Guter Umgang mit dem Smartphone

Der Umgang mit dem Smartphone ist in den letzten Jahren durchwegs Thema der öffentlichen Medien. Kein Wunder, schließlich ist das Smartphone als täglicher Begleiter nicht mehr wegzudenken. Aus Statistiken (vgl. www.rtr.at, Telekom-Monitor, Jahresbericht 2022) geht hervor, dass bereits eine Verbreitung von über 200 % erreicht wurde – somit besitzt statistisch gesehen jede:r Einwohner:in Österreichs im Durchschnitt 2 SIM-Karten. Der Bedarf ist stetig steigend, da die SIM-Karten für Smartphones, Tablets und Datensticks verwendet werden.

Auch bei Jugendlichen gab es bei der Smartphone-Verbreitung in den vergangenen Jahren eine deutliche Steigerung. Für das Jahr 2022 kann man bei der Altersgruppe der 12 bis 19-Jährigen nahezu von einer Vollversorgung sprechen. 96 % haben ein Smartphone.
(vgl. JIM-Studie 2022, S. 6f unter www.mpfs.de).

Verändertes Nutzungsverhalten

Neben der Verbreitung hat sich auch in der Nutzung einiges getan. Besonders durch die rasche Verbreitung der Smartphones spielen Internet, Mailempfang und Apps neben den herkömmlichen Handyfunktionen wie Telefonieren und SMSen eine wesentliche Rolle. Das Smartphone ist für Jugendliche das Gerät, das sie im Vergleich zu Computer oder Tablet mit Abstand am häufigsten zur Internetnutzung einsetzen.
(vgl. JIM-Studie 2022, S. 26 unter www.mpfs.de)
Daneben spielen Funktionen wie Musik hören, Fotos verschicken, Downloads, Apps, Spiele oder die Bezahlfunktion des Handys eine wesentliche Rolle.

In der Werbung wird mit Pauschaltarifen (sogenannten Flatrate-Tarifen) gelockt, die Gratis-Telefonate, Frei-SMS und unlimitiertes Datenvolumen versprechen. Dabei übersehen manche Nutzer:innen, dass solche „Gratis-Angebote“ in der Regel auf z.B. 1.000 Minuten Gesprächszeit begrenzt sind und gewisse Anrufe (z.B. 05 Rufnummern, Mehrwertnummern) generell nicht im Pauschalkontingent inbegriffen sind. Sobald diese Grenzwerte überstiegen werden, stellt der Handybetreiber die Dienste teuer in Rechnung. Um unliebsame Überraschungen zu vermeiden, ist es wichtig, das vereinbarte Datenvolumen unbedingt im Auge zu behalten. Die Kostenbeschränkungsverordnung für alle Mobilfunkverträge regelt, dass ohne Zustimmung von Verbraucher:innen kein höheres Entgelt als € 60,00 für mobile Datendienste verrechnet werden darf.

Handy – Stolperstein

Verschiedene Tarife erschweren Vergleiche (AK Tarifrechner verwenden)
- Inklusiv-Leistungen unterscheiden
- Niedrige Gesprächsgebühren oft mit hohen Zusatzkosten
- Teure Roaminggebühren außerhalb der EU

Abrechnungsprozesse
- Mehrwertnummern (0900 ...) mit maximal EUR 3,64/min oder EUR 10,– pro Anruf oder SMS
- Recht auf kostenlosen Einzelentgeltnachweis
- Einspruch beim Telefonunternehmen und bei Rundfunk und Telekom Regulierungs GmbH

Bild: Sozialministerium/shw

Weitere Kostenfallen: Musik, Videos, Spiele & Apps

Das Handy wird zunehmend als Prestigeobjekt gesehen und daher von jungen Menschen gerne persönlich gestaltet.

