digitalcourage (Hrsg.)

Jessica Wawrzyniak

#KIDS #DIGITAL #GENIAL

Schütze dich und deine Daten!

Das Lexikon von App bis .zip

Verlag Art d'Ameublement

#KIDS #DIGITAL #GENIAL

Schütze dich und deine Daten!

Das Lexikon von App bis .zip

2. erweiterte Auflage,
Juli 2019

★ 26 neue Begriffe

Impressum

Verlag: Art d'Ameublement – cc-by 4.0

Hrsg.: Digitalcourage e.V.

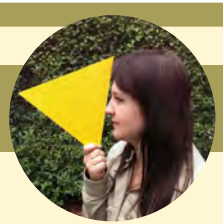
Autorin: Jessica Wawrzyniak

Titelgestaltung: Linda Mieleck, lindamieleck.de

Satz, Layout, Illustrationen: Isabel Wienold, iwi-design.de

Lektorat: Claudia Fischer

ISBN 978-3-934636-20-0



Jessi

Hallo ihr Lieben

Ich bin Jessi und schreibe für euch den Blog **#Kids #digital #genial**. Auf der Internetseite www.kidsdigitalgenial.de erkläre ich euch, wie ihr eure persönlichen Daten und Privatsphäre – zum Beispiel beim Surfen im Internet – schützen könnt. Dort findet ihr die wichtigsten Neuigkeiten, einen App-Check und ein großes Lexikon mit über 150 Begriffen.

Egal ob bei Instagram, YouTube, Snapchat, WhatsApp, Facebook, Twitter, Ask.fm, Musical.ly, Spotify, Netflix,... Ich bin überall unterwegs, um nach Tipps und Tricks für euch zu suchen. Ob ihr die Tipps zur sicheren Mediennutzung und Datenschutz am Ende umsetzen wollt, das könnt ihr selbst entscheiden!

Das Lexikon ist das Kernstück des Blogs, deshalb habe ich es als kleines Heft für euch abdrucken lassen. Wer von euch kann denn mit wenigen Worten erklären, was „Medien" überhaupt sind? Und wie lautet die Einzahl von „Medien"? Blättert euch durch bis zum Buchstaben „M" und schaut es nach!

Ich gebe euch zunächst eine kleine Starthilfe, was „Datenschutz" eigentlich genau bedeutet und dann könnt ihr euch quer durch das Lexikon lesen – von **A** bis **Z** oder angefangen bei eurem Lieblingsbuchstaben.

Und wenn ihr das alles schon wisst, dann gebt das Heft einfach an Freunde weiter. Und auch an eure Eltern! Denn ich bin sicher, dass die auch noch einiges lernen können!

Viel Spaß!
Eure Jessi

Datenschutz

wieso, weshalb, warum?

1. Was sind private Daten?

➢Daten sind in erster Linie Informationen, egal worüber. Private Daten hingegen sind Informationen, die deine Person betreffen, also Informationen wie zum Beispiel dein Name, deine Größe, dein Gewicht oder dein Geburtsdatum. Wer diese Daten hat, kann dich damit erkennen. Diese Daten nennt man „personenbezogene Daten". Aber auch Informationen über deine Interessen, deine politische Meinung und deine Gedanken sind private Informationen.

2. Wieso sind deine Daten Privatsache?

Daten sind Informationen und jeder Mensch hat das Recht, selbst zu bestimmen, was mit den Informationen über die eigene Person (personenbezogene Daten) passiert. Das steht so im Gesetz.

Unter den Begriff Datenschutz fallen viele verschiedene Formen:

- Schutz der informationellen Selbstbestimmung: Du darfst selbst bestimmen, wer Informationen über dich erhält und welche Informationen das sind. In den ersten Jahren übernehmen das zwar deine Eltern für dich, aber sobald du deine Entscheidung begründen kannst, zählst du in der Hinsicht als einwilligungs- und entscheidungsfähig – egal wie alt du bist.
- Schutz vor Datenmissbrauch: Das heißt, dass deine Daten nicht anders genutzt werden dürfen als von dir gewünscht und nur von denen, denen du das erlaubt hast.
- Schutz des Persönlichkeitsrechts bei der Datenverarbeitung: Deine Persönlichkeit darf durch die Nutzung von Daten/Information nicht beeinträchtigt werden. Es ist zum Beispiel nicht erlaubt, dass deine Ehre durch Beleidigungen beeinträchtigt wird, dein Name durch Fake-Profile „beschmutzt" wird oder unerlaubt Fotos von dir verbreitet werden (➢Recht am eigenen Bild).
- Schutz der ➢Privatsphäre: Es ist dein Recht, dass nicht jeder immer wissen muss, was du tust oder denkst. Genauso ist es dein Recht, deine Meinung frei zu äußern, ohne dass du Angst davor haben musst, für deine Meinung bestraft zu werden. Außerdem ist es dein Recht, dich frei bewegen und handeln zu können, ohne dass andere deine Taten verfolgen oder beobachten.

Privatsphäre und Datenschutz sind wichtig! Man muss gar nicht erklären, wieso der Schutz von Daten wichtig ist, sondern Privatsphäre ist eine Selbstverständlichkeit. Es fragt auch niemand nach, wieso es wichtig ist, die Natur zu schützen…so sollte es mit dem Schutz privater Daten auch sein.

3. Wer sammelt deine Daten?

Gerade beim Surfen im Internet gibst du für gewöhnlich sehr viele Daten von dir preis, deshalb musst du auch dort sehr genau aufpassen, welche Daten du angibst und was mit deinen Daten passiert. Dass Kriminelle, zum Beispiel pädophile Straftäter (➢Pädophilie) oder ➢Hacker, und auch ➢Drittanbieter an deinen Daten interessiert sind, erklärt sich von selbst. Aber es liegt in deiner Verantwortung, welche Daten du überhaupt zur Verfügung stellst. Oft merkst du gar nicht, wo du überall Spuren hinterlässt, weil dein Computer oder dein Smartphone das einfach tun, ohne dich zu fragen. In dieser Broschüre erfährst du viele Möglichkeiten, wie du das verhindern kannst.

Hier entstehen Datenspuren:

- Im Internet: ➢Soziale Netzwerke, ➢Betriebssysteme, ➢Suchmaschinen, ➢Cookies, Online-Shops, ➢Smartphones/Tablets, ➢Apps, ➢Clouds, ➢Streaming-Dienste, …
- Mit Hilfe von Lesegeräten und Funk: Kundenkarten, Kreditkarten, Videoüberwachung, Navigationsgeräte, Flugdaten, …
- ➢Internet der Dinge: Smart Home, Fitnessarmbänder, ➢Smarte Autos, gechippte Kleidung, Fernseher, vernetztes Spielzeug…

4. Na und? Ich habe doch nichts zu verbergen!

Der Schutz deiner Daten ist ein Menschenrecht!
In der Vergangenheit haben immer wieder viele Menschen für die Rechte der Menschen in der Bevölkerung gekämpft, und der Schutz deiner Privatsphäre gehört dazu. Durch die Verbreitung deiner persönlichen Daten gibst du dieses Recht freiwillig auf! Im Bus oder in der Straßenbahn magst du es schließlich auch nicht, wenn dir Fremde zu nahe kommen, aber das tun sie genauso, wenn sie auf verschiedenen technischen Wegen private Informationen über dich sammeln.

Andere entscheiden, ob du etwas zu verbergen hast!
Du weißt nicht, ob du etwas zu verbergen hast, denn jede noch so harmlose Information über dich könnte gegen dich verwendet werden, um dir zu schaden. Beispiele:

- Du veröffentlichst vielleicht ein Foto von dir, das du sehr schön findest, aber andere finden dieses nicht so schön und machen sich lustig darüber.
- Oder wenn du zum Beispiel deine homosexuelle Orientierung preisgibst, wozu du stehst und was für dich kein Geheimnis ist, kann es trotzdem sein, dass andere damit nicht klar kommen und du zu einer Zielscheibe für Beleidigungen oder Schlimmeres wirst.
- Außerdem können Informationen über dich, wie zum Beispiel Hobbys, politische Ansichten, sexuelle Orientierung oder Menschen, mit denen du zu tun hast, an einem Tag harmlos sein und am nächsten nicht mehr.

Man hat nicht immer böse Absichten!
Ein Klick ist schnell gemacht, eine Nachricht schnell verschickt, ein ➢Link schnell geteilt oder geliked. Du kannst dich bestimmt nicht mehr daran erinnern, was du in den letzten Tagen ganz genau geliked, kommentiert oder verschickt hast und weißt auch nicht, was du damit vielleicht ausgelöst haben könntest. Du hast dich jedenfalls an Prozessen beteiligt, bei denen auch andere Menschen beteiligt waren, und kannst dir nicht sicher sein, welche Wirkung und welchen Einfluss dein Handeln hat.

Deine Daten bleiben trotz Privatsphäre-Einstellungen nicht privat!
Viele Informationen würdest du nur mit der Familie und Freunden teilen. Deine Kanäle in Sozialen Netzwerken wie zum Beispiel bei Instagram, Facebook und so weiter, stellst du deshalb schlauerweise so ein, dass nur Freunde deine Inhalte sehen können. Aber die Anbieter dieser Seiten sehen deine Daten auch, weil alle deine Daten auf deren ➢Servern gespeichert werden!

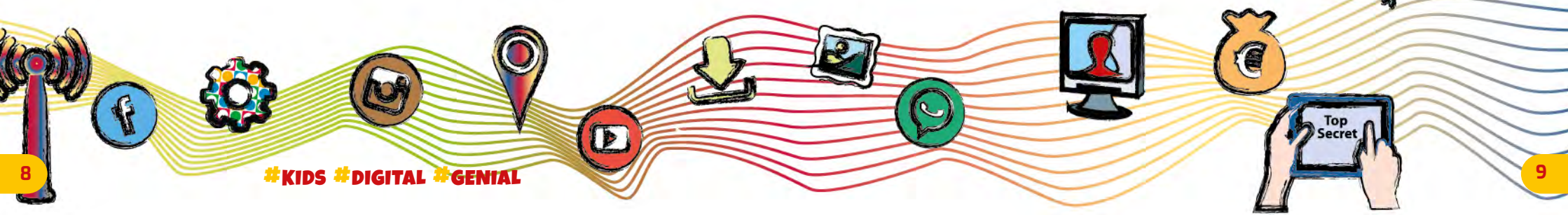
Du hast keinen Überblick über die Verbreitung deiner Daten!
Du weißt nicht genau, an wen deine persönlichen Daten weitergegeben werden, aber es ist dein Recht, dass du selbst darüber bestimmen darfst, wer welche Informationen über dich bekommt. Oft werden deine Daten an sogenannte ➢Drittanbieter weiter gegeben und das steht auch in den ➢AGB der Dienste, die du nutzt. Aber du weißt nicht, an welche Drittanbieter genau und was diese dann mit deinen Daten machen.

Die Polizei wertet private Daten aus!
Strafverfolgungsbehörden, wie zum Beispiel die Polizei, können bei verschiedenen Anbietern Einsicht in deine Daten verlangen und dies tun sie auch, selbst wenn du dich nicht strafbar gemacht hast. Es gibt deshalb keine harmlosen Informationen, denn auch die Tatsache, dass du dir ein Eis in einem bestimmten Laden gekauft hast, könnte dazu führen, dass du in den Kreis der Verdächtigen rückst, wenn in der Nähe dieses Ladens ein Verbrechen stattgefunden hat. Das gilt auch für die Auswertung von Überwachungskameras, die an vielen öffentlichen Orten hängen.

