MOBILE MEDIEN
NEUE HERAUSFORDERUNGEN

Safer Smartphone

Sicherheit und Schutz für das Handy

Arbeitsmaterial für den Unterricht - Heft 11

klicksafe.de
handysektor

Impressum

Titel:
„Safer Smartphone"
Sicherheit und Schutz für das Handy

Reihentitel:
Mobile Medien – Neue Herausforderungen

AutorInnen:
Stefanie Rack (klicksafe)
Fabian Sauer (Handysektor, mecodia)

Comics:
Katrin Mack

3. aktualisierte Auflage März 2019

Kooperationspartner:
Dieses Material wurde in Zusammenarbeit von klicksafe und Handysektor erstellt.

Herausgeber:
klicksafe ist das deutsche Awareness Centre im CEF Telecom Programm der Europäischen Union. klicksafe wird gemeinsam von der Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz (Koordination) und der Landesanstalt für Medien NRW umgesetzt.

Koordinator klicksafe:
Peter Behrens, LMK

The project is co-funded by the European Union, http://ec.europa.eu/saferinternet

Die alleinige Verantwortung für diese Veröffentlichung liegt beim Autor. Die Europäische Union haftet nicht für die Verwendung der darin enthaltenen Informationen.

Verbindungsbüro Berlin:
LMK/Safer Internet DE/klicksafe
c/o die medienanstalten
Gemeinsame Geschäftsstelle der
Landesmedienanstalten
Friedrichstraße 60, 10117 Berlin

Handysektor ist die unabhängige Anlaufstelle für den digitalen Alltag von Jugendlichen. Die Webseite ist ein gemeinschaftliches Projekt der Landesanstalt für Medien NRW und des Medienpädagogischen Forschungsverbundes Südwest (mpfs). Die Projektleitung hat Florian Beutenmüller (mecodia GmbH) inne.

Verantwortlich im Sinne des Presserechts:
Für klicksafe: Birgit Kimmel
Für Handysektor: Mechthild Appelhoff,
Thomas Rathgeb (mpfs)

Bezugsadressen:
klicksafe
c/o Landeszentrale für Medien und
Kommunikation (LMK) Rheinland-Pfalz
Direktor: Dr. Marc Jan Eumann
Turmstraße 10
67059 Ludwigshafen
Tel.: 0621 5202-271
E-Mail: info@klicksafe.de
URL: www.klicksafe.de

Handysektor
c/o Landesanstalt für Medien NRW
Zollhof 2
40221 Düsseldorf
E-Mail: redaktion@handysektor.de
URL: www.handysektor.de

Hinweis:
Männliche/weibliche Form: Die auf den meisten Seiten verwendete männliche Form impliziert selbstverständlich die weibliche Form. Auf die Verwendung beider Geschlechtsformen wird lediglich mit Blick auf die bessere Lesbarkeit des Textes verzichtet.

Layout und Umschlaggestaltung:
.puntomedien verlag.gmbh, Weinheim
Gestalterische Überarbeitung:
Designgruppe Fanz & Neumayer,
Ludwigshafen + Heidelberg

Lektorat:
Vanessa Buffy

Inhalt

Symbole und ihre Bedeutung:


Information, Tipp oder alternative Vorschläge


Check oder (Selbst-)Test


Zusatzaufgabe/Hausaufgabe


Methode


Link

Das Material ist geeignet für den Einsatz ab Klasse 6.

Einführung

Leben mit Smartphones – Neue Herausfo rderungen

Ein Leben ohne Smartphone ist für viele von uns heute nur noch schwer vorstellbar. Die kleinen Alleskönner begleiten uns auf Schritt und Tritt – sind nicht nur Organisationshelfer, sondern auch Unterhaltungs- und Kommunikationsgeräte. In Schule und Unterricht ist das Smartphone mittlerweile ebenfalls ein Thema – ob in Schulkonferenzen die Diskussion über die Handyordnung oder der gezielte methodische Einsatz der Schülergeräte für den Unterricht: Das Handy fordert uns als Pädagogen in vielerlei Hinsicht heraus.

Immer mehr persönliche Informationen sind auf den Geräten von Kindern und Jugendlichen gespeichert. Telefonnummern, Termine, E-Mails, Kurznachrichten, Fotos – die digitalen Begleiter, wie auch die JIM-Studie zeigt, und die anfallenden Datenmengen werden zunehmend größer. Umso wichtiger ist es, diese auch richtig abzusichern. Jedoch nicht alle Jugendliche haben ausreichend Kenntnis über Datenschutz und Sicherheit.

Wissen Ihre Schüler beispielsweise, dass sie eine Bildschirmsperre nutzen sollen? Oder dass eine Antivirus-App wie beim PC auch das Handy schützen kann – beides gehört heute zum Basisschutz für Smartphones.

Laut DsiN-Sicherheitsindex 2015 wissen deutsche Nutzer zwar einiges über Sicherheitsmaßnahmen, setzen diese aber viel zu selten ein. Dies gilt vor allem für 16-19-Jährige, die Gruppe der sogenannten „fatalistischen Nutzer", die neue Angebote mit jugendlicher Unbedarftheit und Neugierde nutzen. Sie klicken oft unbedacht, laden Apps ungeprüft herunter und gehen mit jedem Trend mit. Gefährlich wird es dann, wenn sie sich selbst für kompetente Mediennutzer halten, es aber de facto nicht sind.

Zudem zeigt eine GfK-Befragung, dass die Deutschen generell zwar besonders sensibel sind, wenn es um den Schutz ihrer persönlichen Daten geht, sie problematische Dienste aber trotzdem nutzen. Wodurch lässt sich dieses Verhalten erklären?

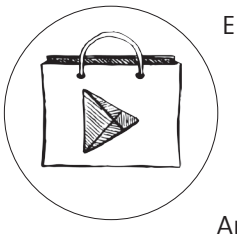
Ein wesentliches Motiv könnte die starke Gewöhnung an den Komfort der digitalen Dienste und Geräte sein, die bis zur Abhängigkeit führen kann. In der Abwägung zwischen den Annehmlichkeiten und den Risiken datensammelnder Apps oder cloudbasierter Lösungen sind offensichtlich sehr viele Nutzer bereit, ein Stück Sicherheit und Datenschutz aufzugeben.

Vielleicht existiert aber auch grundsätzlich ein mangelndes Bewusstsein über die Folgen der digitalen Datenpreisgabe, weil die Thematik zu komplex ist, um sie einer größeren Öffentlichkeit verständlich zu machen.

Ganz nach dem Motto „NSA und Google interessieren sich doch sowieso nicht für mich" gehen viele Nutzer davon aus, dass ihre persönlichen Daten niemandem wichtig genug sind, um gestohlen, ausspioniert oder weiterverkauft zu werden. Die weitgehend einzige Auswirkung von Überwachung und Datensammlung, die bislang erkennbar ist, ist personalisierte Werbung, und diese wird von vielen als nicht störend empfunden. Gerade Jugendliche sehen zudem in der Verknüpfung und ständigen Verfügbarkeit von Daten mehr Chancen als Risiken (Boyd, 2008).

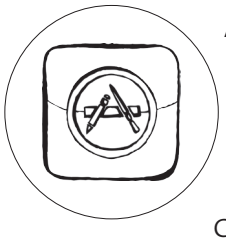
Das Ziel dieser Unterrichtseinheit ist es daher, den Schülern zu vermitteln, dass sie selbst etwas zu ihrer eigenen Smartphone-Sicherheit beitragen können und dies auch lernen sollten, um mündige Mediennutzer zu werden. Dazu erhalten sie einen Einblick in unterschiedliche Gefahrenbereiche der mobilen Mediennutzung und Tipps, wie sie diesen entgegentreten können. Es werden Begriffe definiert und erklärt, deren Kenntnis für eine sichere Nutzung grundlegend sind.

App-gesichert – Wie man Apps und Berechtigungen im Griff behält



Ein neues Smartphone erreicht den Nutzer in den meisten Fällen ausgestattet mit Grundfunktionen wie SMS, E-Mail und Telefonfunktion sowie mit Apps (App ist die Kurzform von englisch application = Anwendung) des Herstellers (Mediatheken, Fitness-Software etc.), die schon vorinstalliert sind. Je nach Gerät sind auch weitere Drittanbieter-Apps, wie Facebook oder Twitter, vorhanden. Ärgerlicherweise können diese in manchen Fällen nicht deinstalliert werden. Alle weiteren Funktionen müssen Nutzer durch Zusatzsoftware selbst nachrüsten, ähnlich wie man das vom Computer schon kennt.

Vorinstallierte Apps loswerden – Wie geht's?
Möchte ich eine vorinstallierte App nicht nutzen, da sie möglicherweise auf persönliche Daten zugreift, so kann sie deaktiviert oder sogar komplett deinstalliert werden. Eine ausführliche Anleitung zum Deaktivieren und Deinstallieren der Anwendungen unter Android liefert Android-PIT: (Abruf: 25.01.2018)
https://www.androidpit.de/vorinstallierte-apps-loeschen-und-deinstallieren



Apps können in der Regel über die digitalen Marktplätze der jeweiligen Handyanbieter her-untergeladen werden. Auf Apple iPhones heißt dieser Marktplatz „App Store", auf Android-Geräten von Google „Play Store". Um sich dort Anwendungen herunterladen zu können, ist ein Benutzerkonto beim jeweiligen Anbieter (Apple oder Google) Voraussetzung, oft auch in Verbindung mit einem Bezahldienst. Dieses Konto wird meist schon bei der Einrichtung des Gerätes angelegt. Bei Android-Geräten ist es zudem möglich, auf alternative App Stores zuzugreifen, die zusätzlich auf dem Handy installiert werden können.

Erklärvideo: Was sind eigentlich App-Berechtigungen?
In einem kurzen Erklärvideo zeigt Handysektor, was es mit Berechtigungen auf sich hat und worauf Nutzer achten müssen.
https://www.youtube.com/watch?v=E59crV5Auvo

Was sind App-Berechtigungen?

Verschiedene Apps bieten verschiedene Möglichkeiten – und benötigen dafür Zugriff auf bestimmte Funktionen des Geräts und damit auch auf Nutzerdaten. So muss eine Fotografie-App auf die Kamera zugreifen können, ein Instant Messenger benötigt Zugang zum Internet und eine App zur Terminverwaltung will Einblick in den Kalender. Welche Zugriffe eine App erhält, wird über die sogenannten Berechtigungen geregelt. Davon gibt es sehr viele – in Android über 160 verschiedene! App-Anbieter können dabei selbst bestimmen, welche Berechtigungen sie für ihre Apps einfordern. Je nach Betriebssystem werden Nutzer dann früher oder später damit konfrontiert.

Ein Freibrief zum Datensammeln?

Manche Berechtigungen wirken auf den ersten Blick fragwürdig und scheinen zum Funktionieren der App nicht unbedingt notwendig zu sein, vor allem vor dem Hintergrund, dass sie „jederzeit" gelten, also auch dann, wenn die App gerade nicht genutzt wird. Eine App mit Zugriff auf Kamera und Mikrofon könnte beides also auch unbemerkt aktivieren und heimlich filmen oder mithören. Da ein sehr großer Teil aller Apps nur mit Zugriff auf das Internet funktioniert, ist die Gefahr von Datenmissbrauch durch die Weiterleitung persönlicher Daten an den App-Hersteller umso größer.

Im Hinblick auf eine sichere Nutzung des Smartphones stellen sich hier folglich zwei Fragen:

1. Warum will der App-Anbieter Zugriff auf Gerätefunktionen und Nutzerdaten?

2. Woran erkenne ich eine seriöse App?

Bei der Beantwortung hilft es, sich Gedanken über die Funktionen einer App zu machen. Als gutes Beispiel bietet sich WhatsApp an, denn kaum eine App will so viele Berechtigungen wie der beliebte Messenger. Ein Blick in die zahlreichen Funktionen der Anwendung schlüsselt jedoch auf, weshalb: Nachrichten werden über das Internet verschickt, und Fotos, Sprachnachrichten oder der eigene Standort können mit anderen Nutzern geteilt werden. Zudem ist es nicht nötig, neue Kontakte hinzuzufügen, da automatisch aus dem Adressbuch des Smartphones ausgelesen wird, welche Kontakte die App ebenfalls nutzen. Hierzu ein Auszug aus den AGB von WhatsApp: *„Du stellst uns regelmäßig die Telefonnummern in deinem Mobiltelefon-Adressbuch zur Verfügung, darunter sowohl die Nummern von Nutzern unserer Dienste als auch die von deinen sonstigen Kontakten. Du bestätigst, dass du autorisiert bist, uns solche Nummern zur Verfügung zu stellen."*
www.whatsapp.com/legal (Abruf: 23.01.17).

Folglich benötigt WhatsApp Zugriff auf Kontakte, das Internet, die Kamera, das Mikrofon, gespeicherte Bilder und Videos sowie den Standort. Zwar lässt sich zum Nutzen der App der Zugriff auf die benötigten Funktionen rechtfertigen – nichtsdestotrotz sollten Apps mit solch weitreichenden Zugriffen immer kritisch betrachtet und hinterfragt werden und alternative Dienste in Betracht gezogen werden.