Das Smartphone bietet unzählige Möglichkeiten wie das Abspielen von Songs, Videoclips sowie Apps und Spiele in vielen Varianten. Die rasante Entwicklung und die Vielzahl von Anbietern ermöglicht es, das eigene Telefon noch individueller zu gestalten. Ebenso birgt dies aber auch Risiken, die oft für Jugendliche nicht sofort erkennbar sind. Mögliche Risiken entstehen unter anderem durch unseriöse Werbeangebote und Abo-Fallen. Aber auch Viren oder infizierte

Software können Schaden am Smartphone verursachen, Handydaten unbemerkt übermitteln oder sogar kostenpflichtige SMS an Mehrwertnummern versenden.

Mehrwertdienste per Anruf oder SMS sind an den Rufnummern (z.B. 0900) erkennbar und können beim Mobilfunkanbieter gesperrt werden.

Oft muss bei Gewinnspielen oder fragwürdigen Angeboten die Handynummer eingegeben werden. Manchmal ist nur schwer erkennbar, dass hier ein Mehrwertdienst-Abo eingegangen wird. Hier ist kritisch anzumerken, dass in vielen Fällen die von den Anbietern angegebenen Passwörter für eine Abbestellung sehr kompliziert und nur schwer zu merken sind. Nur einzelne weisen auf ihrer Website auf die einfache Möglichkeit, das Abo mit einer SMS mit dem Inhalt „Stopp“ (für das Einstellen eines speziellen Dienstes) oder „Stopp alle“ (für das Einstellen aller Dienste eines bestimmten Anbieters) zu kündigen, hin.

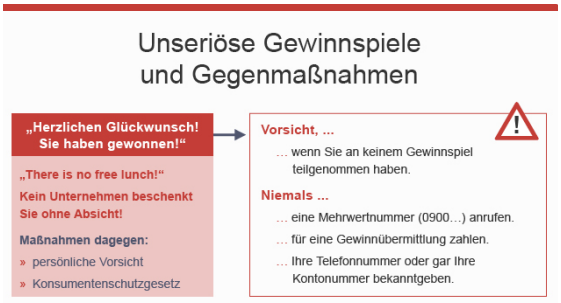

Bild: Sozialministerium/fridrich/oegwm

Auch in Bezug auf Apps sollte man vorsichtig sein. So können etwa „In-App-Käufe“ – das sind Einkäufe innerhalb der Anwendung z.B. für Zusatzpakete oder Spielguthaben – die Kosten in die Höhe treiben. In-App-Käufe können deaktiviert werden.
(vgl. www.saferinternet.at).

Bezahlen mit dem Smartphone

Mit dem Smartphone zu bezahlen ist bei manchen Dienstleistungen durchaus verbreitet. Verschiedene Anbieter machen es möglich, dass Park- und Fahrscheine, Konzertkarten, Logos, Klingeltöne und auch Snacks, Zugkarten, Flugtickets sowie Einkäufe im Einzelhandel mit dem Handy bezahlt werden können. Bei dieser Form des bargeldlosen Bezahlens wird das Smartphone zur mobilen Geldbörse. Der Betrag wird üblicherweise direkt vom Bankkonto abgebucht. Es gibt sowohl kostenlose Angebote, aber auch jene, die mit einmaligen Aktivierungs- und monatlichen Grundgebühren verbunden sind. Hier ist es vor allem empfehlenswert, die unterschiedlichen Angebote und Dienste zu vergleichen und die Kosten vorab zu berechnen.

Entscheidet man sich für das Bezahlen mit dem Smartphone, muss der Dienst häufig über das Internet aktiviert werden und die Kosten werden über das Bankkonto verrechnet. Um zu verhindern, dass bei Diebstahl oder Verlust eine andere Person mit dem Handy bezahlen kann, gibt es die Möglichkeit, eine persönliche PIN anzufordern. Wird dann mit diesem Smartphone bezahlt, erfolgt ein automatischer Anruf. Erst mit Eingabe der PIN wird die Zahlung freigegeben.