Unternehmen verdienen Geld mit deinen Daten!
Private Daten sind für Unternehmen Gold wert. Gerade, wenn du kostenlose Dienste nutzt, wie zum Beispiel Soziale Netzwerke, dann sind diese meistens nicht wirklich kostenfrei, sondern du bezahlst mit den Daten, die du hinterlässt. Dir kommt es also nur so vor, als wären die Dienste kostenfrei, dabei hat sich das Bezahlsystem nur geändert.

Deine Persönlichkeit wird analysiert!
Du machst dich manipulierbar! Wenn du angibst, was dir gefällt (Beiträge, Filme, Produkte, ...), kann ganz einfach eine Persönlichkeitsanalyse von dir erstellt werden. Dadurch bekommst du zum Beispiel Werbung angezeigt, die genau auf deine Interessen zugeschnitten ist (➢personalisierte Werbung). Vielleicht freust du dich darüber, aber eigentlich wurdest du in dem Moment nur manipuliert, um mehr Geld auszugeben.

Die Entwicklung deiner Persönlichkeit wird manipuliert!
Wenn du zum Beispiel immer die Werbung angezeigt bekommst, die dir auf jeden Fall gefällt, wie sollst du denn dann etwas Neues kennenlernen? Womöglich kaufst du die angezeigten Produkte und das bestätigt wieder dein Interesse daran. Ein bestimmtes Bild über dich wird immer fester



gestrickt und beeinflusst deine Entwicklung. Du wirst sozusagen gezwungen, dich so zu verhalten, wie man es von dir gewohnt ist.

Die Analyse deiner Person kann gegen dich verwendet werden!
Ein Beispiel: Anhand deines Surf- und Kaufverhaltens kann eingeschätzt werden, wie viel Geld du hast. Und auch andere Informationen, zum Beispiel welches Gerät du zum Surfen nutzt, kann etwas über deine finanzielle Lage aussagen, denn Apple-Geräte sind zum Beispiel meistens teurer als alle anderen Marken. So kann es beispielsweise passieren, dass dir für ein und dasselbe Produkt (zum Beispiel für eine Reise) ein teurerer Preis angezeigt wird, wenn du mit einem Apple-Gerät surfst. Denn es wird davon ausgegangen, dass du mehr Geld hast. Anderes Beispiel: Vielleicht recherchierst du über eine bestimmte Krankheit oder vertraust jemanden an, dass du selber krank bist. Wenn deine Krankenversicherung an diese Information kommt, kann es sein, dass deine Eltern höhere Versicherungsbeiträge für dich zahlen müssen. Also: Du hast ganz viel zu verbergen!

Deine Daten können Kriminellen in die Hände fallen!
Wenn du beispielsweise irgendwo öffentlich schreibst, dass du jetzt im Urlaub bist oder dich mit deinem Standort am Urlaubsort verlinkst, dann teilst du auch vielen Fremden mit, dass bei dir gerade niemand Zuhause ist, und lockst somit womöglich Einbrecher an. Aber auch andere Kriminelle, wie Hacker, sind an deinen Daten interessiert, weil sie diese weiterverkaufen können. Denn wie schon gesagt: Private Daten sind viel Geld wert.

5. Welche Daten solltest du besonders schützen?

Du solltest grundsätzlich so wenige Daten wie möglich von dir preisgeben, aber es gibt ein paar Informationen, die dir, gerade als Kind oder Jugendliche.r, wirklich gefährlich werden könnten, wenn sie an Fremde gelangen:

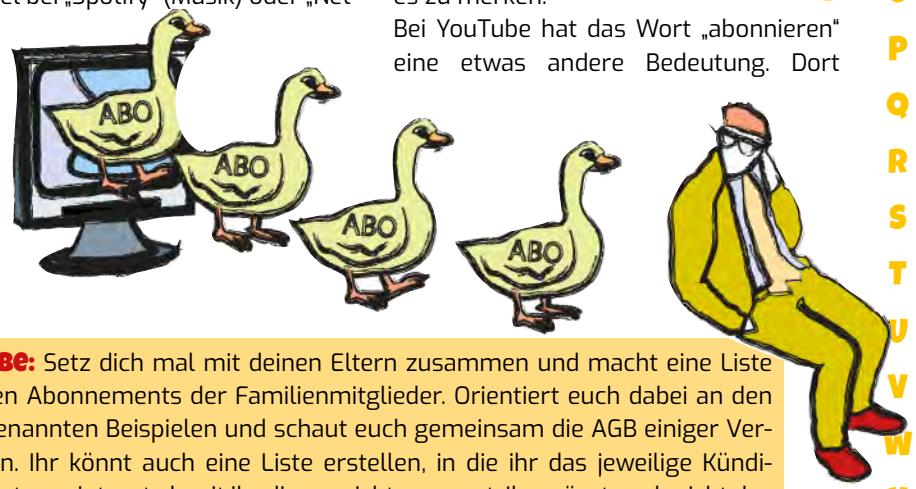
- Vor- und Nachname
- Vollständiges Geburtsdatum
- Namen von deinen Eltern und Freunden (zum Beispiel Freundeslisten)
- Handynummer
- Adresse
- E-Mail-Adresse
- Fotos/Videos von dir und Freunden
- Name deiner Schule
- Standorte, wo du dich aufhältst
- Kontodaten
- ...

Abonnement

Ein „Abonnement“ (Kurzform: „Abo“) ist in der Regel ein Kaufvertrag. In diesem Kaufvertrag wird festgelegt, dass man eine bestimmte Leistung über einen bestimmten (längeren) Zeitraum in Anspruch nimmt und dafür bezahlt.
Abos können in ganz verschiedenen Bereichen abgeschlossen werden, zum Beispiel

- bei Zeitungen, die man für ein Jahr abonniert, also für ein Jahr nach Hause geschickt bekommt und sie deshalb nicht jedes Mal im Kiosk kaufen muss,
- bei Fahrkarten, die dann zum Beispiel für den ganzen Monat gelten, sodass du nicht immer Einzeltickets für den Bus kaufen musst,
- bei ➤Apps und Programmen, zum Beispiel bei Spielen, die automatische ➤Updates bekommen,
- bei ➤Streaming-Diensten, wie zum Beispiel bei „Spotify“ (Musik) oder „Netflix“ (Serien und Filme), sodass man nicht für einzelne Lieder oder Serien bezahlt, sondern einen festgelegten Betrag für eine bestimmte Zeit.

Wichtig: Ein Abo muss in jedem Fall wieder gekündigt werden, wenn man es nicht mehr haben möchte, sonst läuft es weiter und man muss auch weiterhin bezahlen. Deshalb könntest du hin und wieder mal auf eine sogenannte „Abofalle“ stoßen, zum Beispiel wenn du den Dienst eigentlich gar nicht für längere Zeit in Anspruch nehmen wolltest oder keine Möglichkeit findest das Abo zu kündigen. Daher musst du dir immer ganz genau das Kleingedruckte, zum Beispiel die ➤Allgemeinen Geschäftsbedingungen (AGB) durchlesen, wenn du etwas im Internet kaufst. Sonst hast du vielleicht ein Abo abgeschlossen, ohne es zu merken.
Bei YouTube hat das Wort „abonnieren“ eine etwas andere Bedeutung. Dort



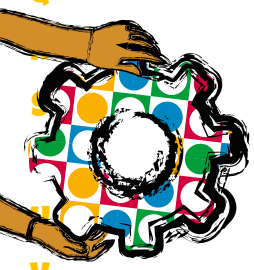
Aufgabe: Setz dich mal mit deinen Eltern zusammen und macht eine Liste mit allen Abonnements der Familienmitglieder. Orientiert euch dabei an den oben genannten Beispielen und schaut euch gemeinsam die AGB einiger Verträge an. Ihr könnt auch eine Liste erstellen, in die ihr das jeweilige Kündigungsdatum eintragt, damit ihr dieses nicht verpasst. Ihr müsst auch nicht das Kündigungsdatum abwarten, sondern könnt auch jetzt schon etwas kündigen, was vielleicht erst im nächsten Jahr ausläuft, zum Beispiel einen Handyvertrag. Vielleicht sind manche Abos auch gänzlich überflüssig?

kannst du einen „Channel“ (deutsch: „Kanal“) abonnieren und somit signalisieren, dass du informiert werden willst, wenn neue Videos hochgeladen werden. Du möchtest dem Geschehen also folgen. „Folgen“ heißt auf Englisch „to follow“, deshalb wird diese Funktion bei „Instagram“ auch so genannt. Dort heißen Abonnenten dann „Follower“. Von der Funktion her unterscheiden sich die Begriffe jedoch nicht.

Account

„Account“ ist das englische Wort für Benutzerkonto. Wenn du im Internet bei etwas mitmachen möchtest, zum Beispiel bei einem Chat in einem ➤Sozialen Netzwerk, einem ➤Forum oder bei einem Spiel, dann musst du dich meistens mit deiner E-Mail-Adresse anmelden/registrieren, dir einen ➤Nickname (Benutzernamen) überlegen und ein Passwort festlegen. Somit legst du dir ein eigenes Benutzerkonto an, welches auch nur du selbst benutzen solltest.

Oft wird auch angeboten, dich mit Google/Facebook/Twitter/Amazon/Github anzumelden, statt einen neuen Account anzulegen. Dabei fließen deine Daten aber eben auch an das Unternehmen, über das du dich anmeldest, deshalb solltest du meistens besser einen neuen Account anlegen. Ein Passwort-Manager hilft dir, den Überblick zu behalten. Das ist eine ➤Software, die alle deine Passwörter verschlüsselt speichern kann und du brauchst dir nur diesen Schlüssel zu merken.



Wichtig: Verrate niemandem dein Passwort, auch nicht deinen besten Freund.-innen, denn wer das Passwort kennt, kann viel Unsinn mit deinem Account anstellen:

- In Sozialen Netzwerken: Die Person könnte peinliche Fotos hochladen, schöne Fotos löschen, Menschen anschreiben, mit denen du gar nicht schreiben möchtest, Lügen verbreiten oder andere beleidigende Inhalte schreiben. Es kann sogar dazu kommen, dass jemand deinen Account nutzt, um dich zu mobben (➤Cybermobbing).
- In Spielen: Wenn sich eine andere Person bei einem Spiel mit deinem Benutzernamen anmeldet, könnte diese zum Beispiel deine Spielstände löschen, manipulieren oder zahlungspflichtige Funktionen nutzen, die du dann bezahlen musst (➤In-App-Käufe).
- In Foren: In einem Forum könnte die Person unter deinem Namen sehr peinliche Fragen stellen und so tun, als wärst du das gewesen.

Aufgabe: Erstelle eine Liste mit allen Accounts, die du angelegt hast. Soziale Netzwerke, Spiele, Foren, Mailadressen, Schulcomputer, Apps und so weiter. Wo bist du überall mit einem Benutzernamen angemeldet? Von welchen Accounts kannst du dich trennen?

