Apps – Programme, die das Handy „smart“ machen

Was sind Apps?

„App“ ist die Kurzform von „Application“ und bedeutet in etwa „Programm“ oder „Software“. Apps erfüllen tausende Funktionen: von der Taschenlampe bis zum Messwerkzeug, vom Videoschnitt bis zum Mückenschutz, vom Wetterdienst bis zum Babyfon. Es gibt fast nichts, was es nicht gibt. Viele Apps sind kostenlos, andere müssen mehr oder weniger teuer bezahlt werden. Apps können aber auch gewisse Risiken mit sich bringen (z. B. Verletzung des Datenschutzes oder unerwartete Kosten).

Wie funktionieren Apps?

Apps sind Programme, die für ganz bestimmte Anwendungsbereiche entwickelt wurden: Freizeit, Kommunikation, Gesundheit, Bildung, usw. Apps sind sehr einfach auf einem mobilen Gerät zu installieren und können auch verschiedenste Funktionen des Handys (z. B. Kontakte) mit Daten aus dem Internet (z. B. Kartenmaterial) verknüpfen, um bestimmte Infos bereitzustellen.

Wo finde ich Apps?

Je nach Handyplattform bzw. Betriebssystem des Smartphones können die Apps über spezielle Onlineshops gesucht, ausgewählt und einfach über die Internetverbindung des mobilen Gerätes bzw. über den Computer heruntergeladen und installiert werden. Nutzer müssen sich dazu einmalig anmelden bzw. für kostenpflichtige Apps z. B. die Kreditkartennummer angeben.

Apps sind in der Regel für ein bestimmtes Handybetriebssystem programmiert und können ohne technische Anpassungen auch nur auf dem entsprechenden System laufen. Die gängigsten Betriebssysteme für Smartphones sind Android, iOS, Symbian, Windows Phone, BlackBerry OS und bada.

Die Betreiber der App-Shops verwalten das Angebot zentral, wobei einige die von den Entwicklern gelieferten Apps auch vor der Freigabe überprüfen (z. B. App Store von Apple). Schadhafte oder beanstandete Apps können aus dem App-Shop bzw. auch von den Endgeräten gelöscht werden.

App Stores für die gängigsten Handy-Plattformen

Apple App Store:

<https://www.apple.com/iphone/apps-for-iphone>

Nokia Ovi Store:

<https://store.ovi.com>

BlackBerry App World:

<https://appworld.blackberry.com>

Google Play Store:

<https://play.google.com/store>

Windows Phone Marketplace:

<https://www.windowsphone.com/de-DE/store>

Welche Apps gibt es?

Aktuell gibt es je nach Store bis zu 800.000 verschiedene Apps für eine Vielzahl von Anwendungen. Die beliebtesten sind z.B. Zugangsprogramme für soziale Netzwerke, Spiele, Nachrichtendienste, Nachschlagewerke oder Fahrplanauskünfte. Die Bandbreite der mehr oder weniger nützlichen Anwendungen ist mittlerweile unüberschaubar.

Achtung: Neben vielen nützlichen Programmen gibt es zahlreiche Scherzprogramme und Programme, die unbemerkt Daten sammeln oder schädliche Software am Gerät installieren.

Wie funktioniert das Geschäft mit den Apps?

Wie vom Internet bekannt, gibt es auch bei Apps kostenlose und kostenpflichtige Angebote. Zahlreiche kostenlose Apps finanzieren sich über Werbeeinschaltungen, die bei Nutzung der Apps angezeigt werden und die Sammlung und Weitergabe von persönlichen Daten. Sie spionieren dadurch ihre Nutzer regelrecht aus. Sie verlangen Zugriff auf Adressbücher, Kalender und SMS sowie uneingeschränkten Internetzugriff oder Zugriff auf GPS Koordinaten. Erfahrungsgemäß verdienen am Erlös der durch den

Verkauf bzw. die Nutzung von Apps erzielt wird, sowohl die Entwickler als auch die Betreiber der Stores mit.

Die größten App-Fallen

► Unbemerkte Übertragung persönlicher Daten

Studien zeigen, dass viele Apps sensible Nutzerdaten übertragen – auch wenn diese für die Funktion der Apps nicht notwendig sind (z. B. Standortdaten bei einer Spiele-App).

► Schadsoftware und Viren

Über die App-Shops werden nicht nur sichere Programme bereitgestellt, sondern immer wieder auch mit Schadsoftware infizierte Apps. Diese verseuchten Programme können Handydaten – z. B. Kontaktdaten – unbemerkt und unbefugt übermitteln oder kostenpflichtige SMS an Mehrwertnummern versenden.