WAP-Billing gilt ebenfalls als Verrechnungsmöglichkeit von mobilen Diensten. Hier erfolgt die Bezahlung jedoch über die nächste Handyrechnung. Besondere Vorsicht ist geboten, denn es passiert sehr schnell, in eine sogenannte Smartphone-Abofalle zu tappen. „Häufig finden sich in Gratis-Apps oder auch auf mobilen Website-Versionen Werbebanner, die zu Abo-Fallen über WAP-Billing führen können“.
(vgl. www.saferinternet.at/faq/internetbetrug/ich-bin-in-eine-wap-billing-falle-getappt-was-tun)

Die Verantwortung der Erziehungsberechtigten

Besondere Brisanz kommt der Tatsache zu, dass Minderjährige ein Vertragshandy nur mit der von Eltern unterschriebenen Haftungserklärung erhalten. Dadurch stehen die paybox-Dienste den Jugendlichen im vollen Umfang zur Verfügung.

Es liegen Fälle vor, bei denen Minderjährige Produkte über Online-Dienste bestellt oder bei Glücksspielen mitgemacht haben. Hohe Kosten waren die Folge, die die Eltern bezahlen mussten. Diese Tatsache wird von den Erziehungsberechtigten bei der Anmeldung des Handys oft übersehen, bzw. sind vielen die Konsequenzen nicht bewusst.

Ständige Auseinandersetzung

Durch die ständige Weiterentwicklung der Möglichkeiten in der Handynutzung ist es unerlässlich, sich ständig mit den Neuerungen zu befassen. Gerade Jugendliche tendieren dazu, allzu freizügig ihre Daten weiterzugeben oder Dienste zu nutzen, ohne sich der Konsequenzen bewusst zu sein. Indem auf die möglichen Fallen hingewiesen wird, erhalten sie Unterstützung beim Erlernen eines bewussten und verantwortungsvollen Umgangs.

Alt und jung

Nahezu in Vergessenheit geraten ist das Festnetz. Um dessen Attraktivität zu steigern, bieten einige Telekommunikationsunternehmen preisgünstige Kombinationspakete an, die neben Festnetz auch Internet, Fernsehen und Tarife für Smartphones beinhalten. Ein Angebots- und Preisvergleich kann sich hier auszahlen.

Eine weitere Entwicklung auf diesem Sektor ist die IP-Telefonie (Internet-Protokoll-Telefonie), auch Internet-Telefonie oder Voice over IP genannt. So kann etwa mit einer (oft kostenlos erhältlichen) Software über das Internet unentgeltlich von Computer zu Computer und gebührenpflichtig ins Festnetz und zu Handys telefoniert werden. Die Einsparungen zahlen sich vor allem bei Auslandsgesprächen aus. Auch Konferenzschaltungen mit mehreren, oft bis zu 25 Gesprächsteilnehmer:innen sind möglich. Vorsicht ist aber auch hier unbedingt geboten, denn oft ist der Datenschutz bei Gratis-Angeboten sehr umstritten.

Multifunktionale Handys

Neben dem Design werden Funktionen wie z.B. eine Kamera mit hoher Bildauflösung für Benutzer:innen immer wichtiger. Video-Funktion, Datenübertragungsmöglichkeiten wie Bluetooth und integrierter MP3-Player werden häufig ebenso vorausgesetzt wie Office-Funktionen und mobiles Internet. Durch unzählige Programme (Apps), die aus dem Internet heruntergeladen werden können, lassen sich die Möglichkeiten von Smartphones erheblich erweitern.