Administrator.in (Admin)

Das Wort „Administration“ bedeutet Verwaltung. Ein Administrator oder eine Administratorin (Kurzform: „Admin“) kümmert sich somit um die Verwaltung, also entweder um „Papierkram“ (zum Beispiel an einer Rezeption) oder um die technische Verwaltung eines Unternehmens/einer Firma. Sie kennen sich also gut mit der ➤Software und ➤Hardware aus, die in einem Unternehmen verwendet werden, und kümmern sich darum, dass die ➤IT einwandfrei läuft.

Auf ➤Webseiten, in ➤Sozialen Netzwerken oder in ➤Foren sind Admins zum Beispiel dafür verantwortlich, dass die Kommunikation untereinander reibungslos funktioniert. Sie haben damit mehr Rechte als andere Nutzer.innen und können beispielsweise Kommentare löschen. Auch in WhatsApp-Gruppen gibt es immer einen Admin, der/die Mitglieder in der Gruppe verwalten kann. Oft kann nur der/die Admin Dinge wie Gruppennamen und Gruppenbild ändern. In manchen ➤Foren teilen sich die Admins die Arbeit mit den Moderatoren. Diese haben weniger technische Mittel zur Verfügung.

Algorithmus

Ein Algorithmus ist ein Bauplan, der ein Problem lösen soll. Die einzelnen Schritte der Vorgehensweise müssen klar und unwidersprüchlich definiert sein, zum Beispiel „Führe den Schritt nur durch, wenn die Bedingung A erfüllt ist. Führe den Schritt so lange durch, bis Bedingung B erfüllt ist.“

Schwer zu verstehen? Dann stell dir vor, du darfst nach dem Essen erst spielen gehen, wenn deine Hände sauber sind (siehe Grafik).

Nicht nur Menschen können eine Aufgabe oder ein Problem lösen, sondern auch Computer. Diese können viel komplexere Probleme mit ganz vielen Bedingungen lösen. Daher werden Algorithmen eingesetzt um große Datenmengen zu verarbeiten und zu analysieren.

Ein Algorithmus, den du ganz bestimmt kennst, ist der ➤EdgeRank bei Facebook und Instagram.

Aufgabe: Schnapp dir Zettel und Stift und denk dir selbst einen kleinen Algorithmus aus! Vielleicht macht es dir so viel Spaß, dass du irgendwann mal professionelles Programmieren lernst und tolle ➤Apps entwickelst.

Allgemeine Geschäftsbedingungen (AGB)

Die „Allgemeinen Geschäftsbedingungen“ (Kurz: AGB) sind das, was viele häufig als „Kleingedrucktes“ bezeichnen. Darin ist festgelegt, welche Regeln du beachten musst (deshalb auch manchmal „Nutzungsbestimmungen“ genannt) und welche vertraglichen Bedingungen du eingehst, wenn du ein Produkt kaufst oder nutzt. Du musst im Internet häufig bestätigen, dass du die AGB gelesen hast, um weiter zu kommen.

Wichtig: Du solltest dir immer durchlesen, was in den AGB steht, denn mit deinem „Okay“ stimmst du allen Punkten, die darin stehen, zu. Somit kann sich der Verkäufer oder Anbieter rechtlich absichern und wenn etwas passiert, bist du verantwortlich, weil du zugestimmt hast. Es sind meist lange und komplizierte Texte, aber es ist wichtig, dass du zumindest überfliegst, ob dir Zahlen (Preise) auffallen, nachschaust, was mit deinen Daten passiert (➢Datenschutz) und welche Verpflichtungen du eingehst. Häufig verstecken sich auch ➢Newsletter-Bestellungen, Gewinnspiel-Teilnahmen oder Abofallen (➢Abonnement) in den AGB.

Aufgabe: Suche deine Lieblings-App im AppStore, allerdings nicht auf deinem Handy, sondern auf dem Computer/Laptop, und drucke dir die Nutzungsbedingungen auf Papier aus. Nimm einen Textmarker und markiere alle Stellen, die du nicht verstehst. Anschließend kannst du deine Eltern fragen oder im Internet nach den unbekannten Begriffen suchen.

Android ★

„Android“ ist ein ➢Betriebssystem für mobile (tragbare) Endgeräte, wie Smartphones, Tablets und teilweise auch Netbooks.

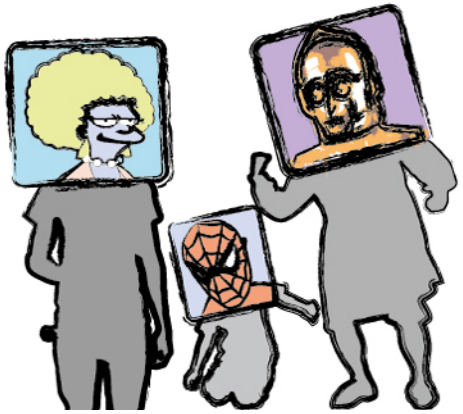
Wichtig: Android wird zwar auf den meisten mobilen Geräten, vor allem auf Smartphones, verwendet, ist aber leider ein sehr unsicheres Betriebssystem, dass sehr viele Daten sammelt. Ausserdem können sich leicht ➢Viren oder andere ➢Schadsoftware unbemerkt installieren und es kann leicht gehackt (➢Hacker) werden. Außerdem arbeiten Google und Android zusammen, wodurch viele ➢Daten von dir gesammelt werden, die alle zusammen ausgewertet werden (➢Datenschutz).

Aufgabe: Suche im Internet mal nach „freien Betriebssystemen“ (➢Open Source), die nicht mit Google zusammen arbeiten, wie zum Beispiel „Replicant“ oder „LineageOS“. Am besten machst du das zusammen mit deinen Eltern, da die Texte und Anleitungen manchmal schwer zu verstehen sind. Wenn du großen Wert auf den Schutz deiner Daten legst, solltest du jedenfalls auf Android verzichten.

Anonymität

„Anonym“ heißt, dass du nicht identifiziert werden kannst, also nicht klar erkannt und zugeordnet werden kann, wer du bist.

Im Internet, zum Beispiel in ➢Sozialen Netzwerken, kannst du oft nach außen anonym bleiben, indem du dir einen ➢Nickname zulegst und somit nicht deinen echten Namen (Klarnamen) verrätst. Dann weiß niemand, wer da schreibt. „Anonym nach außen“ ist an dieser Stelle ganz wichtig, denn wie du schon im einleitenden Kapitel über ➢Datenschutz lesen konntest, hinterlässt du beim Surfen viele Datenspuren, die zum Beispiel auf den ➢Servern der App-Betreiber landen. Deine Klassenkameraden.innen wissen dann vielleicht nicht, dass du hinter dem Namen „Mickymaus“ steckst. Die Polizei zum Beispiel kann dich aber trotzdem finden, weil deine Computeradresse (➢IP-Adresse) gespeichert wird oder deine Kontodaten, wenn du als „Mickymaus“ etwas bezahlst. Verschiedene Sicherheitseinstellungen am Smartphone, Tablet oder Computer sorgen dafür, dass du noch anonymer bleiben kannst.



Anonym zu bleiben ist sehr wichtig, denn dadurch kannst du deine ➢Privatsphäre schützen!

Wichtig: Die Anonymität im Netz kann aber auch ausgenutzt werden, um dir zu schaden. Wenn du mit jemandem chattest, kannst du dir nie sicher sein, mit wem du es zu tun hast. Besonders problematisch ist es, wenn sich viel ältere Personen als gleichaltrige ausgeben und versuchen, dein Vertrauen zu gewinnen (➢Cybergrooming). Aber auch kriminelle ➢Hacker profitieren von der Anonymität im Internet, weil sie somit nur schwer entlarvt werden können.

App-Berechtigungen

Fast jede ➢App benötigt gewisse Freigaben auf deinem Smartphone oder Tablet, für die deine Zustimmung nötig ist. So ist es beispielsweise klar, dass eine Fotobearbeitungs-App auf deine Kamera zugreifen möchte. Und WhatsApp will zum Beispiel Zugriff auf dein Telefonbuch, um Kontakte abzugleichen, Zugriff auf deine ➢GPS-Daten, wenn du deinen Standort versenden möchtest, Zugriff auf die Kamera, wenn du Fotos aufnehmen möchtest und Zugriff auf dein Mikrofon, wenn du eine Sprachnachricht verschicken möchtest.

Doch einige Apps möchten auf Funktionen zugreifen, die gar nicht notwendig sind. WhatsApp möchte beispielsweise wissen, welche anderen Apps du parallel noch nutzt. Und einige Musikerkennungs-Dienste wollen Zugriff auf deine

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

GPS-Daten, obwohl lediglich der Zugriff auf dein Mikrofon nötig wäre. Auch viele Spiele-Apps verlangen mehr Berechtigungen als nötig.

Deshalb solltest du bei jeder App vorher genau prüfen, welche Berechtigungen du mit der Installation der App erteilst. Diese werden dir angezeigt, wenn du die App aus dem Play Store oder App Store herunterladen möchtest. Du kannst auch nachträglich in den Einstellungen deines Smartphones nachschauen, welche App-Berechtigungen verlangt werden.

Bei ➢Android:

1. Wähle „Einstellungen“
2. Klicke auf „Allgemein“ oder „Optionen“
3. Wähle „Apps“ oder „Anwendungsmanager“
4. Scroll runter bis „App-Berechtigungen“

Ab der Android-Version 6.0 kannst du auch einzelne Berechtigungen ausschalten. Wenn du mit den Berechtigungen nicht einverstanden bist, solltest du die App richtig löschen.

1. Klicke auf „Cache leeren“ (➢Cache)
2. Dann auf „Daten löschen“
3. Und als letztes auf „Deinstallieren“

Wenn du in der App einen ➢Account angelegt hast, zum Beispiel bei WhatsApp oder Instagram, dann musst du diesen vorher auch löschen. Sonst löschst du nur das Programm auf deinem Gerät, aber nicht dein Benutzerprofil.