► Abzocke

Viele kostenlose Apps finanzieren sich aus Werbeeinschaltungen, über die man auch Bestellungen tätigen oder auf Angebote im Internet weitergeleitet werden kann. Neben der breiten Masse der seriösen Werbeangebote gibt es auch Fallen, bei denen versteckt Bestellungen oder Abo-Verträge abgeschlossen werden. Die Nutzer

werden dabei nicht ausreichend über die Vertragsbedingungen und Preise informiert. Oft wird dies erst im Nachhinein bemerkt, da manche dieser zweifelhaften Angebote über die Mobilfunkrechnungen abgerechnet werden.

► „In-App“-Käufe

Bei manchen Apps (z. B. bei Spielen) besteht die Möglichkeit, in der Anwendung selbst ein Guthaben oder Punkte zu kaufen (so genannte „In-App“-Käufe), ohne den klassischen Bestellprozess zu durchlaufen. Damit besteht die Gefahr, unbewusst Geld auszugeben. Oft tätigen auch Kinder unbewusst Bestellungen, wenn sie mit dem Smartphone spielen.

Achtung: Viele App-Anbieter erfüllen die Informationspflichten nach dem Konsumentenschutzgesetz nicht. Deshalb ist prinzipiell ein Rücktritt vom Vertrag möglich. Außerdem kann im Falle eines nicht ausreichend geschäftsfähigen Kindes der Vertragsabschluss unwirksam sein. Wenden Sie sich bei Problemen direkt an den Kundenservice der App-Shops.

App-Tipps

► Apps hinterfragen

Fragen Sie sich, welche Apps Sie wirklich brauchen oder unbedingt ausprobieren wollen. Lesen Sie die Bewertungen der Apps und installieren Sie schlecht bewertete Apps besser nicht.

► Apps ausmisten

Löschen Sie Apps, die Sie nicht mehr brauchen. Diese können im Hintergrund auch keine unerwünschten Daten mehr übertragen.

► Nur Apps aus App Stores

Installieren Sie nur Apps aus den offiziellen App Stores, da diese entweder vor der Bereitstellung überprüft wurden oder bei größeren Beschwerden aus dem App Store bzw. vom Handy via Fernlöschung entfernt werden.

► Berechtigungen checken

Kontrollieren Sie bei der Installation von Apps die Zugriffsberechtigungen (z. B. bei Android-Handys bevor Sie auf „Installieren“ klicken) und installieren Sie eine App, die offensichtlich zu viele Berechtigungen für den Funktionsumfang bietet, lieber nicht.

► Betriebssystem nicht ändern

Nehmen Sie keine Änderungen am Handy-Betriebssystem („Jailbreak“ oder „Rooten“ genannt) vor, da diese die Installation von unsicheren Apps erleichtern und auch die Updates des Handy-Betriebssystem beeinträchtigen können.

► Aufpassen bei Gratis-Apps

Seien Sie besonders bei kostenlosen Apps und damit verbundenen Werbelinks vorsichtig.

► Kein Spielzeug

Vorsicht, wenn Kinder mit dem Smartphone spielen. Sie könnten unbemerkt Werbelinks anklicken und damit unbewusst Bestellungen („In-App“-Käufe) tätigen.

► „In-App“-Käufe ausschalten

Deaktivieren Sie „In-App“-Käufe am Handy und schalten Sie diese nur im Bedarfsfall gezielt frei – beim iPhone z. B. unter Einstellungen/Allgemein/Einschränkungen, bzw. bei Android Handys z. B. durch Deaktivierung von Google Checkout, falls Sie sich dort registriert haben.

► **Passwörter & PINs**

Sichern Sie Ihr Smartphone gegen unbefugten Zugriff (PIN-Code, Zugriffsschutz mit Passwort oder Entsperrmuster) und verwahren Sie es sicher.

► **Schutzsoftware**

Installieren Sie eine Schutzsoftware auf Ihrem Smartphone. Damit können Sie schädliche Software erkennen und löschen. Zahlreiche Virenschutzprogramme finden sich inzwischen in den einzelnen Stores unter dem Stichwort „Virenschutz“. Informieren Sie sich umfassend über deren Eigenschaften, Handhabung und achten Sie auf die Bewertung der Apps um einen Favoriten für das Ihnen verwendete Smartphone auszuwählen. Verschiedene Programme bieten auch die Möglichkeit, verlorene Handys zu orten und bei Verlust persönliche Daten per Fernzugriff zu sperren oder zu löschen.