WhatsApp-Alternativen
Telegram: Telegram bietet eine Ende-zu-Ende-Verschlüsselung (jedoch nicht für Gruppenchats) und ist kostenfrei. Die App kann zusätzlich am Computer verwendet werden.
Threema: Die Kommunikation in Threema ist durch eine Ende-zu-Ende-Verschlüsselung gesichert, die App ist kostenpflichtig (3,49 €).

Berechtigungen – sinnvoll oder problematisch?

Um sinnvoll zu sein, müssen die Berechtigungen zur App passen und für die Funktionen notwendig sein. Gerade größere Hersteller liefern deshalb häufig Begründungen, weswegen sie bestimmte Funktionen benötigen. So schlüsselt Facebook dies detailliert für die Face-book-App (siehe Grafik) und den Messenger auf. Aber auch Berechtigungen, die für die Funktionalität einer App sinnvoll sind, können Sicherheitsrisiken bergen, falls App-Anbieter erhobene Daten über die benötigten Funktionen hinaus nutzen. Daher kann nicht grundsätzlich von „sinnvollen" oder „problematischen" Berechtigungen gesprochen werden. Eine endgültige Sicherheit kann es nie geben. Kritisch sollten Nutzer vor allem bei kostenfreien (und werbefinanzierten) Apps sein. Negativbeispiele finden sich immer wieder bei kostenfreien Spielen. Schwarze Schafe finanzieren sich nicht nur durch Werbung, sondern auch dadurch, dass sie ausgespähte Nutzerdaten (Telefonnummern, Adressen etc.) weiterverkaufen. Selbst eine einfache Taschenlampen-App kam schon in die Kritik, da sie Standortdaten an Werbefirmen weiterleitete.

Android-Genehmigung (was du auf deinem Android siehst)	Beispiele für den Verwendungszweck dieser Genehmigung
Deine Textnachrichten lesen (SMS oder MMS)	Wenn du einem Konto eine Telefonnummer hinzufügst, können wir hiermit automatisch deine Telefonnummer bestätigen, indem wir den Bestätigungscode finden, den wir über eine Textnachricht senden.
Dateien ohne Benachrichtigung herunterladen	Auf diese Weise können wir die Nutzererfahrung in der App verbessern, indem wir Neuigkeiten vorab laden.
Deine Kontakte lesen/schreiben	Mit diesen Berechtigungen kannst du deine Telefonkontakte in Facebook importieren und deine Facebook-Kontakte auf dein Telefon übertragen.
Veranstaltungen im Kalender hinzufügen oder ändern und ohne Wissen des Eigentümers Gästen E-Mails senden	Auf diese Weise kannst du deine Facebook-Veranstaltungen im Kalender deines Telefons sehen.
Veranstaltungen im Kalender sowie vertrauliche Informationen lesen	Auf diese Weise kann die App deine Kalenderverfügbarkeit (basierend auf dem Telefonkalender) anzeigen, wenn du eine Veranstaltung auf Facebook anzeigst.

Facebook-Hilfebereich: *https://www.facebook.com/help/452400401467000/* (Abruf: 25.01.2018)

Die Funktionsweise der Berechtigungen darf also durchaus auch als Geschäft zwischen Nutzer und Anbieter verstanden werden: „Ich gebe Dir Zugriff auf meine Daten und vertraue auf einen seriösen Umgang damit, dafür erhalte ich von Dir eine bestimmte Leistung." Man sollte sich als Nutzer aber immer bewusst machen, dass Anbieter sich in einer Position befinden, in der sie diesen Vertrauensvorschuss missbrauchen könnten.

Lesen Sie mehr zu Korrelation und Weiterverkauf von Daten im klicksafe-Material „Ethik macht klick – Werte-Navi fürs digitale Leben", Baustein „Big Data" *www.klicksafe.de/themen/medienethik/privatsphaere-und-big-data/* (Abruf: 25.01.2018).

Berechtigungen in Android

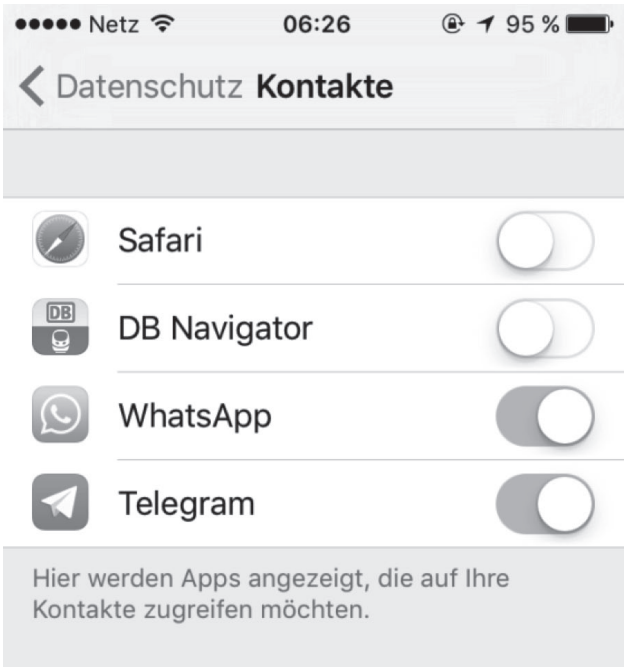
Wer Apps im Google Play Store auf einem Android-Smartphone mit einer älteren Betriebssystem-Version (bis Version 5) herunterlädt, dem wird vor dem Download eine Liste mit allen eingeforderten Berechtigungen angezeigt. Mit der Zustimmung zum Installieren werden auch die Berechtigungen akzeptiert.

Quelle: *www.handysektor.de/apps-upps/appgesichert/berechtigungen.html* (Abruf: 25.01.2018)

Dies geht immer nur im Ganzen, das Auswählen einzelner Berechtigungen ist nicht möglich. Wer also einer App beispielsweise keinen Zugriff auf den Standort geben möchte, kann dies nur tun, indem er die App gar nicht erst installiert. Berechtigungen können seit Version 6 des Betriebssystems einzeln gesteuert werden. Nutzer können in dem Moment, in dem die App zum ersten Mal einen bestimmten Zugriff erhalten will, zustimmen oder ablehnen. Auch einmal gewährte Freigaben können später wieder rückgängig gemacht werden.

Berechtigungen in iOS

Das Apple-Betriebssystem iOS behandelt die Zustimmung zu Berechtigungen schon immer so, wie es die Android-Version 6 macht. Wird eine App geöffnet und will sie dann zum ersten Mal auf eine Funktion oder Daten zugreifen, können Nutzer dem zustimmen oder es ablehnen. Wird der Zugriff verweigert, ist die App logischerweise in ihren Funktionen eingeschränkt. Auch hier lassen sich Berechtigungen im Nachhinein zurücknehmen.



Quelle: *IOS 11.2.1* (Abruf: 25.01.2018)

Mit 6 Tipps zum sicheren App-Download

Beim Herunterladen von Apps gibt es also einiges zu beachten. Und auch bei vermeintlich seriösen Anbietern ist es fast unmöglich herauszufinden, ob sie im Hintergrund wirklich nur das machen, was sie vorgeben. Mit ein paar einfachen Tipps lassen sich Gefahren aber zumindest minimieren:

1. Bestenlisten und Topdownloads sind kein Sicherheitsmerkmal

Apps wie Facebook stehen in den Top 10 der am häufigsten heruntergeladenen Anwendungen meist weit vorne – obwohl sie immer wieder wegen Problemen beim Datenschutz in der Kritik stehen. Dies zeigt deutlich, dass Bestenlisten nicht automatisch ein Anzeichen für sichere oder vertrauenswürdige Apps sind.

2. Nutzerkommentare durchlesen

Top-Downloads sagen nichts über die Sicherheit einer App aus, Nutzerkommentare können jedoch hilfreich sein. Gibt es in den Bewertungen besonders viel Negatives („die App funktioniert nicht richtig", „der Akku wird schnell heiß", „viele Funktionen sind nur durch In-App-Käufe verfügbar" etc.), dann kann man sich eine Installation meist sparen.

3. Alternative App Stores meiden

Neben Google Play können auf Android-Smartphones auch Apps aus alternativen App Stores installiert werden. Dies kann aber zum Problem werden, denn hier gibt es häufig keine Sicherheitsprüfungen der Apps durch die Anbieter der alternativen App-Stores. Google hingegen führt in Google Play eine Sicherheitsprüfung (technische Sicherheit, nicht Datenschutz) von Apps durch. Viren und andere Schadsoftware können also über alternativen App-Stores einfach und unbemerkt auf ein Smartphone gelangen.

4. Nutzungsbedingungen lesen

Die Nutzung ist erst ab 18 Jahren erlaubt? Nach 12 Monaten wird das Angebot kostenpflichtig? Diese und ähnliche Regelungen finden sich für gewöhnlich in den Allgemeinen Geschäftsbedingungen (= AGB), in englischsprachigen Apps häufig auch „Terms Of Service" genannt. In den AGB ist zudem auch geregelt, wie erhobene Nutzerdaten vom Anbieter verwendet werden. Vor dem Download lohnt sich ein Blick in diese Regelungen, um keine bösen Überraschungen zu erleben. Wichtig: Die AGB werden vor dem Download normalerweise nicht automatisch angezeigt, sind aber meist in der Beschreibung der App im App-Store abrufbar. Sollte dies nicht der Fall sein, finden sie sich auf der Webseite des App-Anbieters. Auch wenn das komplette Durchlesen nicht immer hilfreich ist, sollte zumindest auf Mindestalter und Angaben zu Kosten geachtet werden.

5. Berechtigungen beachten

Neben den AGB sind die Berechtigungen die zentrale Möglichkeit, um auf einen Blick zu erfahren, was die App auf dem Smartphone machen darf und welche Daten sie erhält. Berechtigungen sind gerade für junge Nutzer auch einfacher zu verstehen als AGB, da letztere oft mit juristischen Fachbegriffen gespickt sind.
Beim Einschätzen von Berechtigungen von schon installierten Apps hilft die App Clueful (erhältlich für Android), die übersichtlich anzeigt, welche Apps kritischen Zugriff auf persönliche Daten haben. Berechtigungen, die für Funktionen der App nicht benötigt werden, sollten (wenn das System dies erlaubt) deaktiviert werden.

6. App-Updates bedenken

Aktualisierungen von Apps sollten kritisch betrachtet werden, denn sie können positive und negative Folgen haben. Positiv kann eine Aktualisierung sein, wenn die Anbieter dadurch schnell und unkompliziert Sicherheitslücken beseitigen und neue Funktionen hinzufügen können. Negativ hingegen kann sein, dass sie dadurch bei Android-Geräten möglicherweise auch unbemerkt mehr Zugriffe auf Nutzerdaten bekommen. Möglich wird dies, da Berechtigungen bei Android in Gruppen zusammengefasst werden. So gehört zum Zugriff auf SMS sowohl das Auslesen, als auch das Versenden von SMS. Hat ein Nutzer beim Download zugestimmt, dass die App SMS lesen darf, so können die Berechtigungen zum Schreiben und Versenden durch ein Update unbemerkt hinzugefügt werden. Wer automatische App-Updates aktiviert, sollte die Berechtigungen installierter Apps daher regelmäßig prüfen und vorinstallierte Apps, die nicht genutzt werden, deaktivieren (siehe Tippkasten zu Beginn dieses Kapitels).

Fazit: Kommt mir etwas schon vor dem Download komisch vor, dann Finger weg von der App!

Sicheres Smartphone – Wie man sich vor Eindringlingen schützt

Der Schutz vor problematischen Apps ist nur ein erster Schritt zu mehr Sicherheit, denn sie sind bei Weitem nicht die einzige Gefahrenquelle für Smartphones. Wie auch Computer sind Smartphones anfällig für Angriffe durch Schadsoftware. Dies kann zum einen Malware sein. Als Malware bezeichnet man alle Apps, die Nutzer selbst installieren und die dann unbefugt auf Daten zugreifen (z. B. durch zu viele Berechtigungen) oder das Gerät unbenutzbar machen. Zum anderen können aber auch klassische Viren, die allein durch das Aufrufen von Internetseiten, das Anklicken von Links in Kettenbriefen oder auf anderen Wegen auf das Smartphone gelangen, Schaden anrichten. Die optimalen Sicherheitsmaßnahmen sind dabei abhängig vom jeweiligen Betriebssystem.

Sicherheit am iPhone

In iOS ist der Download von Apps lediglich aus dem offiziellen App-Store möglich. Alle dort angebotenen Apps werden von Apple gründlich geprüft, bevor sie zum Download angeboten werden. Daher ist es für Cyberkriminelle fast unmöglich, Malware in Form von Apps auf iPhones einzuschleusen. Doch auch Apples Sicherheitsmaßnahmen konnten schon umgangen werden (Recherche-Stichwort: „App Store China Hack"). Wie im obigen Kapitel beschrieben, ist es für Nutzer trotzdem wichtig, sich genau über die Berechtigungen einer App Gedanken zu machen und Freigaben nur dann zu erteilen, wenn dies nötig ist.