Applikation (App)

„Applikation“ (Kurz: „App“) kommt vom englischen „application software“ (➢Software). Das sind Programme oder Anwendungen, zum Beispiel für

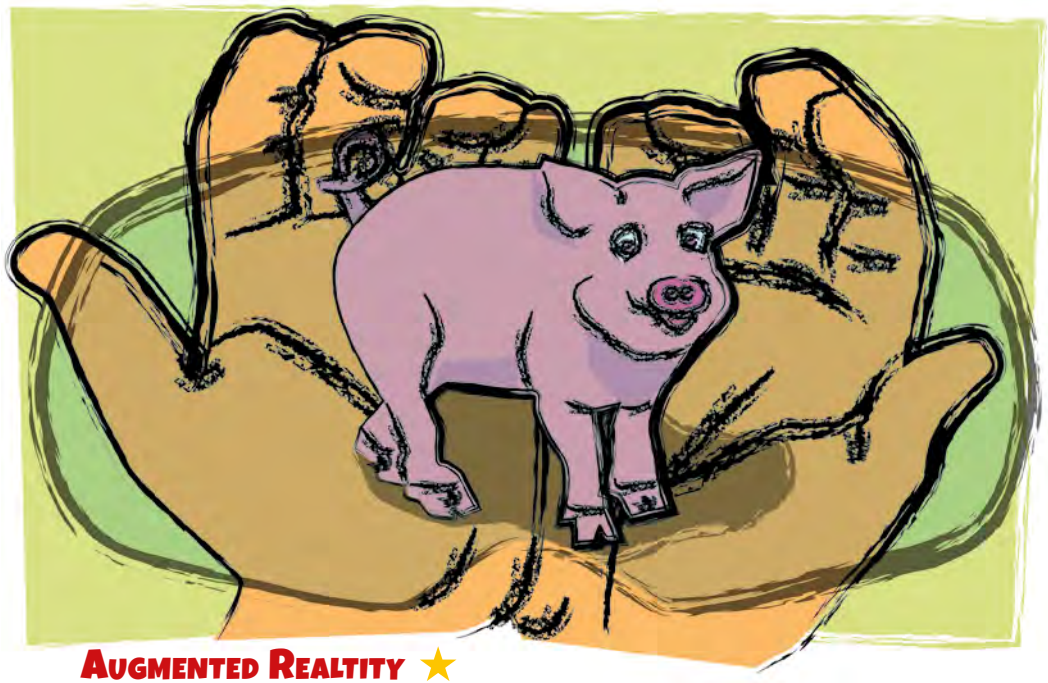
• Wetter, • Uhrzeit, • Fotobearbeitung, • Lexikon, • Radio, • Spiele, • …

Wichtig: Bei der Installation von Apps solltest du immer auf die ➢App-Berechtigungen achten. Diese zeigen an, auf welche Funktionen die App auf deinem Gerät zugreifen kann. Außerdem solltest du Apps nur aus einem vertrauenswürdigen Store (bei ➢Android, zum Beispiel „F-Droid“) für freie ➢Software, bzw. App Store (bei iOS/Apple) herunterladen. Schau dir am besten auch die Bewertungen von anderen Nutzer.innen an, bevor du eine App herunterlädst. Es kann dir zum Beispiel auch im Android Play Store passieren, dass du eine App installierst, die ➢Viren enthält. Das liegt daran, dass alle App-Entwickler ihre Apps dort hochladen dürfen und nicht alle immer auf ➢Schadsoftware überprüft werden können.

TIPP: Es gibt, wie bei jedem Produkt, das man kauft, auch bei kostenpflichtigen Apps, ein Rückgaberecht (Stand: Mai 2018). Dazu wählst du im Play Store/App Store:

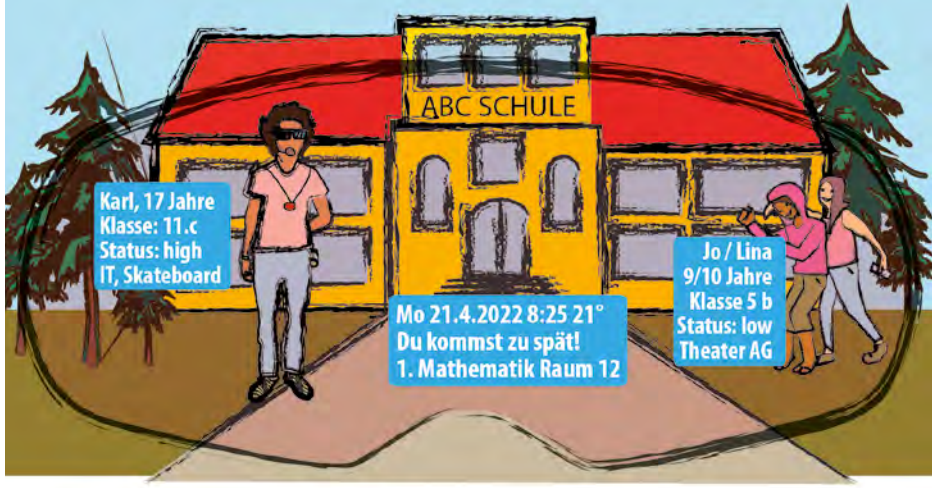
Menü > Konto > Bestellverlauf > App auswählen > Erstattung.

- Fehlerhafte Dateien oder Apps können jederzeit zurückgegeben werden.
- Spiele oder In-App-Käufe: Erstattung des Geldes innerhalb von 48 Stunden nach Kauf möglich. Nach Ablauf der 48 Stunden muss der App-Entwickler kontaktiert werden.
- Filme und Serien: Erstattung innerhalb von 14 Tagen nach Kauf, sofern sie nicht abgespielt wurden.
- Musik: Erstattung innerhalb von 7 Tagen nach Kauf, sofern sie nicht abgespielt wurden.
- e-Books: Erstattung innerhalb von 7 Tagen nach Kauf.



Augmented Realtity ★

„Augmented Reality“ (AR) bedeutet „erweiterte Realität“ (nicht zu verwechseln mit ➢virtueller Realität) und meint die Erweiterung der menschlichen Sinne mit Computertechnik. Die fünf menschlichen Sinne sind Hören, Riechen, Schmecken, Sehen und Tasten. Die meisten AR-Anwendungen beziehen sich auf den Seh-Sinn. Das Spiel „Pokémon GO“ für Smartphones ist zum Beispiel so eine



Anwendung: Die Spieler.innen schauen bei eingeschalteter Kamerafunktion durch ihr Telefon in ihre Umgebung und sehen das, was wirklich da ist, also die Realität, aber es tauchen vor der Kamera Tiere oder Figuren auf, die nicht wirklich vor der Kamera sind. Für Menschen mit Behinderung, vor allem für blinde Menschen, können verschiedene AR-Anwendungen sehr hilfreich sein, zum Beispiel wenn ihnen eine Kamera einen Busfahrplan vorliest oder erklärt, wie ihre Umgebung aussieht. Der Seh-Sinn wird dabei durch den Hör-Sinn erweitert.

Ein ganz bekanntes und umstrittenes Beispiel für eine Erweiterung des Seh-Sinns ist das ➤Wearable „Google Glass“, übersetzt die „Google-Brille“. Das Unternehmen „Google“ arbeitet seit einigen Jahren an einer Brille, die eine eingebaute Kamera und ein Mikrophon hat und mit dem Internet verbunden ist. Im Grunde genommen ist sie ein kleiner Computer auf der Nase. Sie lässt sich durch Augenbewegungen, Kopfbewegungen und Sprachbefehle steuern und sieht aus wie eine Mischung aus einer normalen Brille, einem Haarreifen und einem Headset, das man verwendet, um freihändig zu telefonieren. Die Brille kann den Menschen, die sie tragen, verschiedene Informationen vor den Augen anzeigen, zum Beispiel Informationen zu Bauwerken, die Online-Profile von Personen oder Navigationshinweise, um einen Weg zu finden. Datenschützer.innen haben das Gerät sehr schnell als gefährlich eingestuft, da die Brille vor allem heimliche Videoaufnahmen ganz leicht möglich macht oder unbemerkt Gespräche aufzeichnen kann. Außerdem kann das Unternehmen, das ohnehin schon sehr viele ➤Daten von Menschen sammelt, mit der Brille noch viel besser Daten über die Person sammeln, die die Brille trägt (Bewegungsprofile, Interessen und so weiter).

AUFGABE: Stell dir mal vor, du unterhältst dich mit einer Person, die so eine Datenbrille trägt. Wie geht es dir dabei? Was könnte die Brille über dich anzeigen? Was wäre, wenn die Brille die ganze Zeit filmen würde? Oder wenn dein Gegenüber vielleicht gerade gar nicht zuhört und ein Video anschaut? Schreibe deine Gedanken dazu auf.

Backup

Ein „Backup“ ist eine Sicherungskopie, zum Beispiel von Dateien und Programmen. Wenn du deine ➤Daten lokal auf einem Gerät speicherst, also nur auf dem Gerät und nirgendwo anders, dann gehen diese Daten natürlich verloren, wenn das Gerät mal kaputt ist. Eine Sicherungskopie, zum Beispiel auf einer CD, einem USB-Stick, einer externen Festplatte (über USB angeschlossene Speicherplatte) oder in einer ➤Cloud, sorgt dafür, dass deine Daten zusätzlich an einer anderen Stelle gespeichert werden. Doch bei Backups in einer Cloud, also der Sicherung von Dateien im Internet, solltest du vorsichtig sein. Es sollte eine Cloud sein, in der deine Daten gut geschützt sind, sowohl vor Außenstehenden (mit Passwort) als auch vor den Anbietern der Cloud.

Benutzerkonto

„Benutzerkonto“ oder „Benutzerprofil“ ist das deutsche Wort für ➤Account.

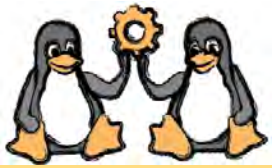
Betriebssystem

Ein „Betriebssystem“ sorgt dafür, dass dein Gerät überhaupt arbeitet, denn das Betriebssystem ist quasi der Übersetzer zwischen der Grafik-Karte im Gerät (damit Bilder und Texte angezeigt werden können), der Sound-Karte im Gerät (damit Töne abgespielt werden können), der Festplatte (auf der ➤Daten gespeichert werden) und jeder anderen ➤Hardware, die in deinem Smartphone oder Computer verbaut ist.

Die bekanntesten Betriebssysteme für Mobilgeräte sind derzeit:

- ➤Android (bei den meisten Geräten, zum Beispiel bei den Marken „HTC“, „LG“, „Samsung“, ...)
- iOS (bei Geräten der Marke „Apple“)
- Windows Phone (meistens bei Geräten der Marke „Microsoft“, doch die Entwicklung wurde 2017 eingestellt).

Für Computer und Laptops gibt es noch diverse andere Betriebssysteme, doch zum Schutz deiner persönlichen Daten solltest du keines der „großen Firmen“ nutzen (zum Beispiel kein „Windows“), sondern stattdessen beispielsweise das freie Betriebssystem ➤„Linux“ verwenden (➤Open Source).



AUFGABE: Wie man Linux installiert, kannst du zum Beispiel bei so genannten „Crypto-Partys“ oder „Linux-Intsall-Partys“ lernen. Das sind Veranstaltungen, bei denen Expert.innen anderen Leuten dabei helfen ihre Geräte datenschutzfreundlich einzustellen – in lockerer Atmosphäre, deshalb „Party“. Meistens kannst du deine Geräte (Smartphone, Laptop und so weiter) einfach mitbringen. Bei Crypto-Partys kannst du zum Beispiel auch lernen wie E-Mail-Verschlüsselung funktioniert. Recherchier doch mal, ob in deiner Nähe Crypto-Partys angeboten werden.

Big Data

Big Data ist ein Sammelbegriff für eine sehr große Menge an Daten. Der Begriff wird häufig eingesetzt, um alle ➢Daten der Menschen zu bezeichnen, die produziert, ➢digital gesammelt, analysiert und verwertet werden. Die Datenmengen sind dabei so groß, dass sie nur von Computerprogrammen mit speziellen ➢Algorithmen ausgewertet werden können, denn Menschen schaffen das in diesem Ausmaß nicht.