► **Automatische Updates deaktivieren**

Wenn Sie einen Datentarif mit begrenztem Datenvolumen nutzen, beachten Sie, dass Apps nicht nur beim erstmaligen Herunterladen, sondern auch während der Nutzung und beim Updaten Datenvolumen verbrauchen. Sie können z. B. die Funktion „automatisches Update“ ausschalten und Updates nur zulassen, wenn Sie noch genügend Datenvolumen zur Verfügung haben oder mit dem Smartphone eine WLAN-Verbindung nutzen.

Tipps für Eltern

Smartphones erfreuen sich nicht nur bei Erwachsenen wachsender Beliebtheit. Auch Kinder entdecken die vielen Vorteile der Geräte, und können sich dabei vor allem für Apps begeistern. Worauf Sie als Eltern im Umgang mit Apps besonders achten sollten:

Auswahl geeigneter Spiele

Die meisten Anbieter von Apps haben eigene Kategorien für Kinder. Werfen Sie einen Blick auf die am häufigsten geladenen Spiele und berücksichtigen Sie dabei auch Bewertungen und Altersangaben. Besonders geeignet sind Quizzes, Gehirn-Trainings- oder Zeichenprogramme. Diese machen Kindern Spaß und haben dabei gleichzeitig einen Lerneffekt. Wenn Sie sich für eine App entschieden haben, testen Sie diese zuerst selbst. Können Sie bei kostenlosen Versionen wirklich alle Funktionen nützen? Immer wieder sind Gratis-Spiele so gestaltet, dass man im kostenlosen Modus nur langsam vorwärts kommt. Testen Sie auch, ob die App wirklich anwenderfreundlich ist. Bei längeren Ladezeiten verlieren Kinder das Interesse. Apps, die nicht diesen Kriterien entsprechen, sollten Sie lieber gleich wieder löschen.

Kostenkontrolle

Apps sind in der Regel nicht teuer. Wer viele Apps gleichzeitig testet, kann allerdings leicht den Überblick verlieren. Tipp: Deaktivieren Sie „In-App“-Käufe. Damit sind Käufe während eines Spiels von vornherein ausgeschlossen. Die meisten Apps verbinden sich mit dem Internet. Deshalb sollten Sie Spiele vor allem dann nutzen, wenn Sie in einem kostenlosen WLAN surfen. Begrenztes Datenvolumen und Daten-Roaming können hier schnell zu hohen Kosten führen. Manche Spiele werben mit kostenlosem, virtuellem Geld („Free Cash“).

Ein Beispiel: Die App verbindet sich mit dem persönlichen Facebook-Account, und zeigt dem Profil an, welche Spiele gerade gespielt werden. Überlegen Sie mit Ihrem Kind gemeinsam, ob das erwünscht ist. Manchen Kindern ist es eher peinlich, wenn die Facebook-Freunde sehen, welche Spiele sie spielen.

Vorsicht: Wer eine WLAN-Verbindung hat, surft nicht immer automatisch über diese. Kontrollieren Sie deshalb vor einem Datentransfer anhand des entsprechenden Symbols auf dem Bildschirm, ob Sie tatsächlich per WLAN verbunden sind.

Sicherer Umgang mit Apps

Bei vielen Apps können Sie beim erstmaligen Laden Einstellungen vornehmen. Dazu gehört die Einstellung „Aktuellen Ort verwenden“. Diese macht Sinn, wenn es sich um eine Navigationsanwendung handelt (z. B. Straßenkarte), ansonsten sollten Sie diese deaktivieren. So genannte „Push“-Nachrichten werden in erster Linie für Werbung genutzt und sind daher nicht zu empfehlen. Bei Pop-up-Fenstern sollten die Kinder immer nachfragen, bevor sie eine Auswahl treffen. Apps regelmäßig ausmisten und alles, was nicht mehr benötigt wird, löschen.

Empfehlungen für Apps

www.saferinternet.at



Den Datenverkehr im Griff

Bei Tarifen mit begrenztem Datenvolumen bzw. beim Auslands-Roaming ist es wichtig, den Datentransfer im Auge zu behalten, sonst kann es mitunter richtig teuer werden. Während der Datentransfer bei Note- und Netbook noch relativ einfach ist, liegt der Fall bei Smartphones und auch bei Tablet-PCs schon schwieriger, denn hier haben Sie weit weniger Kontrolle. Egal ob Android oder iOS als Betriebssystem zum Einsatz kommt, gibt es eine Vielzahl von Aktualisierungen, die auch im Standby-Modus, also bei ausgeschaltetem Bildschirm, aber eingeschaltetem Gerät durchgeführt werden.