Nur durch den sogenannten Jailbreak können nicht geprüfte Apps auf das iPhone gelangen. Dabei wird eine modifizierte Version des Betriebssystems auf dem Gerät installiert, das weniger Sicherheitsmaßnahmen enthält und dem Nutzer daher erweiterte Funktionen und die Installation von Apps ermöglicht, die sonst nicht für das System verfügbar wären (z. B. erweiterte Chat-Apps oder Sprachübersetzer für Siri). Durch zahlreiche Anleitungsvideos auf YouTube und ähnlichen Plattformen ist es für technikaffine Jugendliche möglich, einen solchen Jailbreak vorzunehmen. Apple warnt ausdrücklich vor Jailbreaks, da dadurch Sicherheitslücken entstehen, die nicht mehr automatisch durch Apple behoben werden können. Zudem können dauerhafte Schäden am Gerät entstehen und die Garantie entfallen

Sicherheit bei Android

Im Gegensatz zu iOS werden Apps bei Android-Geräten vor der Freischaltung im App-Marktplatz Google Play nur rudimentär geprüft. Dadurch finden sich hier viel häufiger problematische Apps. Auch wenn die Berechtigungen hier nicht immer kritisch erscheinen, kann Malware beträchtliche Schäden am Gerät anrichten oder unbemerkt Daten stehlen. Besonders Apps aus alternativen App-Stores stellen eine Sicherheitslücke dar, denn dort findet meist überhaupt keine Sicherheitsprüfung der angebotenen Anwendungen statt. Standardmäßig ist die Installation aus „nicht vertrauenswürdigen Quellen" zwar deaktiviert, jedoch können

Nutzer dies einfach ändern. Davon ist abzuraten, um Sicherheitslücken zu meiden.

Aufgrund dieser Entwicklung bieten viele Hersteller von Sicherheitssoftware auch Sicherheits-Apps für Android an. Die meisten Apps der bekannten Hersteller (Avira, AVG, Bitdefender, Kaspersky, Norton etc.) sind kostenfrei verfügbar und für den normalen Nutzer völlig ausreichend. Viele bieten zudem auch Zusatzfunktionen, z. B. für den Diebstahlschutz. Sicherheits-Apps sollten vor Gebrauch genau geprüft werden, da manche den vollen Funktionsumfang erst in einer kostenpflichtigen Premiumversion anbieten.

Updates

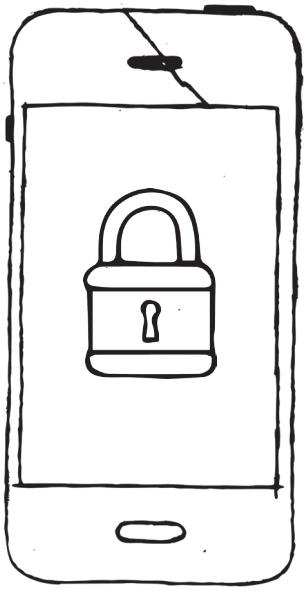
Um bei der Nutzung des Geräts – unabhängig vom Betriebssystem – den notwendigen Schutz zu gewährleisten, sollten Updates sowohl für das System als auch für alle installierten Apps immer möglichst schnell durchgeführt werden. Die meisten Updates schließen nämlich lediglich Sicherheitslücken und sind daher für einen zuverlässigen Gebrauch des Gerätes unerlässlich. Ob Apps automatisch aktualisiert werden, kann in den Einstellungen des Betriebssystems festgelegt werden. Nicht gewünschte, vorinstallierte Apps können hiervon ausgenommen werden, indem man sie deaktiviert (siehe dazu Tippkasten in Kapitel 1). Auch das manuelle Durchführen von Updates ist möglich, damit Nutzer selbst die Kontrolle behalten können. Leider führt das bei vielen aber dazu, dass sie dies vergessen und Updates nie oder nur selten durchführen.

Handy weg! – Was tun bei Diebstahl & Verlust?

Allein im Jahr 2014 wurden nach einer Bitkom-Befragung in Deutschland knapp vier Millionen Smartphones gestohlen oder sind verloren gegangen. Aufgrund all der privaten Daten, die sich auf den Geräten befinden, sind diese Zahlen mehr als beunruhigend. Dabei lassen sich mithilfe von nur wenigen Maßnahmen die meisten damit einhergehenden Probleme beseitigen.

Sicherheit beginnt am Bildschirm

Das erste Einfallstor für Kriminelle ist der Handy-Bildschirm. Daher sollte dieser mit einer Sperre versehen sein. In allen Betriebssystemen kann der Bildschirm mit PIN oder Passwort gesichert werden. Jedoch gilt: Nur ein gutes Passwort und eine lange PIN sind wirklich sicher. Zur Prüfung des eigenen Passworts kann auf Seiten wie *www.CheckDeinPasswort.de* zurückgegriffen werden. Tipps für sichere Passwörter bietet auch klicksafe.



Zudem ermöglichen manche Geräte eine Entsperrung durch Muster-, Gesichts- oder auch Fingerabdruckerkennung. Das Entsperrmuster ist schon deswegen nicht sicher, da der Finger beim Entsperren eine Fettspur auf dem Bildschirm hinterlässt, die von Fremden relativ einfach nachvollzogen werden kann. Auch die Gesichtserkennung ist in aktuellen Geräten noch nicht fortschrittlich genug, um eine sichere Entsperrung zu ermöglichen. Häufig reicht es aus, dem Besitzer des Gerätes ähnlich zu sehen oder eine Abbildung des Besitzers vor die Kamera zu halten. Die Fingerabdruck-Technologie hingegen hat sich als praktische und bequeme neue Möglichkeit etabliert. Es ist nicht mehr nötig, sich ein Passwort zu merken. Die Entsperrung läuft zudem schneller ab. Nichtsdestotrotz sollte bedacht werden, dass dabei sensible biometrische Daten auf dem Gerät gespeichert werden. Ist kein Fingerabdrucksensor vorhanden, sollten Nutzer auf die „klassischen" Möglichkeiten zur Entsperrung (PIN und Passwort) zurückgreifen.

Alles gut verpackt: Verschlüsselung und Backups

Nicht nur über den Bildschirm kann auf die Daten auf dem Smartphone zugegriffen werden. Schließen Diebe ein Datenkabel an das Gerät an, können sie einfach direkt auf viele Daten zugreifen. Daher ist es wichtig, den Speicher des Gerätes zu verschlüsseln. Dies ist bei iPhones und Android-Geräten ab Version 5 schon standardmäßig aktiviert, Besitzer von älteren Android-Smartphones müssen die Einstellung jedoch selbst vornehmen. Zu finden ist die Verschlüsselung unter „Einstellungen" beim Punkt „Sicherheit". Wichtig: Der Akku sollte vollständig aufgeladen sein, bevor der Verschlüsselungsvorgang gestartet wird! Schaltet sich das Gerät währenddessen aufgrund niedriger Akku-Ladung aus, ist kein Zugriff mehr auf das Smartphone möglich.

Nach einem Diebstahl ist nicht nur das Gerät weg, sondern auch die darauf gespeicherten Daten sind verloren. Um sie trotzdem noch nutzen zu können, sollten regelmäßig Sicherheitskopien – sogenannte Backups – erstellt werden. iPhone-Nutzer können dafür auf die iCloud – den Cloudspeicher von Apple – oder eine lokale Sicherung über iTunes zurückgreifen, Besitzer von Android-Geräten können viele Daten direkt über Google absichern. Zudem gibt es für beide Betriebssysteme Apps von Drittanbietern, die eine Datensicherung ermöglichen (beispielsweise Dropbox oder OneDrive). Da es sich dabei hauptsächlich um amerikanische Anbieter handelt, sollte man bei sensiblen Daten eine lokale Speicherung auf der Computerfestplatte in Erwägung ziehen. Jedoch lassen sich auf diesem Wege nicht alle Daten (z.B. Kalendertermine oder Kontaktdaten) unkompliziert und komfortabel sichern.

Zur Datensicherung können Daten-Container wie Truecrypt genutzt werden. Diese lassen sich auch von Schülern unkompliziert nutzen. Wie sie sich einsetzen lassen, zeigt ein Video der Reihe „Einfach erklärt": *https://www.youtube.com/watch?v=IhoG37uis3k* (Abruf: 25.01.2018)

Wenn das Smartphone weg ist: Sicher in drei Schritten

Sollte das Smartphone einmal abhanden gekommen sein, können Nutzer trotzdem immer noch Schutzmaßnahmen ergreifen.

1. Wiederfinden

Die Hersteller bieten über die iCloud (Apple) und den Android-Geräte-Manager (Google) Möglichkeiten an, das Smartphone aus der Ferne wiederzufinden. Diese Funktionen müssen schon vor dem Verlust am Handy aktiviert werden (in den Einstellungen unter dem Menüpunkt „Sicherheit"). Im Verlustfall können sich Nutzer so mit ihren Zugangsdaten an einem anderen Handy oder Computer bei den Diensten anmelden und versuchen, das Gerät orten zu lassen. Sie haben dann die Möglichkeit, ein neues Passwort zur Sperrung zu vergeben oder sogar den Speicher zu löschen. Möglich ist die Ortung allerdings nur, wenn das Gerät gerade angeschaltet ist und entweder über WLAN oder ein mobiles Netz mit dem Internet verbunden ist.

2. SIM-Karte sperren

Um eine Explosion der Handykosten durch teure Anrufe oder Einkäufe von Unbefugten zu verhindern, sollte die SIM-Karte bei erfolglosem Ortungsversuch gesperrt werden. Meist genügt dazu ein Anruf beim Mobilfunkanbieter, oder es gibt eine Möglichkeit zur Sperrung im Online-Kundenportal des Mobilfunkanbieters. In beiden Fällen werden häufig die Kunden-Nummer und weitere Vertragsdaten benötigt.

3. Anzeige erstatten

Bei manchen Mobilfunkanbietern greift eine Haftungsbegrenzung für Kosten, die ein Dieb verursacht, nur dann, wenn der Diebstahl bei der Polizei angezeigt wird. Auch die meisten Handyversicherungen erstatten ein gestohlenes Handy in diesem Fall. Zur Anzeige des Diebstahls wird die IMEI, die individuelle und weltweit einmalige Kennung des Geräts, benötigt. Diese kann über die Kurzwahl *#06# abgerufen werden und sollte schon direkt nach dem Kauf des Smartphones notiert werden.

Infografik „Smartphone sicher“

https://www.handysektor.de/hacker-sicherheit/smartphone-sicher.html

Ausgetrickst – Wie man Kostenfallen ausweicht

Wenn es darum geht, anderen das Geld aus der Tasche zu ziehen, werden nicht nur Kriminelle, sondern auch manche kommerziellen Anbieter sehr kreativ. So ist es kaum verwunderlich, dass es unzählige Arten von Kostenfallen für Smartphones gibt. Nachfolgend findet sich eine Übersicht über die häufigsten Abzocker-Methoden und effektive Gegenmaßnahmen.

Premium-SMS und Mehrwertdienste

Premium-SMS sind Dienste, die über SMS bestellt und abgerechnet werden. Erkennbar an einer fünfstelligen Kurznummer ohne Vorwahl, kosten diese Dienste bis zu 4,99 € pro SMS. Mehrwertdienste (Service- oder Sonderrufnummern) sind an speziellen Vorwahlen (z.B. 0900, 0180, 0137) erkennbar. Angezeigte Kosten beziehen sich meist auf Anrufe aus dem Festnetz, aus Mobilfunknetzen wird es teurer (oft mehrere Euro pro Minute!). Sowohl Premium-SMS als auch Mehrwertdienste kommen häufig bei Gewinnspielen oder für das Downloaden von Logos und Klingeltönen zum Einsatz. Sondernummern können direkt beim Mobilfunkanbieter gesperrt werden (die sogenannte Drittanbietersperre), Premium-SMS sollten nicht genutzt werden. Die Verbraucherzentrale NRW bietet zur Drittanbietersperre einen Musterbrief *https://www.verbraucherzentrale.de/wissen/digitale-welt/mobilfunk-und-festnetz/abzocke-per-smartphone-hilfe-bei-ungewollten-abos-12613* (Abruf: 25.01.2018) zum Download an.

Abofallen

Hinter Bestellungen per Premium-SMS verstecken sich häufig auch Abofallen, die erst nach einem Blick ins Kleingedruckte erkennbar werden. Auch auf Internetseiten finden sich manchmal Abofallen, die hinter vermeintlich kostenfreien Downloads versteckt sind. Müssen zum Download von Software Adressdaten eingegeben werden, so gilt Vorsicht! Wenn Nutzer doch in eine Abofalle geraten, sollten sie offene Rechnungen nicht gleich bezahlen, sondern einen Anwalt aufsuchen oder sich bei der Verbraucherzentrale Hilfe holen. Jugendliche können sich über das Portal *checked4you.de* der Verbraucherzentralen ebenfalls beraten lassen und sollten in jedem Fall ihre Eltern informieren, falls sie in eine Falle getappt sind.