Ein kleiner Überblick, welche Daten wo von dir gesammelt werden:

- Zuhause (durch angeblich ➢„smarte" Haushaltsgeräte, die an das Internet angebunden sind, zum Beispiel Smart TV, Licht- und Heizungssteuerung durch das Smartphone, sowie internetfähiges Spielzeug, ...).
- Durch Geräte, die du bei dir trägst (Smartphone, Fitnessarmbänder, Smart Watch und andere ➢Wearables).
- In ➢Sozialen Netzwerken (Profileinträge, Chatverläufe, Fotos, ➢Metadaten, ...).
- Durch Überwachungskameras im öffentlichen Raum (Straßenbahnen, Bahnhöfe, Parks, Schulen, Supermärkte, ...).
- Durch die Nutzung von Chipkarten wie Kreditkarten und Kundenkarten (von Bekleidungsläden, Supermärkten, Drogerien oder PayBack). Auch im Personalausweis oder in Kleidung befinden sich sogenannte ➢RFID-Chips, die per Funk ausgelesen werden können.
- Und natürlich bei allen Online-Aktivitäten (beim Surfen, Online-Shopping, Musik hören, Banking und so weiter).

Ein kleines Gedankenexperiment zur Verknüpfung dieser verschiedenen Datenquellen findest du im Beitrag ➢Internet der Dinge.

AUFGABE: Mach dir mal einen Tag lang, vom Aufstehen bis zum Schlafengehen, bewusst, welche Daten von dir gesammelt werden und schreibe diese auf. Oder du kannst alle Kameras, an denen du vorbei kommst, und alle Geräte, die zum Beispiel dein Busticket auslesen, fotografieren. Danach solltest du dir überlegen, was du tun kannst, um deine Daten zu schützen.

Blog

Ein „Blog" (auch „Weblog") ist eine Art Online-Tagebuch oder Journal (wie ein Magazin oder Notizbuch). **#Kids #digital #genial** (www.kidsdigitalgenial.de) ist zum Beispiel auch ein Blog, da auf der Startseite immer wieder News (Neuigkeiten) dazukommen, ähnlich wie bei einer Online-Zeitung. Die Leute, die einen Blog betreiben, nennt man „Blogger".

Bluetooth

„Bluetooth" ist ein Funkstandard, der es ermöglicht, ➢Daten zwischen Geräten auszutauschen. Früher durften die Geräte nur maximal 100 Meter voneinander entfernt sein, denn weiter reichte das Signal nicht. Oft wird diese Verbindung für kabellose Kopfhörer, Lautsprecher oder für Freisprechanlagen in Autos genutzt.

Wichtig: Wenn die Bluetooth-Funktion eingeschaltet ist, bietest du anderen Geräten in einem gewissen Radius die Möglichkeit zum Datenaustausch. Dadurch gibst du auch kriminellen ➢Hackern die Möglichkeit, auf dein Gerät zuzugreifen. Du kannst allerdings in den Einstellungen auf deinem Gerät auch einstellen, dass für andere nicht sichtbar ist, wenn deine Bluetooth-Verbindung aktiv ist.

TIPP: Bluetooth braucht Strom. Wenn du die Bluetooth-Verbindung ausschaltest, dann sparst du auch Akku-Kapazität.

Browser

Einen „Browser" (oder auch „Webbrowser") benötigst du, um Internetseiten des ➢World Wide Web (WWW) aufrufen zu können. Dort sind Funktionen enthalten wie zum Beispiel „vor", „zurück", „Lesezeichen anlegen", „Suche" und viele weitere Funktionen, die du benötigst, um auf einer ➢Webseite surfen zu können.

Die bekanntesten Browser sind derzeit

- Google Chrome
- Apple Safari
- Mozilla Firefox
- und Internet Explorer.

Doch diese speichern oft viele ➢Daten über dein Surfverhalten. **Du solltest in deinem Browser unbedingt einige Einstellungen zum Schutz deiner Daten (➢Datenschutz) und ➢Privatsphäre vornehmen:**

1. Stell ein, dass keine Chronik angelegt wird, denn diese speichert alle Suchbegriffe, die du eingibst, und Seiten, auf denen du gesurft hast.
2. Deaktiviere die ➢Cookies, denn sie speichern ebenfalls Informationen über dein Surfverhalten.
3. Installiere ein ➢Plug-in, das Werbung blockiert, am besten „uBlock Origin".
4. Speicher deine Passwörter nicht im Browser, denn sonst können womöglich andere von deinem Gerät auf deine ➢Accounts zugreifen. Auch für kriminelle ➢Hacker ist es deutlich einfacher, an deine Passwörter zu kommen, wenn sie gespeichert sind.
5. Installiere das Plug-in „NoScript", um ➢Tracking zu vermeiden.
6. Wenn du ganz sicher gehen willst, dass du beim Surfen anonym bleibst (➢Anonymität), solltest du keinen der genannten Browser nutzen, sondern den „Tor-Browser". Ansonsten bietet der „Firefox" in Bezug auf Datenschutzeinstellungen die beste Variante.

Browser-Einstellungen am Smartphone oder Tablet (Firefox):

1. Öffne deinen Browser („Internet“) und klicke auf die Menü-Taste (meist links unter dem Display).
2. Klicke auf „Einstellungen“.
3. Anschließend auf „Datenschutz und Sicherheit“.
4. Setze ein Häkchen bei „Sicherheitswarnungen anzeigen“.
5. Entferne das Häkchen bei „Cookies akzeptieren“.
6. Formulardaten solltest du ebenfalls nicht speichern (zum Beispiel wenn du Felder ausfüllen musst mit deinem Namen, Alter, Adresse und so weiter).
7. Entferne das Häkchen bei „Standortzugriff aktivieren“, (➤Standortdaten) damit keine ➤GPS-Ortung möglich ist.
8. Entferne das Häkchen bei „Passwörter merken“.

Cache

Der „Cache“ ist ein Speicher, in dem verschiedene ➤Daten zwischengelagert werden. So ist es beispielsweise möglich, dass eine aufgerufene Internetseite beim zweiten Aufruf nicht mehr so lange zum Laden braucht wie beim ersten Aufruf.

Auch wenn dies natürlich auf den ersten Blick ein Vorteil für dich ist, werden hier trotzdem sensible Daten gespeichert, die du im Hinblick auf ➤Datenschutz und ➤Privatsphäre regelmäßig löschen solltest. Den Cache kannst du in den Einstellungen deines ➤Browsers oder in den Einstellungen deiner ➤App löschen.

Clickbaiting ★

Clickbaiting bedeutet „Klickköder“ („bait“ = Köder). Damit ist ein Verkaufs- und Verbreitungs-Trick gemeint, um möglichst viele Klicks für Fotos, Artikel und andere ➤Links im ➤Web zu bekommen und somit eine ➤virale Verbreitung zu erzielen. Dazu werden meistens Überschriften gewählt, die besonders neugierig machen sollen, wie zum Beispiel „Das musst du unbedingt lesen!“ oder „Was dieser Frau passiert ist, ist unglaublich!“. Meistens sind die Inhalte dahinter längst nicht so interessant, wie die Überschrift glauben lässt. Aber du wirst damit auf Seiten geleitet, die sehr viel ➤Online-Werbung enthalten, oder auf Gewinnspielseiten, oder Seiten, auf denen ➤Newsletter abonniert werden sollen. Manchmal verbergen sich Schock-Videos hinter den Links, die keinen anderen Sinn haben, als Angst zu verbreiten, so wie bei gruseligen ➤Kettenbriefen. Ein weiterer Trick des Clickbaitings sind bunt leuchtende oder blinkende Überschriften und Pfeile, die dazu verleiten sollen, einen Link anzuklicken. Diese Masche begegnet dir ganz besonders auf Facebook und in anderen ➤Sozialen Netzwerken, da dort viele Menschen unterwegs sind, die diese Links weiterverbreiten oder „teilen“, wie es in vielen Sozialen Netzwerken genannt wird.

Wichtig: Seriöse, also ernst zu nehmende und professionelle Journalist.innen und Redakteur.innen haben Clickbaiting bislang oft als unprofessionell eingestuft. Sie schreiben zwar auch interessante Überschriften, damit die Texte gelesen werden, aber sie bringen meistens schon in der Überschrift Informationen unter, die klar erkennen lassen, um was es in dem Artikel gehen soll. Andererseits begegnet man auch in professionellen Medien immer häufiger solchen „geheimnisvollen“ Überschriften, was keine gute Entwicklung ist.

Client

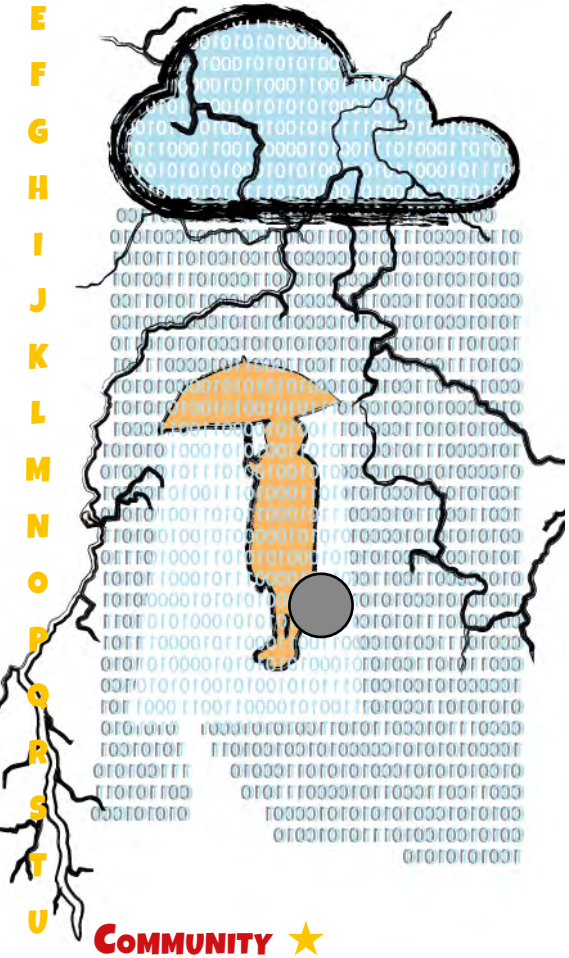
Ein „Client“ (Deutsch: „Kunde“) ist eine ➤Software, also ein Computerprogramm, die mit einem ➤Server kommuniziert und somit Daten überträgt. Ein Client speichert also selbst keine Daten, sondern ermöglicht den Zugriff zu einem Server, auf dem Daten gespeichert werden.

Cloud

Eine „Cloud“ (Deutsch: „Wolke“) ist ein Speicherplatz im Internet. Wenn du zum Beispiel Fotos, Videos oder Musik auf deinem Gerät speicherst, dann ist dein lokaler Speicherplatz, also der Speicherplatz auf deinem Gerät, irgendwann voll. Wenn du deine ➤Daten in einer Cloud speicherst (dafür brauchst Du einen Internet-Zugang), dann sind diese nicht auf deinem Gerät gespeichert, sondern auch von anderen Geräten abrufbar. Das Gute ist, dass du deine Daten dann von jedem Gerät mit Internetzugang abrufen kannst, egal wo du gerade bist. Meistens legst du dir dazu einen ➤Account an und kannst dich dann von überall einloggen (➤Login) und auf deine gespeicherten Daten zugreifen.

Wichtig: Natürlich schweben deine Daten nicht wirklich in einer Wolke in der Luft herum, sondern werden auf riesigen ➤Servern irgendwo anders in der Welt abgespeichert. Diese Cloud-Server sind bei verbrecherischen ➤Hackern besonders beliebt, weil sie dort viele Daten

abgreifen können, wenn es ihnen gelingt, in das System einzudringen. Das Passwort, das du für deinen Account bei einem Cloud-Dienst nutzt, sollte deshalb möglichst sicher sein. Außerdem sind deine Daten ab dem Moment, wo du sie in der Cloud speicherst, nicht mehr wirklich privat, denn zumindest die Menschen, die an diesen Servern arbeiten, können deine gespeicherten Daten abrufen. Gerade bei Fotos kann es ein unangenehmes Gefühl sein, zu wissen, dass auch andere diese sehen können.