Einige Beispiele: das regelmäßige Abrufen von E-Mails von einem oder mehreren hinterlegten E-Mail-Konten, die laufende Aktualisierung von Wetterdaten oder Nachrichten-Feeds oder auch das Lokalisieren des Geräts, sofern das nicht ausschließlich über das eingebaute GPS-Modul erfolgt. Besonders viel Datenverkehr verursacht das Updaten der installierten Apps, wenn Sie das über den dazugehörigen App-Shop oder -Markt automatisch erledigen lassen. Vor allem das Aktualisieren größerer Apps sollten Sie gezielt erledigen, wenn Sie in einem kostenlosen WLAN eingebucht sind.

Unter Android finden Sie alle dafür benötigten Einstellungen unter „Einstellungen, Konten & Synchronisierung“. Hier können Sie pauschal die Synchronisierung von Daten unterbinden, indem Sie unter „Automatische Synchronisierung“ das Häkchen entfernen oder – noch umfassender – das Häkchen bei „Hintergrunddaten“ entfernen. Wer es individueller mag oder braucht, kann unten die automatisch auf das Internet zugreifenden Apps und Konten durchsehen und individuell entscheiden, welchen er wie viel Autonomie ermöglichen will. Ein möglicher Kompromiss ist es z. B. bei Wetter-Apps, die Häufigkeit der Synchronisierung von wenigen Minuten auf mehrere Stunden herabzusetzen.

Unter „Einstellungen, Ort“ können Sie, falls Sie Datenverkehr sparen wollen, festlegen, dass die Bekanntgabe Ihres Aufenthaltsorts ausschließlich über das integrierte GPS-Modul erfolgt, nicht über die IP-Adressenzuordnung. Entfernen Sie das Häkchen bei „Wireless nutzen“ (der Punkt heißt bei einigen Android-Versionen „Drahtlosnetzwerke“ und findet sich unter „Standort & Sicherheit“).

Bei iPhone und iPad werden die Apps standardmäßig nur auf Nachfrage aktualisiert und ab 20 MB nur heruntergeladen, wenn eine WLAN-Verbindung gegeben ist. Zusätzlich sollte man aber unter „Einstellungen, Mail, Kontakte, Kalender“ die so genannten „Push“-Funktionen unterbinden, indem die Einstellung von 1

auf 0 gesetzt wird. Wenn die manuelle Aktualisierung für Sie nicht ausreicht, können Sie darunter das Zeitintervall für automatische Aktualisierung auf „Stündlich“ setzen. Zusätzlich können Sie unter „Einstellungen, Store“ festlegen, dass App-Store-Daten generell nur über eine WLAN-Verbindung bezogen werden.

Die beschriebenen automatischen Einschränkungen sparen übrigens nicht nur Datenverkehr ein, sondern unterstützen damit verbunden auch die Akkuleistung. So verlängern Sie ganz nebenbei die Laufzeit Ihres Smartphones oder Tablet-PCs.

Konsumenten sollten ihren Verbrauch laufend kontrollieren. Dies ermöglichen die Netzbetreiber meist online oder per Abfrage. Hierbei sollte aber immer auf die Aktualität der Informationen geachtet werden.

Wer ein Smartphone mit vielen Funktionen verwendet, sollte daher unbedingt auch einen passenden Tarif wählen. Es empfiehlt sich, gleich beim Kauf des Telefons Rat von Experten einzuholen, die Handbücher der Handys genau durchzulesen und jedenfalls laufend die angefallenen Kosten immer wieder zu kontrollieren.

Sollte trotzdem eine viel zu hohe Rechnung ins Haus flattern, besteht die Möglichkeit, binnen einer Frist von drei Monaten schriftlich Einspruch beim Betreiber zu erheben.

Kostenbeschränkungsverordnung (KobeV)

Mit 1. Mai 2012 trat die Kostenbeschränkungsverordnung (KobeV) der Regulierungsbehörde RTR in Kraft. Darin ist vorgesehen, dass Kostenüberschreitungen bei Datenverbindungen künftig nur noch maximal 60 Euro pro Abrechnungszyklus betragen dürfen (zusätzlich zur monatlichen Grundgebühr). Das ist zwar noch immer viel Geld, aber wenigstens dürften die extremen Kostenausreißer der Vergangenheit angehören.

Unverändert hoch bleiben hingegen die Tarife der Betreiber, wenn Datenguthaben überschritten werden. Zwar soll künftig bei 60 Euro Schluss sein, dieser Betrag dürfte aber sehr rasch erreicht werden, wenn die Tarife für Datentransfers außerhalb der vertraglich vereinbarten Volumina um bis zu 6000 Mal höher liegen.