Passwörter

Durch die vielfältigen Anwendungen steigt auch die Anforderung, die Zugänge zu diesen Anwendungen sicher zu gestalten. Geräte und Online-Konten (E-Mail, Soziale Netzwerke, Bank) sind in der Regel durch Passwörter geschützt. Damit Passwörter sicher sind, sollten sie folgende drei Kriterien erfüllen:

- ⇨ Mindestens 12 Zeichen
- ⇨ Eine Kombination aus Groß- und Kleinbuchstaben, Zahlen und wenn möglich Sonderzeichen.
- ⇨ Für jede Anwendung ein eigenes Passwort

Je länger ein Passwort ist und je mehr Zeichenkombinationen in Frage kommen, desto schwerer ist es zu knacken. Empfohlen werden mindestens 12 Zeichen. Aus den verwendeten Zeichen sollten allerdings keine bloßen Folgen von Buchstaben (abcd...), Ziffern (12345...) oder von Tasten auf einer Tastatur (qwertz...) gebildet werden. Ein gutes Passwort ist nicht in einem Wörterbuch zu finden, es steht auch in keiner direkten Verbindung mit der Anwenderin oder dem Anwender (Namen, Geburtsdaten, Telefonnummern, ...).
Durch Datenlecks großer Unternehmen oder manipulierte E-Mails geraten Passwörter in falsche Hände. Verwendet man unterschiedliche Passwörter für verschiedene Konten können sich Kriminelle in so einem Fall nur in jeweils einen

Account und nicht gleich in mehrere einloggen. Ein Kompromis wären Gruppen von Konten, für die jeweils ein Passwort verwendet wird, z.b. unwichtige Accounts/wichtige Accounts/Spiele-Webseiten/E-Mail Konten.
(Vgl. www.saferinternet.at/faq/datenschutz/wie-sieht-ein-sicheres-passwort-aus und www.saferinternet.at/faq/datenschutz/wie-kann-ich-passwoerter-sicher-aufbewahren)

Von der lange aufrecht erhaltenen Empfehlung, Passwörter regelmäßig zu wechseln, raten Expert:innen mittlerweile ab. Um sich die Passwörter leichter merken zu können und damit einen Wechsel zu erleichtern, hatten viele Nutzer:innen ihre Passwörter zu einfach gestaltet.
(Vgl. www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/sichere-passwoerter-so-gehts-11672)

Um trotz dieser Anforderungen zu einer praktikablen Vorgangsweise zu kommen, gibt es ein paar Hilfestellungen für die Gestaltung von Passwörtern.
Sätze, die einem leicht einfallen, können als Eselsbrücken dienen. Von diesem Sätzen werden dann z.B. alle Anfangsbuchstaben und die Satzzeichen zu einem Passwort zusammengefügt. So wird z.B. auf diese Weise aus „Ein blaues, kleines Pferd liest Kaffeesatz auf dem Ausflugsdampfer.“ zum Passwort: Eb,kPlKadA.
(Vgl. www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/starke-passwoerter-so-gehts-11672)

Oder man wählt vier zufällige Wörter und verbindet diese mit Sonderzeichen oder Zahlen. Z.B. so: „Babybrei$Einhorn$Thomas$Semmel“
(Vgl. www.saferinternet.at/faq/datenschutz/wie-sieht-ein-sicheres-passwort-aus)

Durch die genannten Kriterien entsteht mit der Zeit eine Vielzahl komplexer Passwörter – und diese Fülle ist trotz der eben genannten Hilfestellungen schwer zu merken. Merkhilfen wie Zettel am PC, in der Brieftasche oder am Kalender sind unsicher und damit nicht geeignet. Werden Passwörter-Listen in analoger Form erstellt, sollten diese geheim abgelegt werden. Jene in digitaler Form sollten verschlüsselt werden.
Unterstützung bieten dafür sogenannte Passwort-Manager. Solche Programme, mit denen Passwörter verwaltet und verschlüsselt gespeichert werden können, wurde von der Stiftung Warentest getestet und unter folgendem Link veröffentlicht: www.test.de/Passwort-Manager-im-Test-5231532-0

Davon zu unterscheiden sind Login-Allianzen von großen Anbietern wie Amazon, Google oder Facebook. Diese auch als Single-Sign-On bezeichneten Lösungen bieten an, sich mit den Login-Daten von diesen Anbietern bei anderen Apps und Portalen anzumelden. Dadurch entsteht zum einen das schon erwähnte Problem, dass durch den Verlust eines Passwortes viele Anwendungen zugänglich werden. Zum anderen stellt bei diesem Verfahren auch der Datenschutz ein Problem dar: Die Anbieter eines Single-Sign-On Verfahrens können damit feststellen, wo sich die User:innen sonst noch anmelden.