In-App-Käufe

Auch Anbieter von Apps, die auf den ersten Blick kostenfrei sind, haben Wege gefunden, um Geld zu verdienen. Die Optionen reichen von klassischer Werbung bis hin zu In-App-Käufen. Manche Apps setzen auf das sogenannte „Premium"-Prinzip: Die kostenfreie App ist hier lediglich der Türöffner, und der komplette Funktionsumfang einer App kann erst mit einem kostenpflichtigen Update genutzt werden. Gerade Anbieter von Spielen setzen auf den Verkauf von Zusatzfunktionen und haben dabei speziell die junge Zielgruppe im Blick. Für Kleinstbeträge (meist unter einem Euro) erhalten die Spieler Zusatzkomponenten oder mehr Ressourcen und haben so beim Spielen womöglich mehr Erfolg. Auch diese kleinen Beträge können sich schnell summieren. In-App-Käufe sollten daher im System gesperrt werden. Bei iOS ist eine komplette Sperrung möglich. Bei Android können In-App-Käufe zumindest per Passwort blockiert werden (konkrete Tipps auf *http://www.klicksafe.de/smartphones/.)*

Was passiert mit den gesammelten Daten?

Bei vielen Apps ist die Nutzung der jeweiligen Berechtigungen sinnvoll, z. B. die Ortung für Navigation oder Stauerkennung. Natürlich können diese sensiblen Daten aber auch missbraucht werden. Über den Aufenthaltsort können Rückschlüsse über den Wohnort, die Schule, den Arbeitsplatz und das Freizeitverhalten ermittelt werden – und das unbemerkt und ohne aktives Teilen von Informationen durch den Nutzer. Die gesammelten Daten sind also besonders attraktiv für Werbetreibende, die sich für die Gewohnheiten ihrer Zielgruppen interessieren.

Wie kann die Ortung verhindert werden?

Bei Smartphones mit iOS-Betriebssystem kann der Zugriff auf den Standort für jede App einzeln freigegeben werden. Möglich ist dies in den Einstellungen unter „Datenschutz" und „Ortungsdienste". In Android ist eine solch detaillierte Freigabe erst ab Version Android 6 möglich (mehr zur Einstellung von Berechtigungen im vorherigen Kapitel). In älteren Versionen kann der Zugriff auf den Standort in den Einstellungen nur komplett (de)aktiviert werden.

Bewegungsprofil – Wie man unbemerkte Ortung verhindert

Der Zugriff von Apps auf den Standort ist eine der am häufigsten geforderten Berechtigungen. Viele benötigen sie zur Bereitstellung bestimmter Funktionen, manche jedoch missbrauchen sie zur Erstellung von Bewegungsprofilen. Dazu werden viele Aufenthaltspunkte des Smartphones verknüpft und zu einem Profil zusammengefasst. Technisch möglich wird dies aufgrund der Tatsache, dass moderne Smartphones mit einer Vielzahl von Sensoren ausgestattet sind. Damit kann das Gerät bis auf mehrere Kilometer (über das Mobilfunknetz) oder sogar wenige Meter (mit WLAN oder GPS) geortet werden.

Handysektor-Erklärvideo:
„Was ist eigentlich ein Bewegungsprofil"

Quelle: *www.handysektor.de/mediathek/videos/erklaervideo-bewegungsprofil.html* (Abruf: 25.01.2018).

Cloud – Wie man Informationen in der Daten-Wolke sicher speichert

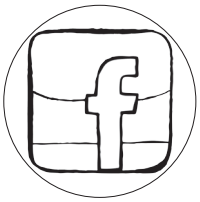
Wie der Begriff „Internet“ schon verrät: die digitale Welt ist eine vernetzte Welt. Alle Computer, Smartphones, Server stehen miteinander in Verbindung und tauschen Daten aus. Dazu gehören auch die Server und Datenspeicher, die das Rückgrat des Internets bilden. Diese stehen auf der ganzen Welt verteilt, meist in großen Datenzentren. Der genaue Aufbau dieser Verbindungen ist allerdings für den „einfachen“ Nutzer nicht sichtbar und wirkt wie von einer Wolke verschleiert. Daher hat sich als Überbegriff für diese Server, Webdienste und Angebote das Wort „Cloud“ (engl. Wolke) etabliert.

Die Cloud ist mehr als nur ein Speicher

Zu Beginn des Cloud-Zeitalters um das Jahr 2007 (Start von Dropbox und Google Docs) wurden damit vor allem Speicherdienste assoziiert, die so etwas wie eine externe Festplatte im Internet anbieten. Zu den bekannten Vertretern gehören unter anderen Dropbox, Google Drive oder OneDrive. Auf ihnen lassen sich Daten ähnlich wie auf einer Festplatte ablegen. Der Vorteil: Der Zugriff auf die Dienste erfolgt per Nutzername und Passwort und man ist daher nicht mehr an ein einziges Endgerät gebunden. Daten können so am PC verarbeitet, dann in den Cloud-Speicher geladen und an einem anderen Computer oder am Smartphone wieder geöffnet werden – und das völlig automatisch und ohne, dass die Geräte direkt, z.B. über ein Kabel, miteinander verbunden sind. Zudem können die online gespeicherten Daten sehr einfach mit anderen Nutzern ausgetauscht werden, was beispielsweise kollaboratives Arbeiten oder das Austauschen von Urlaubsfotos erleichtert.

Heutzutage wird der Begriff Cloud viel weiter gefasst und geht über das reine Speichern von Daten hinaus. Auch komplexe Software wird mittlerweile in der Cloud angeboten. Die Bandbreite reicht von Office-Programmen (z.B. Google Docs und Google Tabellen, Microsoft Office Online) bis hin zu komplexer Bildbearbeitung (z.B. Photoshop Express Editor). Auch hier liegt der Hauptvorteil darin, dass auf die Dienste und die darin gespeicherten Daten (z.B. Textdokumente) von fast jedem internetfähigen Gerät zugegriffen und somit auch gemeinsam an Dokumenten gearbeitet werden kann. Das Installieren von Software auf einem Computer wird damit teilweise überflüssig.

Apps als Tor in die Cloud



Doch tatsächlich sind mittlerweile auch fast alle auf Computern oder Smartphones installierten Apps mit Cloud-Diensten verbunden. Am eindrucksvollsten zeigt sich das, wenn am Smartphone der Flugmodus aktiviert wird. Fast jede App, die dann nicht mehr funktioniert (da sie keinen Internetzugriff mehr hat), greift auf irgendeine Form von Cloud-Dienst zurück. Die meisten Smartphone-Apps sind also nicht viel mehr als das Tor zu einem Cloud-Angebot. Dazu gehören natürlich auch soziale Medien wie Facebook, Instagram oder Snapchat, die ebenfalls darauf setzen, dass wir unsere privaten Daten ihren Internetspeichern anvertrauen. In vielen Webdiensten und Apps hat man heute die Möglichkeit, statt einer Registrierung das Prinzip „Single Sign-On“ (SSO) zu nutzen. Dabei können Nutzer ihre Login-Daten für Facebook, Google oder Twitter einsetzen, um diesen Dienst zu nutzen. Dies ist aus verschiedenen Gründen problematisch: Meldet man sich bei einem der SSO-Anbieter ab, kann man alle damit verknüpften Profile nicht mehr nutzen. Außerdem darf nicht vergessen werden, dass der SSO-Anbieter durch die Verknüpfung der Profile Einsicht in das Nutzungsverhalten hat.

Bei diesen unterschiedlichen und unübersichtlichen Angeboten von Speichern über Software bis zu Social Media haben alle Cloud-Dienste eindeutige Charakteristika: In ihnen können Informationen online gespeichert, mit anderen geteilt und von überall auf der Welt geräteunabhängig abgerufen werden. Auf jedes Cloud-Angebot trifft mindestens eines, meist sogar mehrere dieser Merkmale zu.

Wo genau liegen meine Daten?

Obwohl die Server, die das Internet bilden, über den ganzen Globus verteilt sind, stehen die meisten in Rechenzentren von nur einigen wenigen Unternehmen. Viele große Anbieter von Cloud-Diensten nutzen deren Infrastruktur. So liegen die Daten von Dropbox oder Instagram etwa auf Servern von Amazon. Was kaum jemand weiß: Obwohl Amazon hauptsächlich als Webshop bekannt ist, ist das Unternehmen zudem einer der größten Serveranbieter der Welt!

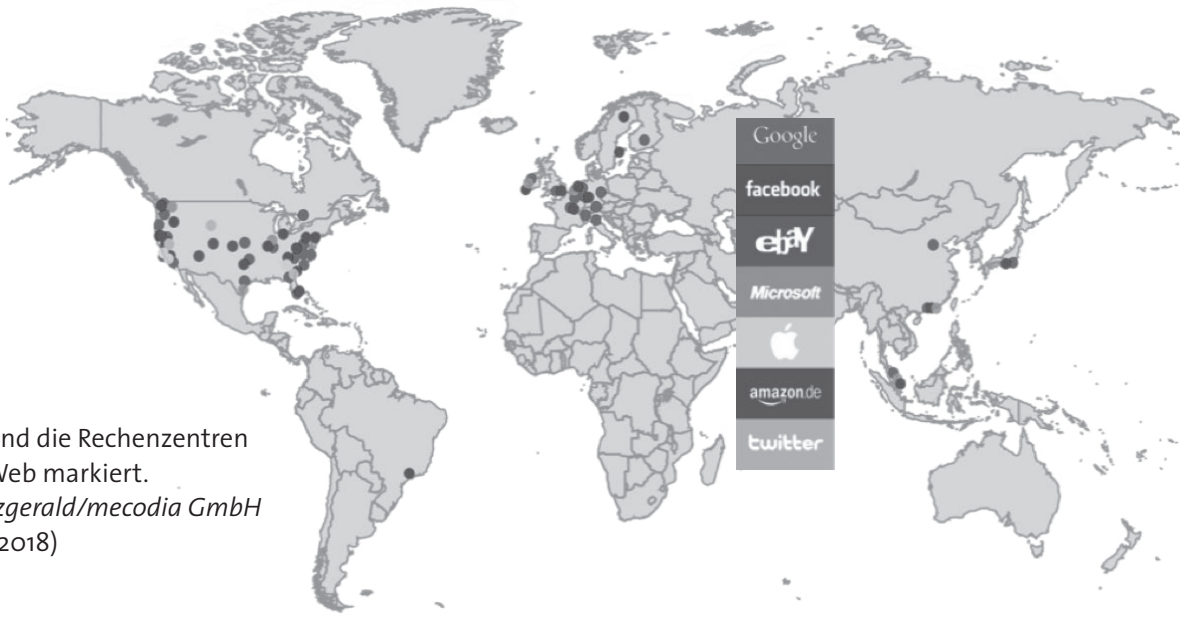
Selbst wenn in Europa – auch in Deutschland – einige Rechenzentren existieren, z.B. von Amazon, Microsoft, Google oder Facebook, heißt das nicht, dass alle Daten von deutschen Nutzern auch auf diesen Servern gespeichert werden. Der größte Teil der Daten wird noch immer in den USA abgelegt und verarbeitet. Vor allem im Hinblick auf den NSA-Skandal ist das durchaus bemerkenswert.

Wie steht es um die Sicherheit von Cloud-Diensten?

Unabhängig von dem Land, in dem sich Daten befinden, können Anbieter einige Sicherheitsmaßnahmen ergreifen. Die wichtigste ist die Verschlüsselung. Liegen die Daten unverschlüsselt auf den Servern, kann jeder mit Zugang zum Speicher alle Informationen auslesen – also auch Hacker, die sich Eintritt zum System verschaffen. Sind sie allerdings verschlüsselt abgespeichert, können nur autorisierte Nutzer mit den entsprechenden Zugangsdaten auf die Daten zugreifen. Cyberkriminelle oder Geheimdienste haben dann keine Möglichkeit, die Informationen auszuwerten – für sie sind diese Daten reinstes Kauderwelsch. Dies ist jedoch nur der erste Schritt.

Wie im Umschlag: Verschlüsselte Datenübertragung

Sind Daten nur auf dem Speicher und nicht auf dem Weg dorthin verschlüsselt, besteht kein vollständiger Schutz. Deshalb ist es wichtig, auch den Übertragungsweg vom Endgerät des Nutzers bis zum Server zu verschlüsseln. Dies ist vergleichbar mit dem Unterschied zwischen einem Brief und einer Postkarte. Ein Brief ist sicher verpackt und kann nur vom Adressaten gelesen werden. Eine Postkarte hingegen ist auch während der Übersendung für alle zugänglich, und auf dem Weg zum Empfänger kann jeder einen Blick auf den Inhalt werfen. Beim Teilen von Daten mit anderen Menschen besteht im besten Fall sogar eine Ende-zu-Ende-Verschlüsselung. Das bedeutet, dass nur die Endnutzer mit ihren Zugangsdaten auf die Inhalte zugreifen können. Selbst für den Anbieter des Dienstes ist das Ausspähen dann unmöglich, da ihm der richtige „Schlüssel“ fehlt.