Ebenfalls nicht gefeit ist man vor hohen Kosten bei Mehrwertnummern oder SMS. Denn für Sprachverbindungen und SMS sind in der Kostenbeschränkungsverordnung keine Sperrmöglichkeiten vorgesehen.

Mit dem neuen Telekommunikationsgesetz steht Ihnen eine kostenlose Papierrechnung zu. Nützen Sie diese Möglichkeit und kontrollieren Sie anhand der Rechnung die aufgelaufenen Kosten, und erheben Sie gegebenenfalls Einspruch beim Netzbetreiber bzw. bei der Regulierungsbehörde.

Neue Roamingverordnung

Am 1. Juli 2012 trat die Neufassung der EU-Roaming-Verordnung in Kraft.

Die Regelungen der Roaming III-Verordnung gelten zunächst für die 27 Mitgliedstaaten der Europäischen Union. Seit 7.12.2012 gilt die RoamingVO auch in den EWR-Staaten Norwegen, Island und Liechtenstein. Die Kostenbegrenzungsfunktion bei Datenroaming gilt weltweit.

Diese Verordnung besagt, dass

- ▶ dem Roamingkunden eine Option bereitgestellt werden muss, welche Informationen über die bisherige Nutzung des Datenvolumens bzw. die entstanden Kosten aufzeigt;
- ▶ dem Roamingkunden ein Höchstbetrag angeboten wird, der EUR 50,- netto nicht übersteigt (zusätzlich zur monatlichen Grundgebühr und sonstiger Entgelte);
- ▶ dass an das mobile Gerät des Roamingkunden eine geeignete Meldung übermittelt wird, sobald 80 % des vereinbarten Höchstbetrages oder der Obergrenze für das Datenvolumen erreicht wurden.
- ▶ wenn der Roamingkunde auf eine entsprechende Meldung nach Aufbrauchen des Volumens nicht reagiert, ist die Erbringung und Inrechnungstellung von Datenroaming unverzüglich einzustellen.

Die Obergrenze von EUR 50,- gilt für alle Kunden, die keine andere Obergrenze gewählt haben.

Nach wie vor günstiger ist es aber jedenfalls das „Daten-Roaming“ im Ausland generell zu deaktivieren und das Internet wenn möglich nur über kostenlose W-Lan Netzwerke zu verwenden.



Bei der Rechnung stimmt etwas nicht!

Gegen eine unklare Rechnung sollte jedenfalls binnen drei Monaten ab Erhalt schriftlich Einspruch beim Telekombetreiber erhoben werden. Im Einspruchsschreiben sind die Gründe darzulegen, warum die Rechnung für unrichtig erachtet wird. Gleichzeitig mit dem Einspruchsschreiben sollte bei der Rundfunk und Telekom Regulierungs-GmbH ein Antrag auf Aufschub der Fälligkeit des strittigen Rechnungsbetrags gestellt werden.

Fällt die Antwort des Telekombetreibers nicht zufriedenstellend aus oder kommt binnen sechs Wochen gar keine Antwort, kann ein Schlichtungsverfahren bei der RTR beantragt werden (Adresse siehe Ende des Folders). Das Verfahren ist bis auf eigene Aufwendungen wie Kopierkosten kostenlos. Die Schlichtungsstelle wird versuchen, vermittelnd einzugreifen und eine Lösung zu erzielen.

Konsumentenberatung der AK Vorarlberg

Widnau 2 – 4 , 6800 Feldkirch

Telefon 050/258-3000

konsumentenberatung@ak-vorarlberg.at

Regulierungsbehörde

RTR/Schlichtungsstelle Telekommunikation

www.rtr.at

Internetombudsmann

www.ombudsmann.at

Impressum

Stand: Juni 2015

Herausgeber: AK Vorarlberg

Widnau 2 – 4, 6800 Feldkirch

Telefon 050/258-0, Fax 050/258-1001

kontakt@ak-vorarlberg.at, www.ak-vorarlberg.at

Foto: shutterstock, fotolia

Die vorliegende Broschüre wurde nach bestem Wissen verfasst. Dennoch kann keine Haftung für die Richtigkeit und Vollständigkeit sämtlicher Informationen übernommen werden. Die allgemeinen Informationen ersetzen im konkreten Einzelfall keine rechtliche und persönliche Beratung.



Konsumentenberatung

Widnau 2 – 4, 6800 Feldkirch
Telefon 050/258-3000
Fax 050/258-3001

konsumentenberatung@ak-vorarlberg.at
www.ak-vorarlberg.at

Stark für Sie.

www.ak-vorarlberg.at