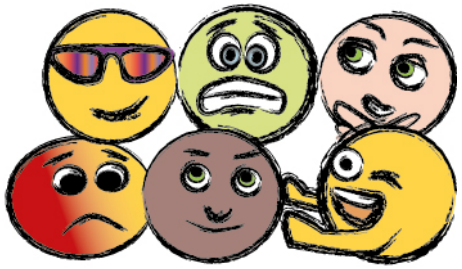


Zwei der bekanntesten Clouds sind „Dropbox“ und „Google Docs“, doch hier gibt es einige Lücken im ➤Datenschutz, deshalb solltest du lieber eine andere Cloud nutzen. Sicherer ist es jedoch für dich, wenn du ganz auf Cloud-Dienste verzichtest. Statt dessen kannst du deine Daten zum Beispiel mit der App „SyncThing“ verschlüsselt auf einem Computer speichern, der bei dir Zuhause oder bei dir bekannten Leuten steht.

AUFGABE: Auch in der Schule werden oft Clouds genutzt, um Bücher, Texte, Hausaufgaben, Fotos und so weiter auszutauschen. Versuch doch mal deine Klassenkamerad.innen von einer sicheren und verschlüsselten Cloud-Variante zu überzeugen. Wenn ihr alle an einem Strang zieht, könnt ihr euch gemeinsam für den Schutz eurer Daten stark machen!

Community ★

„Community“ ist das englische Wort für „Gemeinschaft“. Das Wort begegnet dir wahrscheinlich oft in ➤Sozialen Netzwerken und Foren (➤Forum), denn dort kommen viele verschiedene Personen aus der ganzen Welt zusammen, die eine Gemeinschaft bilden.



Cookie

„Cookies“ (Deutsch: „Kekse“) speichern Daten über dein Surfverhalten. Sie helfen, dich zu identifizieren, also klar zuzuordnen, dass du es bist, der/die gerade auf der Webseite surft. Mit ➤Anonymität, ➤Privatsphäre oder ➤Datenschutz hat das also nicht viel zu tun.
Wenn Du das Speichern von Cookies nicht ausgeschaltet hast (was du am besten tun solltest), dann solltest du sie regelmäßig in den Einstellungen deines ➤Browsers löschen. Den Firefox kann man zum Beispiel so einstellen, dass er beim Beenden alle Cookies löscht.

Copyright ★

„Copyright“ ist das englische und amerikanische Wort für ➤„Urheberrecht“. Es gibt ein eigenes Zeichen dafür, nämlich den Buchstaben „C“ in einem Kreis, der darauf hindeutet, dass das Recht an einem Bild oder Text jemandem gehört und nicht ohne Erlaubnis kopiert werden darf.
Für musikalische Werke wird ein „P“ in einem Kreis verwendet, welches für „Phonogram“ also „Ton“ steht. In Deutschland haben diese Zeichen aber keine Bedeutung, da es ausführliche Urheberrechtsgesetze gibt, die eingehalten werden müssen, egal ob das Werk mit diesem Symbol gekennzeichnet ist oder nicht.

AUFGABE: Das Zeichen kann ganz einfach über die Computertastatur eingefügt werden. Wenn du das ➤Betriebssystem „Windows“ auf dem Computer installiert hast, dann musst du die Taste „Alt“ gedrückt halten und zusätzlich auf dem Ziffernblock der Tastatur die Tasten 0, 1, 6 und 9 (hintereinander) drücken. Danach kannst du die „Alt“-Taste wieder loslassen. Im Textverarbeitungsprogramm „Microsoft Word“ funktioniert die Tastenkombination [Alt Gr] + [C]. Wenn du „iOS“, also „Apple“, nutzt, dann musst du [Alt] + [G]“ drücken. Bei ➤„Linux“ ist es meistens [Alt Gr] + [Shift] (das ist die Großschreib-Taste) + [C]. Probier es aus!

Creative Commons

„Creative Commons“ (Deutsch: „kreatives Volk“) ist eine gemeinnützige Organisation, die sich um Künstler.innen wie Fotograf.innen, Musiker.innen und Autor.innen kümmert. Diese stellen ihre Fotos, Musik und Texte frei für alle Menschen zur Verfügung, ohne Geld dafür zu verlangen. Sie können dabei die Bedingungen selbst festlegen, indem sie folgende Fragen beantworten: Soll mein Name bei dem Werk veröffentlicht werden? Darf das Werk verändert werden? Darf das Werk zum Geldverdienen oder für Werbung verwendet werden? Und wie soll

das Werk weiter gegeben werden? Es gibt dafür verschiedene Creative-Commons-Lizenzen:

- **CC BY** (by heißt „von") – Verbreitung und Veränderung des Werks erlaubt, auch wenn damit Geld verdient wird oder Werbung gemacht wird, aber der Name des Urhebers muss genannt werden.
- **CC BY-SA** (sa steht für „share alike" und heißt „Teilen zu gleichen Bedingungen") – die Verbreitung und Veränderung des Werks ist erlaubt, auch wenn damit Geld verdient wird oder Werbung gemacht wird, aber der Name des Urhebers muss genannt werden. Wenn das Werk verändert und verbreitet wurde, muss wieder die CC BY-SA-Lizenz vergeben werden.
- **CC BY-ND** (nd steht für „no derivates" und bedeutet „keine Veränderung") – die Verbreitung des Werks ist erlaubt, auch wenn damit Geld verdient wird oder Werbung gemacht wird, aber der Name des Urhebers muss genannt werden und man darf das Werk nicht verändern.
- **CC BY-NC** (nc steht für „non commercial" und bedeutet „nicht-kommerziell") – die Verbreitung und Veränderung des Werks ist erlaubt, aber nicht, wenn damit Geld verdient oder Werbung gemacht wird. Der Name des Urhebers muss genannt werden.)
- **CC BY-NC-SA** (die Verbreitung und Veränderung des Werks ist erlaubt, aber nicht, wenn damit Geld verdient wird oder Werbung gemacht wird. Der Name des Urhebers muss genannt werden. Wenn das Werk verändert und verbreitet wurde, muss wieder die CC BY-NC-SA-Lizenz vergeben werden.)

- **CC BY-NC-ND** (Verbreitung des Werks erlaubt, aber nicht wenn damit Geld verdient wird oder Werbung gemacht wird. Der Name des Urhebers muss genannt werden und es ist keine Veränderung des Werks erlaubt.)
- **CC0 = Public Domain** (Es ist nicht nötig eine Quelle oder einen Namen anzugeben, denn die Urheber treten ihr ➤Urheberrecht ab. Sie schenken es teilweise bewusst, teilweise unwissentlich der öffentlichen Gemeinschaft. Das Werk gehört somit nicht mehr ihnen und sie können nicht bestimmen, was damit passiert. Auch die Angabe dieser Lizenz ist rechtlich nicht nötig.)
- **Public Domain Mark** (Damit markiert man Werke, die sich schon in der „Public Domain" befinden, also gemeinfrei sind.)

Die letzten beiden Lizenzen (CC0 und Public Domain Mark), fallen nicht mehr so ganz in den Bereich der CC-Lizenzen, da sie komplett auf Namensnennungen verzichten.

Cybergrooming

„Cybergrooming" bezeichnet die erste Stufe der Anmache im Internet („grooming"= anbahnen, vorbereiten) mit dem Ziel, eine Straftat zu begehen, wie zum Beispiel sexuellen Missbrauch oder um (kinder)pornographisches Material zu bekommen. Meist erfolgt diese Anmache durch Schmeicheleien im Chat und das langsame Aufbauen einer Vertrauensbasis von Personen, die sich ein falsches Profil angelegt haben, also sich als jemand anderes ausgeben (falscher Name, falsches Alter, falsche Fotos,...). Oft handelt es sich dabei um ➤Pädophile. Als nächstes verlangt die Person häufig Fotos, Videochats oder ein persönliches Treffen. Trau dich, das Gespräch zu beenden, wenn dir etwas komisch vorkommt.

Aufgabe: Sprich mit deinen Freundinnen und Freunden oder deinen Geschwistern darüber, ob sie so etwas schon einmal erlebt haben. Oft muss nur einer den Anfang machen, damit man sich traut, darüber zu reden. Ihr solltet euch gemeinsam stärken und vielleicht überlegen, ob ihr erwachsene Personen um Hilfe bittet. Cybergrooming ist eine Straftat, kein Spaß!

Cybermobbing

„Cybermobbing" bezeichnet die Schikane und Ausgrenzung von Personen über technische Geräte, vor allem über das Internet (zum Beispiel in ➤Sozialen Netzwerken). Die Angriffe finden über E-Mail oder SMS, durch lästige Anrufe, in Chats, ➤Foren, ➤Blogs und auf Foto- oder Videoplattformen statt. Cybermobbing hat verschiedene Erscheinungsformen, dazu gehören zum Beispiel Beleidigung/Beschimpfung, (sexuelle) Belästigung, sozialer Ausschluss oder ➤Stalking.

Oft werden unerlaubt unvorteilhafte oder peinliche Fotos oder Videos verbreitet, womit das ➤Recht am eigenen Bild verletzt wird.

Cybermobbing unterscheidet sich von „normalem" Mobbing durch verschiedene Kriterien:

- **Ausgrenzung:** Durch die Möglichkeit, sich in Sozialen Netzwerken und Chats zu Gruppen zusammen zu schließen, ist es auch viel einfacher möglich, jemanden mit wenigen Klicks aus einer Gruppe auszuschließen.

- **Schnelle Verbreitung von Fotos/Videos/Nachrichten:** Mit nur wenigen Klicks können zum Beispiel peinliche Fotos, an viele andere verschickt werden. Die Verbreitung ist oft kaum zu stoppen.
- **Anonymes, großes Publikum:** Es ist nicht zu überblicken, wer bereits an dem Mobbing beteiligt ist oder wer gewisse Inhalte bereits gesehen/gelesen hat.
- **Es hört nicht auf:** Auch wenn die technischen Geräte ausgeschaltet werden, läuft das Mobbing trotzdem weiter. Wird zum Beispiel das Smartphone ausgeschaltet, so werden die Nachrichten zugestellt, sobald das Gerät wieder eingeschaltet wird. Und die Verbreitung von Beleidigungen und Fotos läuft im Hintergrund trotzdem weiter. Cybermobbing findet also 24 Stunden, 7 Tage die Woche statt.

Die Gründe für Cybermobbing sind sehr vielfältig und oft total banal. Oft reicht es aus, dass man etwas „anders" ist als die anderen (zum Beispiel Haarfarbe, Hautfarbe, Gewicht, Religion, Kleidung, ...). Aber es kommt auch vor, dass jemand nur aus Langeweile anfängt, andere zu mobben. Manche Mobber.innen ärgern andere auch nur, um selber nicht gemobbt zu werden. Deshalb gibt es beim Mobbing auch oft sogenannte „Mitläufer", die nur mitziehen, um nicht selber in die Schusslinie zu geraten. Ganz schlimm ist allerdings auch die Gruppe der Zuschauer. Denn sehr viele Leute bekommen das Mobbing mit, aber tun nichts dagegen. Manchmal werden Mobbingfälle auch nicht so ernst genommen, weil viele Kinder „normalen" Streit schon als Mobbing bezeichnen. Es sollte aber vorsichtshalber jeder Fall ernst genommen werden.