Auf der Karte sind die Rechenzentren der „Big 7“ im Web markiert.
Quelle: *Peterfitzgerald/mecodia GmbH* (Abruf: August 2018)

Sichere Übertragung prüfen

Ob Daten im Netz sicher übertragen werden, lässt sich bei Webseiten recht einfach ermitteln. Steht bei der aufgerufenen Internetadresse zu Beginn nicht nur „http“, sondern „https“, so steht dies für eine verschlüsselte Verbindung. Nicht ganz so einfach ist es bei Apps. Dort hilft meist nur eine Recherche über den Anbieter, um die Frage der Verschlüsselung zu klären. Offen bleibt in jedem Fall, ob die Daten auch auf den Servern der Anbieter sicher gespeichert werden. Es gibt einige Anbieter von Datenspeichern (z.B. Spideroak) oder Messengern (z.B. Signal, Telegram), die explizit damit werben, den Nutzern eine sichere und gut verschlüsselte Übertragung und Speicherung ihrer Daten zu bieten. Eine wirkliche Möglichkeit, dies nachzuprüfen, haben Nutzer faktisch nicht.

Der Weg der Daten

Die Datenschutzregeln innerhalb Deutschlands und der EU zählen zu den strengsten der Welt. Doch selbst, wenn ein deutsches Cloud-Angebot genutzt wird, ist die Verschlüsselung wichtig. Denn der genaue Weg, den Daten durch das Internet bis zu ihrem Ziel nehmen, ist kaum nachvollziehbar. Selbst beim Zugriff auf ein deutsches Angebot können Informationen um die halbe Welt geleitet werden. Egal ob WhatsApp, Skype oder Bild.de – der Weg der Daten ist immer international. Besonders eindrucksvoll zeigen das die Seiten:
https://apps.opendatacity.de/prism

Das Problem mit dem gekündigten „Mietvertrag“

Bei der Nutzung von Cloud-Diensten begeben sich Nutzer in eine bisher ungekannte Abhängigkeit. Gibt es technische Probleme oder Datenverluste beim Anbieter, sind wichtige Dokumente oder die Urlaubsfotos möglicherweise für immer verloren, es sei denn, es gibt eine Sicherheitskopie auf dem lokalen Computer – aber genau die wollte man sich ja durch die Nutzung von Cloud-Diensten ersparen!

Was ist Streaming?

Die sogenannten Streaming-Dienste sind eine neue Form der Cloud-Nutzung. Bei diesen Anbietern werden Inhalte nur „gestreamt“, d.h. sie liegen nur im Zwischenspeicher des Gerätes. Wie beim Video-dienst YouTube können diese Dienste also nur noch mit Internetverbindung genossen werden. Die große Verbreitung von Streaming-Angeboten hängt stark mit dem Ausbau von Breitbandinternet und mobilem Internet mit hohen Datenraten zusammen, da diese das ruckelfreie Übertragen von Multimediainhalten erst ermöglichen.

Ähnlich problematisch wie bei Cloud-Speichern kann es bei der Nutzung von Streaming-Diensten verlaufen. Wird also die lokale DVD- oder CD-Sammlung durch das Monatsabo für Filme und Serien bei Netflix oder Musik bei Spotify ersetzt, so sind alle Inhalte dort nur „gemietet“. Meistens liegt keine lokale Kopie mehr vor, und wenn doch, kann sie nur innerhalb des Dienstes genutzt werden. Immer wieder kommt es vor, dass die Anbieter Lizenzen nicht verlängern oder Musiker ihre Musik aus den Streaming-Diensten zurückziehen. Es kann also durchaus vorkommen, dass die Lieblingsserie oder der Lieblingsmusiker von heute auf morgen aus dem Angebot verschwinden.

Die Cloud sicher nutzen – und gute Alternativen finden

Auch wenn absolute Sicherheit unmöglich scheint, haben Nutzer trotzdem einige Möglichkeiten, ihre Daten in der Welt der Cloud besser zu schützen.

1. Deutsche Anbieter vorziehen
Gegen Dropbox und Co. ist grundsätzlich nichts einzuwenden. Nutzer sollten sich aber vor der Nutzung darüber informieren, ob die Daten beim gewählten Dienst sicher und gut verschlüsselt übertragen und gelagert werden. Wenn möglich, sollten sie (vor allem bei sensibleren Daten) auf deutsche Anbieter zurückgreifen. Diese sind gesetzlich an Sorgfalts-, Auskunfts-, und Löschpflichten gebunden und müssen Nutzerdaten daher sorgfältiger behandeln, als dies z.B. bei amerikanischen Diensten der Fall ist.

2. Automatischen Upload deaktivieren
Viele Kamera- und Cloudspeicher-Apps bieten einen automatischen Upload von Fotos oder Dokumenten direkt vom Smartphone. Diese Funktion sollte deaktiviert werden. Besser ist es, jede Datei einzeln auf ihre „Cloud-Tauglichkeit" hin zu prüfen.

3. Kritische private Daten nur offline speichern
Besonders kritische Daten wie intime Fotos oder geheime Dokumente sollten grundsätzlich nur offline gespeichert werden – hier geht Sicherheit vor. Eine lokale Sicherheitskopie auf einer externen Festplatte beugt zudem Datenverlusten in der Cloud vor.

4. Passwortschutz nicht vergessen
Und wie immer gilt: Nichts geht über ein sicheres Passwort! Keine noch so gute Verschlüsselung hilft, wenn der Zugang zum Cloud-Dienst mit einem schwachen Passwort gesichert ist.

Die eigene Cloud in der Schule

„Tech-Nerds" bauen sich zu Hause einen eigenen Server und nutzen dafür Software wie ownCloud *http://owncloud.org*. Mit der Software lässt sich mit einigem technischen Know-how und der passenden Hardware eine eigene Cloud erstellen. Dies bietet sich auch als Projekt für den Informatik-Unterricht oder eine Internet-AG an.

Zukunftsvisionen – Wohin geht der Weg?

Auch wenn die Rolle der Cloud in Zukunft weiter zunehmen wird, ist sie für den meisten Deutschen aktuell noch nicht besonders wichtig. Nur 11% aller 15- bis 19-Jährigen halten Cloud-Dienste nach einer Umfrage der GfK aktuell für unverzichtbar. Das mag aber auch daran liegen, dass viele Cloud-Dienste für den Nutzer unbemerkt im Hintergrund ablaufen. Schon in naher Zukunft werden sie für die meisten Internet- und Smartphone-Nutzer folglich immer wichtiger werden, und die Bedeutung von lokalen Datenspeichern wird abnehmen.

Eine logische Weiterentwicklung zeichnet sich aktuell schon ab: Mit dem Nextbit Robin ist das erste Smartphone auf dem Markt, das fast komplett auf lokalen Speicher verzichtet, Daten und Apps befinden sich fast ausschließlich in der Cloud. Die Schlussfolgerung: Ohne Internetzugang funktioniert nichts mehr. Smartphones, Computer und Tablets degenerieren zunehmend zu Bildschirmen mit Internetanbindung, Berechnung und Speicherung finden nur noch online statt, und Nutzer sind mehr und mehr den Anbietern ausgeliefert. Auch das „Internet der Dinge" (engl. IoT = Internet of Things) wird uns in Zukunft beschäftigen. Fast jedes elektronische Gerät kann an das Netz angeschlossen und mit neuen Funktionen ausgestattet werden – auch im Klassenzimmer. Die mit all diesen Entwicklungen einhergehenden Herausforderungen der sicheren Datenübertragung und -speicherung sowie die offensichtlichen Datenschutzprobleme werden uns zukünftig verstärkt beschäftigen. Gehen wir mit dem rasanten Fortschritt, oder treten wir einen Schritt zurück und betrachten alles aus der Distanz? Und haben wir überhaupt noch eine Wahl? Auch diese Fragen sollten wir mit den Schülern reflektieren.

Links und weiterführende Informationen

Materialien:

- Always on – Arbeitsmaterial für den Unterricht Heft 1 aus der Reihe „Mobile Medien – Neue Herausforderungen“ *www.klicksafe.de/AlwaysOn*
- Smart mobil – Ein Elternratgeber zu Handys, Apps und mobilen Netzen *www.klicksafe.de/service/materialien/broschueren-ratgeber/smart-mobil-elternratgeber-handys-smartphones-mobile-netze/s/smart/mobil*

Webseiten:

- CheckDeinPasswort *https://checkdeinpasswort.de*
- klicksafe informiert über Passwörter *www.klicksafe.de/themen/datenschutz/privatsphaere/wie-sollte-ein-sicheres-passwort-aussehen/*
- Handysektor Infografik „Smartphone sicher“ *https://www.handysektor.de/hacker-sicherheit/smartphone-sicher.html*

Literaturverzeichnis

- Bitkom - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (05. August 2015). Was tun bei Handy-Verlust?. Von Bitkom *https://www.bitkom.org/Presse/Presseinformation/Was-tun-bei-Handy-Verlust.html* (Abruf: 25.01.2018).
- Boyd, Danah (2008): Taken Out of Context: American Teen Sociality in Networked Publics. Dissertation, University of California, Berkeley. Von Danah *www.danah.org/papers/TakenOutOfContext.pdf* (Abruf: 25.01.2018).
- Deutschland sicher im Netz e.V. (2015). DsiN-Sicherheitsindex 2015 | Digitale Sicherheitslage der Verbraucher in Deutschland. Von DsiN *https://www.sicher-im-netz.de/sites/default/files/download/2015_dsin_verbraucher-index-studie_web.pdf* (Abruf: 25.01.2018).
- Die Welt (06. Dezember 2013). Taschenlampen-App spioniert Handynutzer aus. Von Welt.de *http://www.welt.de/wirtschaft/webwelt/article122654943/Taschenlampen-App-spioniert-Handynutzer-aus.html* (Abruf: 25.01.2018).
- GfK (30. Juli 2015). Cloud? Kein Muss für Deutsche. Von GfK *http://www.gfk.com/es-ar/insights/press-release/cloud-kein-muss-fuer-deutsche/* (Abruf: 25.01.2018).
- Herrmann, E. (23. Juli 2015). Diese Apps kommen ohne Werbung oder absurde Zusatzbe-rechtigungen aus. Von AndroidPIT *https://www.androidpit.de/kostenlose-apps-ohne-werbung-oder-zusatzberechtigungen* (Abruf: 25.01.2018).
- Kling, B. (19. September 2015). Dutzende iOS-Apps mit Malware XcodeGhost verseucht. Von ZDNet *http://www.zdnet.de/88246866/dutzende-ios-apps-mit-malware-xcodeghost-verseucht/* (Abruf: 25.01.2018).
- Kremp, M. (18. Februar 2016). Nextbit Robin im Test: Geister-Apps aus der Datenwolke. Von SPON *http://www.spiegel.de/netzwelt/gadgets/nextbit-robin-im-test-dieses-smartphone-hat-den-wolkenspeicher-a-1077571.html* (Abruf: 25.01.2018).
- Tanriverdi, H. (9. Februar 2015). Samsung hört mit – aber nur manchmal. Von SZ.de *http://www.sueddeutsche.de/digital/aufregung-um-spracherkennung-samsung-hoert-mit-aber-nur-manchmal-1.2341288* (Abruf: 25.01.2018).