Weitere Sicherheitsmaßnahmen

Bei vielen Online-Dienstleistern wie z.B. im Bankenbereich wird mittlerweile zusätzlich zum Passwort ein zweiter Weg angeboten bzw. verlangt, um sich zu identifizieren. Diese Zwei-Wege- oder Zwei-Faktor-Authentifizierung gibt es in mehren Varianten. Eine der bekannteren ist eine Kombination aus Passwort und Codes, die per SMS verschickt werden. Als Alternativen zu den SMS-Codes gibt es Sicherheitscodes über eine Codegenerator-App, eine E-Mail an eine hinterlegte E-Mail-Adresse, einen physischen Sicherheitsschlüssel und Sicherheitscodes zum Ausdrucken.
Das Wesen liegt bei all diesen Methoden darin, dass immer beide Sicherheitsmaßnahmen verwendet werden müssen, damit der Zugang gewährt wird. Der Diebstahl eines Passwortes würde also für den Zugang z.B. zum Bankkonto nicht mehr genügen, für die Diebe müsste auch die zweite Maßnahme verfügbar sein.
Das kann allerdings auch für die Eigentümer:in-

nen zu Problemen führen, wenn einer der beiden Wege nicht mehr verfügbar ist (z.B. wenn das Smartphone kaputt ist). Deshalb empfehlen Expert:innen immer mehrere Methoden zur Zwei-Wege-Authentifizierung zu aktivieren: z.B. zusätzlich zu SMS-Codes auch eine Codegenerator-App, E-Mail oder Ausdruck von Codes.
(Vgl. www.saferinternet.at/news-detail/benutzerkonten-doppelt-schuetzen)

Für das Entsperren von Smartphones haben sich neben Passwörtern und PIN auch andere Verfahren etabliert. Vor allem Muster, die einfach nur gewischt werden müssen, erfreuen sich großer Beliebtheit. Mit der Verbindung von neun Punkten ergäbe sich auch ein schwer zu erratendes Muster. Werden allerdings nur vier Punkte verbunden und damit evtl auch noch einfache Buchstaben wie M oder Z gebildet, dann sind diese schon bei der Eingabe leicht zu erkennen. Wenn das Handydisplay nach der Verwendung nicht abgewischt wird, ist das Muster darauf häufig auch im Nachhinein noch sichtbar.

Methoden zum Entsperren, die biometrische Merkmale verwenden, wie Fingerabdruck-Sensoren, und Iris-Scan gelten dagegen als relativ sicher und praktisch.
Im Vergleich dazu funktioniert die Gesichtserkennung z.T. noch nicht zuverlässig. Schwaches Licht, wehende Haare, Sonnenbrillen oder eine Schutzmaske können die Entsperrung verhindern. Viele Selfie-Kameras lassen sich auch noch von Fotos überlisten.
(Vgl. www.verbraucherzentrale.de/wissen/digitale-welt/mobilfunk-und-festnetz/smartphones-sicher-sperren-13788)

Mehr Informationen zum Thema Kontosicherheit bzw. Privatsphäre bei verschiedenen Anwendungen (z.B. WhatsApp, TikTok, Snapchat etc.) sind im Privatsphäre-Leitfaden von Safer-Internet zu finden:
www.saferinternet.at/privatsphaere-leitfaeden

Anmerkungen