Was du unbedingt tun solltest, wenn dich jemand über fiese Nachrichten oder mit Bildern mobbt:

1. Bleib ruhig! – Nimm es dir nicht zu Herzen!
2. Blockiere den Mobber! (zum Beispiel in Sozialen Netzwerken)
3. Sichere Beweise! (zum Beispiel durch Screenshots)
4. Hol dir Hilfe! – Alleine geht es nicht! Wende dich am besten an eine erwachsene Person.

Darknet

Das Darknet (übersetzt: Dunkles Internet) ist ein Teil des Internets, der nicht für jede.n zugänglich ist. Internetseiten, die im Darknet abgelegt sind, sind zum Beispiel nicht über herkömmliche ➢Suchmaschinen zu finden, denn die Inhalte werden verschlüsselt und extra so auf ➢Servern gespeichert, dass nicht nachvollziehbar ist, wo diese ➢Daten gespeichert sind. Dazu wird die ➢IP-Adresse verschleiert, indem Daten beispielsweise über viele verschiedene Server geschickt und umgeleitet werden. Wenn nicht klar ist, wo die Daten gespeichert sind, können sie auch nicht so leicht aufgerufen werden, denn ein Server, bzw. ➢Client weiß dann ja nicht, mit welchem anderen Server er Kontakt aufnehmen soll. Auch andere Daten, die normalerweise beim Surfen preisgegeben werden (➢Metadaten), werden im Darknet nicht gespeichert. Das Darknet kann auch nicht über die „normalen" ➢Browser aufgerufen werden, sondern nur über spezielle Zugänge.

Das Darknet ermöglicht somit anonymes Surfen im Internet (➢Anonymität), was sowohl Vorteile als auch Nachteile hat: Zum einen können Menschen den versteckten Teil des Internets nutzen, um ihre Meinung frei zu äußern, ohne dafür bestraft zu werden. In den meisten Ländern wird man für seine eigene Meinung nicht bestraft, aber es gibt auch ein paar Länder, in denen Menschen verfolgt werden, wenn sie ihre Meinung sagen. Besonders für Journalist.innen und Personen, die sich politisch engagieren, hat die Nutzung des Darknets viele Vorteile. Aber auch Kriminelle, die zum Beispiel mit Waffen oder Drogen handeln wollen, nutzen die Anonymität aus. Das heißt jedoch noch lange nicht, dass sich jeder ganz einfach eine Waffe im Darknet kaufen kann, denn die einzelnen Netzwerke sind ja nicht öffentlich und wer in solch ein geschlossenes Netzwerk aufgenommen werden will, muss meist auf anderen Wegen zu den Personen dort Kontakt haben.

Datenbank

Eine Datenbank ist ein ➢EDV-System, in dem verschiedenste Daten gespeichert, geordnet, kategorisiert und auch verarbeitet werden.

Beispiel: In einer Datenbank eines Online-Shops werden zum Beispiel Informationen über den Käufer gesammelt (Adresse, Telefonnummer und so weiter), aber auch über die bestellten Produkte und noch viel mehr. Wenn man

eine bestimmte Information sucht, kann es ewig dauern, bis man diese gefunden hat. Deshalb kann man innerhalb dieser Datenbank die Suche eingrenzen, zum Beispiel „alle Personen, die das rote T-Shirt bestellt haben“ oder „alle Personen die in Berlin wohnen“ oder „alle Kunden, die noch nicht bezahlt haben“ und so weiter.

AUFGABE: Du solltest mal überlegen, bei welchen Diensten du überall angemeldet bist, sowohl im Internet (zum Beispiel in ➤Sozialen Netzwerken und Online-Shops) als auch außerhalb des Internets (zum Beispiel beim Arzt) und in wie vielen Datenbanken persönliche Daten von dir hinterlegt sind. Wahrscheinlich bist du überrascht, wie viele Datenbanken da zusammen kommen. Nun kannst duentscheiden, ob du in Bezug auf ➤Datenschutz etwas dagegen unternimmst. Die verknüpften Daten in Datenbanken und Analysen dieser Daten sind natürlich auch für ➤Drittanbieter sehr interessant, deshalb solltest du sichergehen, dass deine Daten nicht verkauft werden. Dafür solltest du dir die ➤Allgemeinen Geschäftsbedingungen (AGB) der Anbieter genau ansehen.

Digital

„Digital“ (Gegenteil von „analog“) ist zunächst ein technischer Begriff. Digitalisierung heißt, dass ➤Daten wie zum Beispiel Texte, in eine Ansammlung von Nullen und Einsen übersetzt werden, die von allen Computern gelesen werden können.

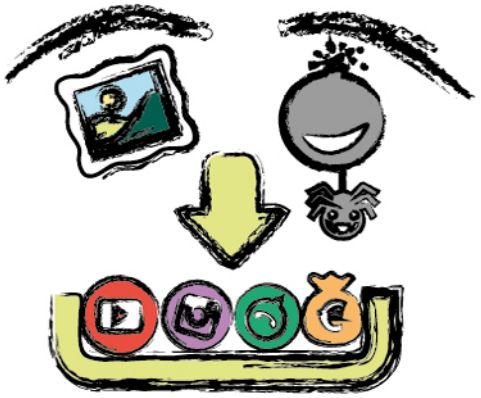
Digitale Technik bezeichnet die Übertragung von elektronischen Signalen, die nur in genau dem Zeitpunkt übermittelt werden, indem sie gebraucht werden. Diese Signale sind stark vereinfacht, sodass sie mit Maschinen sehr schnell verarbeitet werden können und gut für die Speicherung und Verarbeitung von unterschiedlichsten Daten/Informationen geeignet sind.

Die Umwandlung von Analogem zu Digitalem nennt sich Digitalisierung. Digitalisierte Daten werden durch Zeichen über ein elektronisches Gerät, meistens über einen Computer, dargestellt und dafür wird immer Strom (oder ein Stromspeicher wie Batterie oder Akku) benötigt. Dazu einige Beispiele:

- Ein handgeschriebener Text (analog) wird in den Computer eingetragen und gespeichert. Das heißt: Der Text wurde digitalisiert.
- Ein gedrucktes Buch ist analog, ein e-Book ist digital.
- Der Sensor in einem Thermometer misst die Temperatur (analog), welche danach in Zahlen auf einem Display angezeigt wird (digital).
- Die Armbanduhr, die dir auf einem Display 15:23 Uhr anzeigt ist digital, eine Armbanduhr mit Ziffernblatt und Uhrwerk ist analog.
- Ein Foto, das im Fotoalbum klebt, ist analog, ein Foto auf dem Computer, Smartphone oder Tablet ist digital.

AUFGABE: Geh mal zu Hause durch eure Wohnung und schau nach, welche Dinge analog und welche digital funktionieren. Wie würde dann die jeweils andere Variante dazu aussehen? Wie funktioniert zum Beispiel euer Radio? Digital oder analog? Auch wenn die Anzeige digital ist, kommt das Signal vielleicht doch aus einer analogen Antenne?

Download



Etwas „downloaden“ (englisches Wort, das eingedeutscht wurde) bedeutet übersetzt „herunterladen“. Du speicherst dabei eine Datei auf deinem Gerät, die vorher noch nicht dort gespeichert war, sondern auf einem externen ➤Server.

Wichtig: Sobald du eine Datei (zum Beispiel ein Foto, ein Lied oder ein Programm) heruntergeladen hast, ist sie in deinem Besitz. Aber nicht jeder Download ist erlaubt. **Nur weil jemand die Datei zum Herunterladen anbietet, heißt es noch nicht, dass du sie auch besitzen darfst.** Manchmal hättest du zum Beispiel dafür bezahlen müssen. Technisch lässt sich meistens nachvollziehen, wer die Datei heruntergeladen hat und in solchen Fällen drohen dir zum Beispiel hohe Geldstrafen, deshalb solltest du immer genau überprüfen, ob der Download erlaubt/legal ist. Du kannst dir als Faustregel merken, dass aktuelle Musik und Filme in den seltensten Fällen kostenfrei heruntergeladen werden dürfen, denn die Urheber/Macher ➤Urheberrecht möchten ja Geld damit verdienen und ihre Werke deshalb verkaufen.

Außerdem kann es schnell passieren, dass du dir ➤Schadsoftware herunter lädst, deshalb solltest du dir sicher sein, dass du die Datei von einer vertrauenswürdigen Seite beziehst. Bei kostenlosen Downloads ist die Wahrscheinlichkeit, dass du dir zum Beispiel einen ➤Virus herunter lädst, zwar höher als bei bezahlten Downloads, aber auch da ist es nicht ausgeschlossen.

TIPP: Für Musik und Filme gibt es viele Angebote im Internet, bei denen du keine Datei herunterladen musst und dir zum Beispiel trotzdem den Film angucken darfst, zum Beispiel bei Internetradios, Videoplattformen wie YouTube oder ➤Streaming-Portalen.

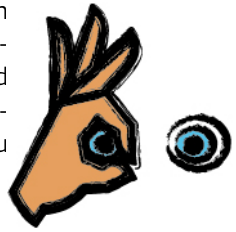
Drittanbieter

Ein „Drittanbieter“ oder „Fremdanbieter“ ist eine Person oder ein Unternehmen, das dir ein Produkt oder einen Service anbietet, obwohl du meistens nicht explizit darum gebeten hast. Am leichtesten lässt es sich anhand von Werbung im Internet erklären:

Du surfst auf einer Internetseite über Haustiere und bekommst beispielsweise in einem Werbebanner Angebote für Schuhe aus einem bestimmten Laden angezeigt. Dieser Laden, bzw. das Unternehmen, ist dann der Drittanbieter.

Drittanbieter sind immer an Informationen über dich interessiert, denn so erfahren sie, was dir gefällt und was sie dir anbieten sollen, damit sie mehr verkaufen können. Im Internet können sie sehr viel über dich erfahren, denn dein Surfverhalten sagt sehr viel über dich aus: Auf welchen Seiten du surfst und welche Suchbegriffe du eingibst, was dir gefällt (besonders einfach ist dies zu analysieren, wenn du in ➤Sozialen Netzwerken den „Gefällt-mir-Button“ drückst), welche Produkte du als letztes gekauft hast (dadurch verrätst du zum Beispiel nebenbei auch, ob du viel oder wenig Geld hast), ob du männlich oder weiblich bist oder wie alt du bist. Und die Drittanbieter zahlen, wenn nötig, sogar Geld (zum Beispiel an die Anbieter von Sozialen Netzwerken), um ➤Daten über dich zu bekommen.