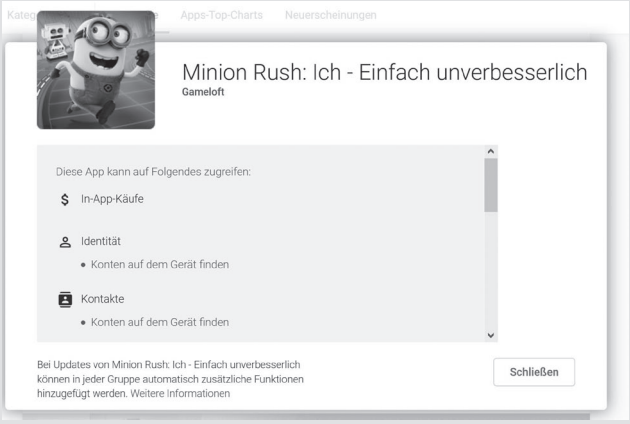
Projekt	1	2	3
Titel	Standort, Mikro, Kamera... ??? Durchblick bei Berechtigungen	Smartphone – aber sicher! Der Smartphone-Führerschein	Daten in den Wolken
Ziele	Die SuS können App-Berechtigungen einschätzen.	Die SuS lernen Sicherheitseinstellungen und andere Funktionen ihres Handys kennen.	Die SuS erkennen, welche Vor- und Nachteile mit der Speicherung von Daten in der Cloud verbunden sind.
Zeit	60 min.	120 min., pro Station ca. 10 min.	45 min.
Methoden	Memory, Beurteilung, Test Berechtigungen von Lieblings-Apps	Stationenarbeit	Sammlung Pro & Kontra (Tafelbild), Tipps gestalten, Recherche
Material	Video App-Berechtigungen (02:54), Screenshots, Memory-Kärtchen, Beamer, App Clueful	Smartphoneführerscheine kopieren, Laufzettel, Stationenbeschreibungen ausdrucken, Schülerhandys	Video Cloud (03:16), Kopiervorlage Wolke
Zugang Internet/PC	Nein (Video App Berechtigungen downloaden)	Ja (PC Raum). Handys u. Kopfhörer sollen explizit in den Unterricht mitgebracht werden. Wenn möglich Wlan für Handys aktivieren.	Nein (Video downloaden)

Standort, Mikro, Kamera… ??? Durchblick bei Berechtigungen

Projekt 1	***Ziele***	*Die SuS können App-Berechtigungen einschätzen.*
	Zeit	*60 min.*
	Methoden	*Memory, Beurteilung, Test Berechtigungen von Lieblings-Apps*
	Material	*Video App-Berechtigungen (2,54 min.), Screenshots, Memory Kärtchen, Beamer, App Clueful*
	Zugang Internet/PC	*Nein (Video „Berechtigungen" downloaden)*

Einstieg

Zeigen Sie das Handysektor-Erklärvideo „Berechtigungen" auf *http://bit.ly/1SoI2qP* und stellen Sie die Frage: *Wozu sind bei Apps Berechtigungen nötig? Berechtigungen, die auf Standort, Kontakte, Bilder etc. zugreifen, sind bei einer App einerseits zum Funktionieren notwendig, andererseits gibt es – vor allem bei kostenlosen Apps – Zugriffe, die dafür nicht nötig wären. Dann wird vor allem darauf abgezielt, Daten zu sammeln und zu verkaufen.*



Quelle: *https://play.google.com/store/apps/* (Abruf: 25.01.2018)

Zeigen Sie anhand einer bei SuS beliebten App im Google Playstore die geforderten Berechtigungen: *https://play.google.com/store/apps*
Anleitung Berechtigungen überprüfen bei iOS und Android unter *www.handysektor.de/apps-upps/appgesichert/berechtigungen.html*

Bei dem neuen Betriebssystem Android 6 und bei iOS (bereits bei älteren Versionen) kann man gezielt einzelne Berechtigungen erteilen. Weisen Sie die SuS darauf hin! Screenshots aus den Stores und Betriebssystemen zum Präsentieren finden Sie unter *www.klicksafe.de/mobilemedien*

Erarbeitung

Berechtigungen sind häufig in großen Gruppen zusammengefasst und schwammig formuliert. Um die Bedeutung von Berechtigungen besser verstehen zu können, sollen die SuS in einem Memory Berechtigungen mit der jeweiligen Erklärung zusammenbringen – oder Sie zeigen die Kopiervorlage im Anhang über den Beamer.

Methode Memory: Empfehlenswert ist die Arbeit in Vierergruppen. Kopieren Sie dazu die Kopiervorlage „Memory-Kärtchen" in entsprechender Anzahl. Die SuS schneiden die Kärtchen aus und legen sie auf dem Tisch aus. Sie können auch die vereinfachte Variante spielen, d.h. Kärtchen offen liegen lassen und nicht – wie beim Memory üblich – verdeckt. In Gemeinschaftsarbeit finden die SuS die zusammengehörigen Paare. Zeigen Sie zur Auflösung die Kopiervorlage „Memory-Kärtchen" via Beamer oder OHP.

Einschätzung	Teilen Sie das Arbeitsblatt aus. Die SuS entscheiden bei vier Apps, ob sie diese auf Grundlage der geforderten Berechtigungen herunterladen würden oder nicht, und begründen ihre Entscheidung. Die Apps sowie ihre Berechtigungen sind zwar frei erfunden, orientieren sich aber an realen, von Jugendlichen häufig verwendeten Apps aus verschiedenen Nutzungskategorien (Messenger, Spiele etc.). Vielleicht müssen Sie bei den Berechtigungen In-App-Käufe erklären > *www.handysektor.de/lexikon.html* Auswertung am Platz. • **App Swarmy:** OK/Nein > Wenn man die In-App-Käufe an seinem Gerät bzw. im Store deaktiviert, kann diese App genutzt werden. • **App Soundo:** OK/Nein > Eine Musik-App mit diesen Funktionen benötigt die meisten Berechtigungen zum Funktionieren. Der Zugriff auf die Kontaktdaten dient zwar zur Verbindung mit den Freunden, ist aber wegen der Weitergabe von Kontaktinformationen an Dritte als problematisch einzustufen und für das Funktionieren nicht notwendig. • **App WConnect:** OK > Eine Messenger-App mit diesen Funktionen benötigt alle Berechtigungen zum Funktionieren. In fast allen Messengern kann man den Standort mit anderen teilen, insofern ist es nicht außergewöhnlich, den Zugriff zu erteilen. Man sollte aber, wenn es die Möglichkeit gibt, die Ortung ausschalten (in den Einstellungen des Handys Ortung deaktivieren oder, wenn möglich, für betreffende App ausschalten). • **App Style Checkas:** Nein > Diese App sollte man nicht installieren, da sie die Berechtigung für zu viele Zugriffe verlangt, die für das Funktionieren nicht nötig sind.
Sicherung	Die SuS formulieren am Ende der Einheit mündlich oder an der Tafel gemeinsam Tipps, wie man bei App-Berechtigungen die Kontrolle behalten kann. Sie können die folgenden Tipps übernehmen.

TIPP: Wie behalte ich die Kontrolle über Berechtigungen?

1. Zugriffe mithilfe des Betriebssystems einschränken (bei iOS oder bei Android 6)
2. Schon vor dem Download Entscheidung treffen:
   Welche Apps brauche ich wirklich?
3. Alternative Dienste nutzen, die auf weniger Daten zugreifen.
   Informationen dazu einholen.
4. Apps ausmisten. Nicht mehr verwendete Apps löschen, denn Apps greifen auch dann noch auf Daten zu, wenn sie nicht mehr aktiv genutzt werden (siehe AB App-Ausmistaktion).

Hausaufgabe/Zusatzaufgabe:

Die SuS überprüfen ihre drei Lieblings-Apps auf dem eigenen Handy auf deren Zugriffsberechtigungen. Bei der Einschätzung kann ihnen die App Clueful helfen, die Apps aufgrund von deren Berechtigungen einschätzt (App nur für Android erhältlich).

Kopiervorlage Berechtigungen Memory-Kärtchen

Berechtigung	Erklärung
Körpersensoren	Manche Smartphones verfügen über Sensoren, mit denen z. B. der Puls gemessen werden kann. Darauf wollen vor allem Fitness-Apps zugreifen.
Kalender	Durch den Zugriff auf den Kalender können Apps während Terminen das Handy stumm schalten oder Geburtstage aus Sozialen Netzwerken als Termin anlegen.
Kamera	Viele Apps, die Fotos machen, QR-Codes einlesen oder das LED-Licht als Taschenlampe nutzen, benötigen dafür diese Freigabe.
Kontakte	Viele Apps nutzen diese Zugriffe, um Kontaktdaten abzugleichen, z. B. WhatsApp.
Standort	Über den Standort können Apps ermitteln und teilen, wo sich ein Nutzer gerade befindet, z.B. in Sozialen Netzwerken. Außerdem kann die Berechtigung für Navigation genutzt werden.
Mikrofon	Diese Berechtigung benötigen alle Apps, mit denen man Geräusche aufnehmen kann, z. B. WhatsApp für Sprachnachrichten.
Telefon	Mit manchen Apps, die Zugriff auf das Telefon haben, können Nutzer direkt einen Anruf starten. Systemreiniger-Apps können mit dieser Berechtigung die Anrufliste löschen.
SMS	Mit Zugriff auf SMS können Apps Kurznachrichten senden und auslesen. Das nutzen alternative SMS-Apps oder Apps für Bestätigungscodes, z.B. WhatsApp.
Speicher	Komplexe Spiele, Galerie- oder Musik-Apps können mithilfe dieser Berechtigung Daten auf einem externen Speicher (Speicherkarte) abspeichern.

Quelle: *Berechtigungen Google Play Store (Stand 25.01.2018). Erklärung: Handysektor*

Standort, Mikro, Kamera… ??? Durchblick bei Berechtigungen

Durch BERECHTIGUNGEN erlaubst du dem Anbieter einer App schon beim Download den Zugriff auf Informationen und Funktionen auf deinem Handy (z.B. Telefonbuch, Mikrofon). Nicht immer aber sind Berechtigungen „böse“ oder „schlecht“, denn manche Berechtigungen brauchen Apps einfach zum Funktionieren.

Aufgaben:

1. Wann ist eine Berechtigung „OK“ oder wann sagst du eher „Nein“?
Würdest du dir die vier Apps **Swarmy**, **Soundo**, **Wconnect** und **Style Checkas** auf dein Handy laden?
Entscheide und begründe. Du kannst zu jeder App ein Logo erfinden!

2. Überlege dir vier Tipps, wie du die Kontrolle über Berechtigungen behältst.

_____

_____

_____

_____

TIPP: App-Ausmist-Aktion – Mach's wie mit deinem Kleiderschrank

Apps greifen auch dann noch auf deine Daten zu, wenn du sie gar nicht mehr aktiv nutzt. Das kannst du prüfen, z.B. bei Android-Handys unter Einstellungen > Datenverbrauch („Hintergrunddaten“). Er-stelle eine Liste mit den zehn Apps, die du in den letzten vier Wochen benutzt hast. Lösche die anderen – vor allem kostenlosen – Apps, die du nicht mehr benötigst, von deinem Handy.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

handysektor klicksafe.de

SWARMY

Beschreibung:
Leite den Fischschwarm durch ein Unterwasserlabyrinth.

Berechtigungen:

- In-App Käufe
- Internetzugriff

App-Logo:

Meine Entscheidung:

Soundo

Beschreibung:
Mit Soundo kannst du nicht nur Musik hören, sondern auch Musik erkennen.

Berechtigungen:

- Mikrofon
- Internetzugriff
- Kontakte

App-Logo:

Meine Entscheidung:

WCONNECT

Beschreibung:
Die neue Messenger-App verbindet alle deine Wünsche: Chatten, Video- und Sprachnachrichten.

Berechtigung:

- Internetzugriff
- Mikrofon
- Kontakte
- Kamera
- Standortdaten

App-Logo:

Meine Entscheidung:

Style Checkas

Beschreibung:
Bist du Beauty oder Loser? Die App sagt es dir.

Berechtigung:

- Internetzugriff
- Mikrofon
- Kontakte
- Kamera
- Standortdaten
- SMS
- Speicher
- In-App Käufe

App-Logo:

Meine Entscheidung:

Smartphone- aber sicher! – Der Smartphone-Führerschein

Projekt 2	***Ziele***	*Die SuS lernen Sicherheitseinstellungen und andere Funktionen ihres Handys kennen.*
	Zeit	*120 min., pro Station ca. 10 min.*
	Methoden	*Stationenarbeit*
	Material	*Smartphone-Führerscheine kopieren, Laufzettel, Stationenbeschreibungen ausdrucken, Schülerhandys*
	Zugang Internet/PC	*Ja (PC Raum). Handys u. Kopfhörer sollen explizit in den Unterricht mitgebracht werden. Wenn möglich Wlan für Handys aktivieren*

Vorbereitung

Kündigen Sie rechtzeitig an, dass die SuS ihre Handys mit in den Unterricht bringen sollen. Bereiten Sie den Raum mit 5 Stationen und den Stationenbeschreibungen vor. An jeder Station sollte ein PC oder Tablet mit Internetverbindung zur Verfügung stehen. Wenn dies nicht möglich ist, können die SuS auch an ihren Handys recherchieren und die Videos anschauen (Schul-WLAN?). Für das Quiz an Station 4 ist ein PC notwendig. Legen Sie an Station 3 Papier für die Gestaltung der Tipps für den sicheren App-Kauf aus. Kopieren Sie die Führerscheine in der entsprechenden Anzahl der SuS.

Einstieg

Steigen Sie mit den Ergebnissen einer Studie in die Stunde ein: Laut einer Studie gehören 16- bis 19-jährige Nutzer zur Gruppe der „Fatalistischen Handynutzer“. Fatalistisch bedeutet schicksalsergeben. Was bedeutet das, und wie könnt ihr euch das erklären?
Quelle: *www.sicher-im-netz.de/sites/default/files/download/2015_dsin_verbraucher-index-studie_web.pdf,* S.22, (Abruf: 25.01.2018) Erklärung: Trotz guter Kenntnisse und hohem Gefährdungsgefühl verzichtet diese Gruppe auf Basisschutzmaßnahmen wie z. B. Passwörteränderungen.

Alternative: Abfrage in der Klasse zum Thema sicheres Handy: Wer von euch nutzt die Bildschirmsperre? Wie häufig wechselt ihr eure Passwörter? Wer hat Antiviren-Programme auf seinem Handy? Wer nutzt Privatsphäre-Einstellungen in Diensten wie WhatsApp oder Facebook?

Teilen Sie die SuS in fünf Gruppen ein und verteilen Sie die Laufzettel. Da alle Gruppen alle Stationen durchlaufen, ist es egal, an welcher Station sie beginnen. Teilen Sie daher die Gruppen den einzelnen Stationen zu. Für jede Station werden ungefähr 10 Minuten benötigt.

Erarbeitung

Kündigen Sie auf ein akustisches Signal hin den Stationenwechsel an.

TIPP: Informationen recherchieren lassen

Wenn die SuS Hintergrundinformationen benötigen, lassen Sie die Recherche in einer Suchmaschine an PC oder Tablet durchführen. Bei Handysektor finden die SuS ein Lexikon, in dem Begriffe wie IMEI erklärt werden: *www.handysektor.de/lexikon.html* Die SuS haben auch die Möglichkeit, sich gegenseitig zu helfen. So können „Experten“ für bestimmte Handys und Handy-Betriebssysteme ernannt werden, die bei Fragen speziell an den Stationen 1 bis 3 gruppenunabhängig helfen.

Sicherung

Die Gruppenergebnisse sowie die „unbekannten Funktionen“ (Tafelanschrieb Station 2) sollen vorgestellt und besprochen werden. Die Smartphone-Führerscheine werden bereits unterschrieben an die SuS ausgeteilt.

Station 1: Sicherheit - Schütz dein Phone!

Sicherheit für euer Smartphone ist bestimmt ein Thema für euch, oder? Dann sollten die Einstellungen an euren Geräten auch so aussehen wie in der Tabelle unten. Wenn ihr etwas nicht findet, fragt jemanden aus eurer Gruppe, der das gleiche Smartphone hat, oder gebt eure Frage zusammen mit eurem Betriebssystem in eine Suchmaschine ein. Streicht auf eurem Laufzettel durch, was ihr bereits richtig eingestellt habt. Wenn ihr im Unterricht etwas nicht erledigen konntet, holt es zu Hause nach.

TIPP: Auf *www.handysektor.de/lexikon.html* findet ihr Erklärungen zu den Begriffen.

GPS, WLan und Bluetooth	**ausschalten** (wenn du es nicht brauchst)
Betriebssystem Update	**durchführen**
AntiVirus App (nur für Android notwendig, beim Download auf gute Bewertung im Store achten)	**installieren**
Bildschirmsperre (am Sichersten mit Passwort)	**einschalten**
IMEI (= die Seriennummer eures Handys, bei Verlust oder Diebstahl der Polizei melden)	**herausfinden und notieren**
In-App-Käufe (z.B. Zusatzkäufe in Spiele-Apps wie Münzen oder Edelsteine)	**ausschalten**
„Handy suchen“ (iPhone: schau in den Einstellungen nach; Android: schau unter android.com/devicemanager im Internet nach)	**herausfinden und aktivieren**
Roaming	**ausschalten**
Hausaufgabe: Drittanbietersperre/Mehrwertdienste sperren lassen (z.B. Premium-SMS für Casting-Shows)	**sperren lassen** beim Telefonanbieter (Eltern bzw. Vertragsinhaber anrufen lassen)

Zusatzaufgabe: Hier gibt es Videos von Handysektor, die euch bei den Aufgaben helfen können und weitere Infos liefern: Was ist eigentlich ein Bewegungsprofil?
Unter *http://bit.ly/1RxIGdo* und
Kostenfallen unter *http://bit.ly/1Rjv4oN*

Station 2: Funktionen - Check dein Phone!

Fast jede Woche kommt ein neues Handy auf den Markt, mit immer spektakuläreren Funktionen: Fingerabdrucksensor, verbesserte Spracherkennung, mobile Bezahlfunktionen und noch viel mehr.

Kennt ihr euer Handy eigentlich in- und auswendig? Wählt aus der folgenden Liste mindestens drei Aufgaben aus, am besten etwas, das ihr noch nicht gemacht habt.

- Erstellt ein Foto, das ihr direkt am Handy mit Funktionen, die euch zur Verfügung stehen, bearbeitet.
- Erstellt ein kurzes Video (max. 10 Sekunden) und zeigt es jemandem aus eurer Gruppe.
- Findet heraus, ob es Einstellungen für die Beschränkung von Nutzungszeiten gibt (bei iOS unter „Bildschirmzeit“).
- Erstellt eine Nachricht per Spracheingabe, z.B. SMS oder WhatsApp.
- Erstellt einen Termin in eurem Kalender, z.B. die nächste Klassenarbeit.
- Denkt euch etwas Eigenes aus.

Zusatzaufgabe: Unbekannte Funktionen
Habt ihr bei eurer Reise ins Handy Funktionen entdeckt, die ihr noch nicht kanntet? Wenn nicht, dann macht euch auf die Suche! Schreibt sie an die Tafel und erklärt sie am Ende der Stunde euren Klassenkameraden und -kameradinnen.

Station 3: Apps – Alles unter Kontrolle?!

Apps kaufen und installieren ist kinderleicht, oder?
Dass man dabei aber auch einiges beachten muss, zeigt euch das Video „Appgesichert“ unter *http://bit.ly/1RfJ303*

Quelle: *www.handysektor.de/mediathek/videos/erklaervideo-appgesichert.html, (*Abruf: 25.01.2018)

Notiert die vier wichtigsten Tipps aus dem Video und gestaltet sie ansprechend für eure Klassenkameraden und -kameradinnen (auf Papier, in einem Textverarbeitungsprogramm am PC oder mithilfe einer Design-App wie Pic Collage am Handy oder Tablet).

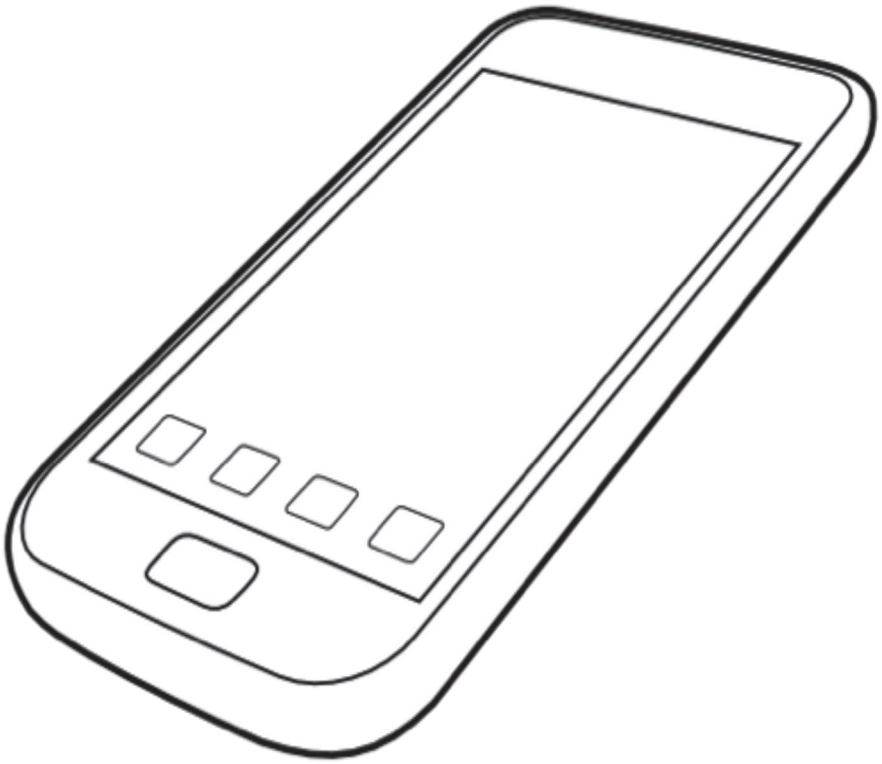
Station 4: Quiz „Smart mobil?!“

Testet euer Handywissen am Computer mit dem klicksafe- Quiz „Smart mobil“. Wählt das Quiz mit den Zusatzinfos! Habt ihr alle gut aufgepasst? Jeder merkt sich eine Frage, die er besonders schwierig fand und stellt sie am Ende des Quiz' nochmal in der Gruppe.
Quiz: https://www.klicksafe.de/quiz

Quelle:
https://www.klicksafe.de/quiz (Abruf: 14.02.2019)

Station 5: Das sichere Handy der Zukunft

Das Handy der Zukunft liegt vor euch, allerdings nur als leere Skizze. Welche Sicherheitsfunktionen sollte es haben? Welche Apps braucht es zum Schutz? Zeichnet oder schreibt eure Ideen darauf!



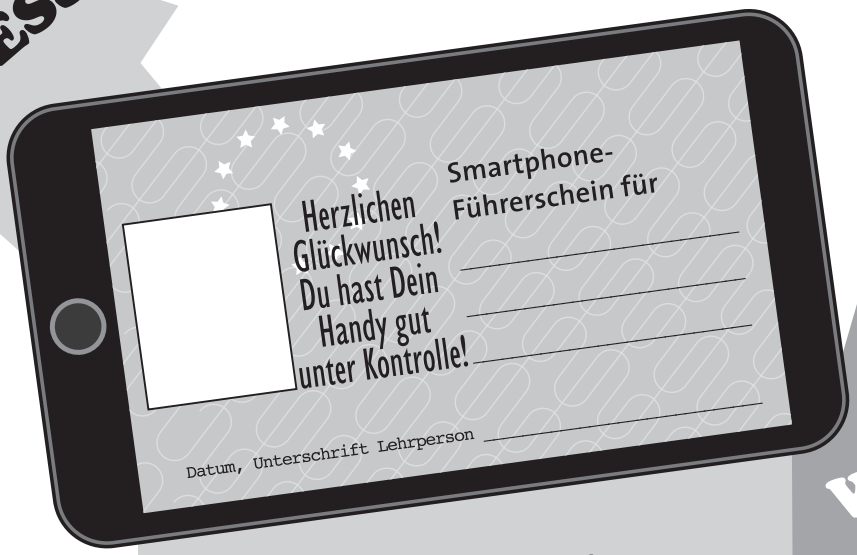
Zusatzaufgabe:
Habt ihr Lust auf weitere Informationen zum Thema sicheres Handy? Recherchiert zu folgenden Begriffen: Blackphone und Kryptohandy, und notiert euch auf der Rückseite eures Laufzettels, was ihr dazu herausfindet.

YEEESS

WOOW

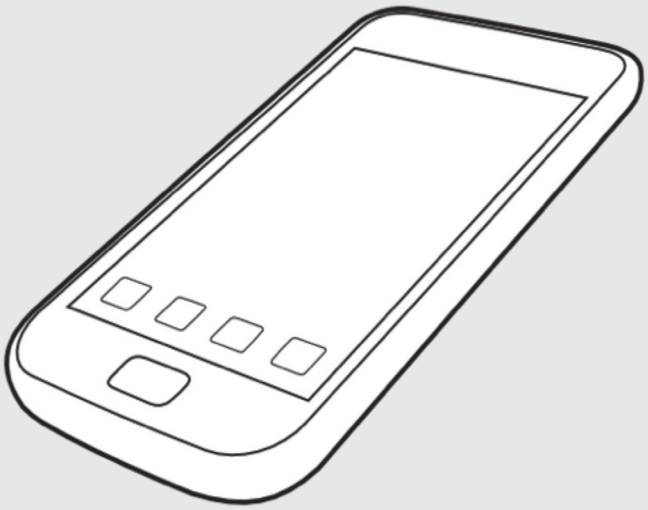
1. Sicherheit - schütz dein Phone
2. Funktionen - check dein Phone
3. Apps - alles unter Kontrolle
4. Handywissen - SmartMobil
5. Das sichere Handy der Zukunft

YEEESS



WOOW

1. Sicherheit - schütz dein Phone
2. Funktionen - check dein Phone
3. Apps - alles unter Kontrolle
4. Handywissen - SmartMobil
5. Das sichere Handy der Zukunft

Laufzettel: Der Smartphoneführerschein - Name:	
Station	Hake ab, was du erledigt hast:
1. Sicherheit	☐ GPS, WLan und Bluetooth ☐ Update Betriebssystem ☐ AntiVirus App ☐ Bildschirmsperre ☐ IMEI ☐ In-App- Käufe ☐ „Handy suchen“ ☐ Roaming
2. Funktionen	☐ bearbeitetes Foto ☐ kurzes Video ☐ Beschränkung von Nutzungszeiten ☐ Nachricht per Spracheingabe (SMS, Whats App) ☐ Termin ☐ eigene Idee: _____ Hausaufgabe: ☐ Drittanbietersperre/Mehrwertdienste
3. Apps	Tipps für den sicheren App-Kauf: 1. _____ 2. _____ 3. _____ 4. _____
4. Handywissen	Erreichte Punktzahl: _____ von _____
5. Sicheres Handy der Zukunft	

Daten in den Wolken

Projekt 3	***Ziele***	*Die SuS erkennen, welche Vor- und Nachteile mit der Speicherung von Daten in der Cloud verbunden sind.*
	Zeit	*45 min.*
	Methoden	*Sammlung +/- (Tafelbild), Tipps gestalten, Recherche*
	Material	*Video Cloud (3,15 min.), Kopiervorlage Wolke*
	Zugang Internet/PC	*Nein (Video downloaden)*

Einstieg

Fragen Sie das Vorwissen der SuS zum Thema ab: Ihr habt sicher schon mal von Cloud oder Clouding gehört. Wisst ihr, woher diese Bezeichnung kommt? Die Erklärung ist auf dem Arbeitsblatt und im Handysektor-Erklärvideo zu „Cloud“ zu finden. Teilen Sie das Arbeitsblatt zu Projekt 3 aus und zeigen Sie das Video:
www.handysektor.de/mediathek/videos/erklaervideo-cloud.html

Erarbeitung

Die SuS tragen die Vor- und Nachteile der Datenspeicherung in einer Cloud auf dem Arbeitsblatt zusammen. Besprechen Sie die Aufgabe, vielleicht mit Unterstützung eines Tafelbildes. Die SuS ergänzen ihre Notizen.

Vorteile:

- Programme können ohne lokale Installation über das Internet genutzt werden.
- Man kann gleichzeitig mit Freunden an einem Dokument arbeiten.
- Man kann Computerspiele in guter Qualität streamen
- Die Cloud kann als Datenspeicher genutzt werden, sodass ein größerer lokaler Speicher auf den Geräten zur Verfügung steht.
- Daten können auf allen Geräten synchronisiert werden.
- Der Zugriff auf Daten ist von überall aus möglich.
- Die Cloud-Anbieter verfügen bei Handyverlust über Sicherheitskopien.

Nachteile:

Es besteht Unsicherheit in Bezug auf den Datenschutz (Wie gehen Dienste mit Daten um? Wird etwas weitergegeben/ausgewertet?)

- Die Sicherheit von Cloud-Diensten ist nur schwer überprüfbar.
- Wo stehen die Server? Welches Recht gilt?
- Ohne Internetverbindung ist kein Zugriff auf die Daten möglich.
- Was passiert mit den eigenen Daten, wenn ein Cloud-Anbieter seinen Dienst einstellt und die Daten (Filme, Musik etc.) nicht lokal gespeichert sind?

Die SuS untersuchen anhand der Tabelle die von ihnen genutzten Dienste auf Datenspeicherung in der Cloud und kommen wahrscheinlich zu dem Ergebnis, dass ein Großteil der Dienste, die sie nutzen, ihre Daten in der Cloud speichert.

Test: Sind meine Daten in der Cloud?

Idee 1:

Wenn folgende Fragen mit Ja beantwortet werden können, speichern die Dienste Daten in der Cloud:

- „Kann ich dort Daten (Texte, Bilder, Videos, Termine etc.) speichern und von anderen Geräten abrufen?“
- „Kann ich mit der App Informationen (Texte, Bilder etc.) mit anderen teilen/austauschen?“
- „Kann ich über die App auf Medien (Musik, Videos/Filme) aus dem Netz zugreifen, ohne diese Daten herunterladen zu müssen?“
- „Funktioniert die App nur mit Internetzugang?“

Idee 2:

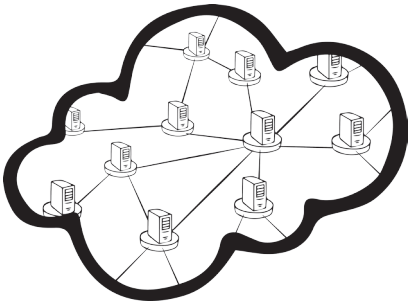
Schüler schalten ihr Smartphone in den Flugmodus. Die meisten Apps, die dann nicht mehr funktionieren – weil sie keinen Internetzugriff mehr haben –, greifen auf eine Form von Clouddienst zurück. Ausgenommen sind hiervon alle Arten von Browsern (z.B. Chrome, Safari etc.), die einfach nur Internetseiten anzeigen.

Sicherung

Die SuS lesen die Tipps auf dem Arbeitsblatt und gestalten einen ausgewählten Tipp in Form einer Wolke. Teilen Sie dazu die Kopiervorlage zu Projekt 3 aus. Sie können die Tipps auch zuteilen, sodass alle fünf Tipps ausgestaltet werden. Die Wolken werden vorgestellt. Sie können im Klassenraum aufgehängt werden. Zum Abschluss der Einheit sollen die SuS entscheiden können: Welche Cloud-Dienste will ich weiterhin nutzen, welche Daten gebe ich an die Cloud ab und welche lege ich lieber lokal ab. Sprechen Sie zum Abschluss mit den SuS über folgende Themen: Gehen wir mit dem rasanten Fortschritt, oder treten wir einen Schritt zurück und betrachten alles aus der Distanz? Und haben wir überhaupt noch eine Wahl?

Definition: iCloud, Synchro, Clouding… Was ist eigentlich die Cloud?

Computer und Speicher sind heute auf der ganzen Welt miteinander vernetzt. Der genaue Aufbau wirkt aber wie von einer Wolke (engl. Cloud) verschleiert. Wenn Informationen nicht zentral auf einem Rechner, sondern irgendwo in einem großen Server-Netzwerk liegen, dann sind sie in der Cloud.



Aufgaben:

1. Schaut euch das Handysektor-Erklärvideo „Was ist eigentlich die Cloud?“ an.
Notiert, welche Vor- und Nachteile sich aus der Speicherung von Daten in der Cloud ergeben.
Video: *www.handysektor.de/mediathek/videos/erklaervideo-cloud.html*

_____ _____

_____ _____

_____ _____

2. Tom aus dem Video nutzt bereits Cloud-Dienste: Seine E-Mails liegen in der Cloud, und er streamt Musik und Filme. Welche Cloud-Dienste nutzt du selbst bereits? Schreibe sie auf.

Kategorie	Ja/Nein	Name des Dienstes
E-Mails		
Smartphone> Kalender, Musik, Fotos etc. (z.B. iCloud, Google Drive)		
Musik-Streaming (z.B. Spotify)		
Video-Streaming (z.B. Netflix)		
Cloud Gaming (z.B. OnLive)		
Textverarbeitung (z.B. Google Docs)		
Datenspeicher (z.B. Dropbox)		

3. Lies die folgenden Tipps von Handysektor durch. Such dir einen der Tipps aus und schreibe ihn in die Wolkenvorlage. Du kannst die Vorlage auch noch schön gestalten.

Damit du Cloud-Dienste gefahrlos nutzen kannst,
hier die wichtigsten Tipps:

1. Speichere sensible private Daten wie intime Fotos oder geheime Dokumente nicht in der Cloud.

2. Deaktiviere den automatischen Upload von Bildern oder Dokumenten von deinem Smartphone und entscheide stattdessen für jede Datei, ob du diese in die Cloud laden möchtest (Bild Beispiel iCloud, Quelle: klicksafe, iOS 9.3.1).

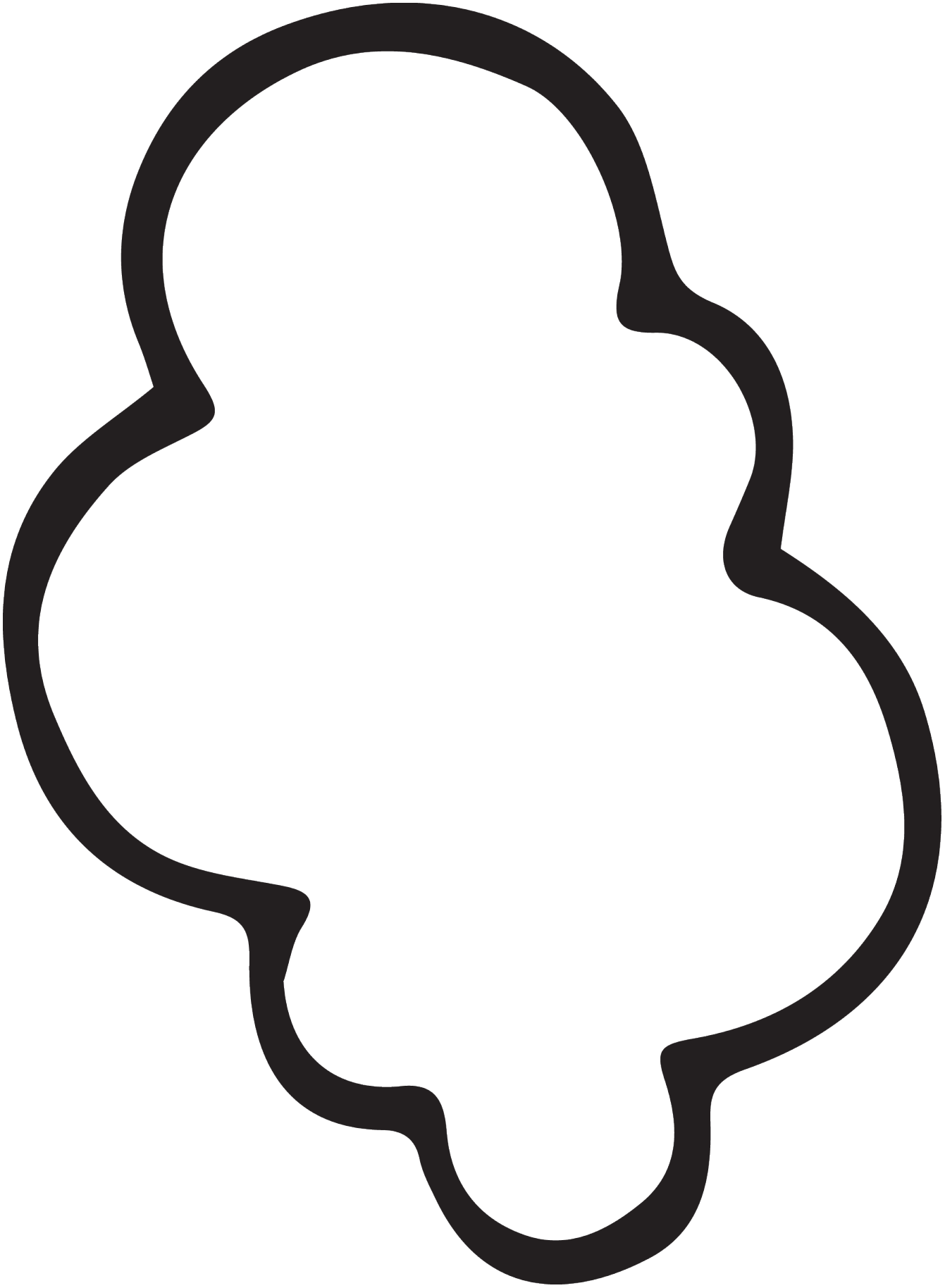
Quelle: *www.handysektor.de/themenmonate/detailansicht/article/safer-cloud-datenschutz-in-der-wolke.html*

3. Verwende ein sicheres Passwort, um deinen Cloud-Zugang zu schützen. Verwende dieses Passwort nirgendwo sonst.

4. Nutze, wenn möglich, die Zwei-Wege-Authentifizierung*, um deinen Zugang zur Cloud zusätzlich abzusichern.

5. Speichere alle Dateien zusätzlich bei dir, z.B. auf einer externen Festplatte. Die Gefahr ist gering, dass Daten in der Cloud verloren gehen, aber so gehst du auf Nummer sicher!

** Zwei-Wege-Authentifizierung bedeutet, dass dir dein Anbieter einen Einmalcode per SMS auf dein Handy schickt, den du zusätzlich zu deinem Passwort beim Anmelden eingeben musst. Da der zweite Code über einen anderen „Weg" verschickt wird, müsste ein Krimineller sowohl dein Passwort knacken als auch an dein Handy gelangen, um Zugang zu deinen Daten zu erhalten.*



Co-financed by the Connecting Europe Facility of the European Union

Herausgeber:

klicksafe ist das deutsche Awareness Centre im CEF Telecom Programm der Europäischen Union.

klicksafe sind:

Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz, www.lmk.de

Landesanstalt für Medien NRW – www.medienanstalt-nrw.de

und

Handysektor ist die unabhängige Anlaufstelle für den digitalen Alltag von Jugendlichen. Die Webseite ist ein gemeinschaftliches Projekt der Landesanstalt für Medien NRW und des Medienpädagogischen Forschungsverbundes Südwest (mpfs). Die Projektleitung hat Florian Beutenmüller (mecodia GmbH) inne.

Bezugsadresse: klicksafe

c/o Landeszentrale für Medien und
Kommunikation (LMK) Rheinland-Pfalz
Turmstraße 10
D - 67059 Ludwigshafen
E: info@klicksafe.de
W: www.klicksafe.de

.puntomedien