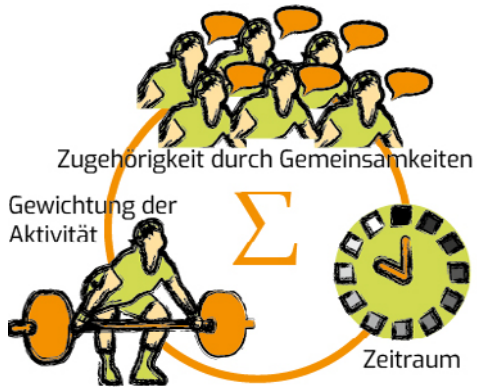
Wichtig: Mit Hilfe dieser Daten können sie sogenannte ➤„personalisierte Werbung“ schalten, also Angebote von Produkten, die dich besonders ansprechen, weil sie auf deine Person und deine Interessen zugeschnitten sind. Auch wenn das zunächst nach einem Vorteil für dich klingt: Das ist es nicht! Denn es sind deine persönlichen Daten und du darfst selbst bestimmen, wer diese Daten von dir erhält. **Du musst deine Daten schützen und deshalb darauf achten, dass deine Persönlichkeit nicht von Fremden analysiert wird** (➤Datenschutz). Wenn du Angebote im Internet nutzt, dann solltest du dir immer die ➤Allgemeinen Geschäftsbedingungen (AGB) durchlesen, denn darin steht meistens drin, wenn deine Daten an Drittanbieter verkauft werden. Sobald du die AGB akzeptierst, stimmst du dem zu.



EdgeRank

Der „EdgeRank“ ist ein ➤Algorithmus von Facebook und Instagram. Dieser Algorithmus bestimmt, welche Nachrichten dir in deiner Chronik/Story angezeigt werden. Hast du dich schon gewundert, wieso manchmal ein Beitrag ganz oben steht, obwohl er schon ein paar Tage alt ist, und erst danach aktuellere Beiträge angezeigt werden? Das liegt daran, dass „EdgeRank“ anhand deiner Aktivitäten in den beiden ➤Sozialen Netzwerken analysiert und verknüpft, welche Beiträge für dich interessant sein könnten. Dabei wird auch beachtet, welche Mitteilungen andere interessant finden (zum Beispiel durch die Anzahl der Likes und Kommentare). Daraus ergibt sich dann, welche Beiträge dir angezeigt werden. Da Instagram und Facebook seit 2012 zusammen gehören, tauschen die Netzwerke ihre Analysen untereinander aus, um noch besser abzuschätzen, was dir wohl wichtig ist.

Diese Filterung ist wirklich schlecht, denn Facebook und Instagram bestimmen damit, wen du zu sehen bekommst, indem sie dir keine anderen Möglichkeiten geben. Sie schränken dich damit ein. Verschiedene Informationen und Beiträge von Personen, zu denen du schon länger keinen Kontakt hattest, werden dir teilweise gar nicht mehr angezeigt. Dieses Phänomen nennt sich auch ➤Filterblase.



Aufgabe:
Denk mal darüber nach, zu welchen Menschen du schon lange keinen Kontakt mehr hast, obwohl ihr immer gut befreundet wart. Sind diese Personen wirklich weniger interessant als diejenigen, die dir auf deiner Startseite angezeigt werden? Schreib ihnen doch mal wieder etwas Nettes.

EDV

„EDV“ ist die Abkürzung von „elektronische Datenverarbeitung“. Wenn beispielsweise bei einem Stellenangebot für einen Job „EDV-Kenntnisse“ verlangt werden, dann ist damit der Umgang mit Datenverarbeitungsprogrammen gemeint, zum Beispiel Textverarbeitungsprogrammen wie Microsoft Word (oder der ➤Open-Source-Variante LibreOffice), Kalkulationsprogramme wie Excel (oder OpenOffice Calc), Bildbearbeitungsprogramme und der Umgang mit verschiedenen ➤Datenbanken.

Ende-zu-Ende-Verschlüsselung

Bei der Ende-zu-Ende-Verschlüsselung werden deine Daten, die du über das Internet verschickst, verpackt/verschlüsselt, sobald du sie auf den Übertragungsweg schickst, und sie werden erst von dem Empfänger wieder geöffnet/entschlüsselt. Auf dem Weg dazwischen können diese ➤Daten nicht, bzw. nur sehr schwer, ausgelesen werden (so wie ein Brief in einem Briefumschlag). Das ist besonders wichtig, da kriminelle ➤Hacker oft Daten auf dem Übertragungsweg abgreifen und auslesen. Wenn zum Beispiel der Anbieter eines Online-Spiels nicht mit Verschlüsselung arbeitet und du dich mit deinem Passwort dort anmeldest, dann wird dieses Passwort einfach offen und unverschlüsselt

an den ➤Server übertragen und kann um einiges einfacher ausgelesen werden, als wenn es verschlüsselt übertragen wird.

Wichtig: Wenn dies geschehen ist, dann ist dein Passwort „verbrannt", also nicht mehr geheim und nicht mehr benutzbar. Kriminelle können dieses Passwort dann auch bei anderen ➤Accounts durchprobieren. Es ist nicht immer ganz einfach herauszufinden, ob ein Anbieter mit Verschlüsselung arbeitet, deshalb ist es sehr wichtig, dass du für verschiedene Accounts immer verschiedene Passwörter anlegst. Vor allem beim Austausch von Textnachrichten, Sprachnachrichten, Fotos und Videos solltest du darauf achten, dass du einen Kommunikationsdienst verwendest, der mit Ende-zu-Ende-Verschlüsselung arbeitet. Auf ➤Webseiten erkennst du an der Internetadresse, ob die Seite verschlüsselt übertragen wird oder nicht: Steht „https" vor der Domain („Hypertext Transfer Protocol Secure", auf deutsch: „sicheres Hypertext-Übertragungsprotokoll"), dann ist die Seite verschlüsselt. Das „s" steht für sicher.

AUFGABE: Wenn du für verschiedene Dienste das gleiche Passwort verwendest, dann denk dir neue aus und ändere sie. Wenn es zu viele Passwörter werden, kannst du mit Programmen wie „KeePass" arbeiten. KeePass merkt sich die Passwörter für dich und du musst dir dann nur das Passwort für deinen KeePass merken. Dieses „Masterpasswort" darfst du dann aber auf keinen Fall weitergeben, sonst verrätst du alle deine Passwörter gleichzeitig.

Fake News

„Fake News" sind gefälschte Nachrichten und Tatsachen, also eigentlich Lügen. Sie werden ganz bewusst gefälscht, um eine große Aufmerksamkeit zu bekommen. Ein Gerücht oder eine versehentliche Falschmeldung ist also keine Fake News. Wenn gefälschte Nachrichten für politische Zwecke eingesetzt werden, dann handelt es sich oft auch um politische Propaganda. In manchen Ländern können sie sogar zu Kriegen und Morden führen. Es ist nicht ganz einfach, zwischen den verschiedenen Formen von Falschmeldungen zu unterscheiden.

Fake News sind auch für Expert.innen nicht immer auf den ersten Blick zu erkennen. Es gibt allerdings ein paar Hinweise, auf die du achten kannst:

1. **Aufmerksam mitdenken:** Nur weil eine Nachricht besonders weit verbreitet wurde und in ➤Sozialen Netzwerken besonders oft geteilt wurde, heißt es noch nicht, dass die Nachricht auch der Wahrheit entspricht. Wenn dir eine Nachricht besonders spektakulär vorkommt und du nicht ganz genau weißt, ob die Inhalte stimmen, solltest du die Nachricht lieber nicht weiter verbreiten.
2. **Nicht blenden lassen:** In vielen Falschmeldungen stehen Zahlen, Statistiken oder Zitate von Experten, um die Nachricht seriöser und echter wirken zu lassen. Wenn der Text ziemlich einseitig geschrieben ist, dann solltest du den Inhalt kritisch hinterfragen, denn ein seriöser Artikel zeigt meistens mehrere Seiten und Perspektiven zu einem Thema auf.
3. **Auf sprachliche Fehler achten:** Wenn du in den Texten besonders viele Rechtschreib- oder Grammatikfehler findest, dann ist etwas faul. Redaktionen achten auf eine angemessene Sprache und korrigieren ihre Texte mehrfach, bevor sie veröffentlicht werden.
4. **Quellen prüfen:** Schau dir an, wer den Text verfasst hat, oder zu wem die Internetseite gehört. Dafür kannst du in das ➤Impressum schauen, denn dort müssen Name, Anschrift und Kontaktmöglichkeiten gegeben sein. Wenn ausländische Anbieter dahinter stecken, dann ist ziemlich sicher etwas faul. Wenn es gar kein Impressum gibt oder die Quelle nicht ausfindig gemacht werden kann, dann erst recht. Du kannst auch bei www.mimikama.at oder www.hoaxmap.org prüfen, ob die Meldung bei bereits gelisteten Falschmeldungen dabei ist (➤Hoax).
5. **Bilder prüfen:** Wenn in der Meldung Bilder dabei sind, dann solltest du dir diese genau anschauen. Achte dabei besonders auf Dinge im Hintergrund. Vielleicht erkennst du, dass das Bild in einer anderen Stadt oder in einem anderen Land aufgenommen wurde (anhand von Schriftzügen oder Bauwerken), oder dass Teile von dem Bild von der Farbe, Lichteinfall/Schatten oder Perspektive nicht richtig passen, weil sie schlecht bearbeitet worden sind. Wenn mit dem Bild etwas nicht passt, kannst du sicher sein, dass es sich um eine Falschmeldung handelt.

AUFGABE: Probier mal die umgekehrte Bildersuche aus (www.images.google.com oder www.tineye.com), um zu schauen, ob ein Bild an verschiedenen Stellen hochgeladen wurde. Dort lädst du das gesuchte Bild hoch, und das Netz wird nach diesem Bild abgesucht. So kannst du prüfen, ob das Bild aus einem anderen Artikel kopiert wurde. Tipp: Die Bildersuche kannst du auch nutzen, wenn du vermutest, dass private Bilder von dir unerlaubt im Umlauf sind.

Filterblase

Das Wort „Filterblase“ bezeichnet ein Phänomen, das durch Algorithmen (➢Algorithmus) im Internet entsteht. Die meisten ➢Webseiten-Betreiber (besonders große Konzerne), versuchen so viel wie möglich über dich herauszufinden, indem sie ➢Daten zu deinem Surfverhalten speichern und auswerten. Sie versuchen herauszufinden, was dir gefällt, aber das tun sie nicht, um dir einen Gefallen zu tun. Sie möchten Geld verdienen und dir die Produkte anbieten, die dir am besten gefallen könnten. Den wahrscheinlich größten Teil zur Filterblase trägt Google bei. Wenn du die Suchmaschine nutzt, bekommst du an den oberen Stellen erst einmal Werbeanzeigen eingeblendet, die auf dich zugeschnitten sind (daneben ist dann das Wort „Anzeige“ eingeblendet). Nicht immer sind die ersten Suchergebnisse die einzigen oder am besten passenden auf deine Suchanfragen. Denn Google bestimmt, welche Seiten dir angezeigt werden sollen.

Das ist sehr gefährlich, wenn es um die Bildung einer eigenen Meinung und Interessen geht. **Sobald aus deinem Surfverhalten ersichtlich wird, wofür du dich interessierst, sinken deine Möglichkeiten, etwas Neues kennenzulernen.** Auch in Bezug auf die Gruppen/Cliquen, denen du angehörst, deine Freundschaften und andere Kontakte, schlägt die Filterblase zu. Facebook und Instagram nutzen beispielsweise den Algorithmus ➢„EdgeRank“ (unter diesem Stichwort kannst du nachlesen, was das für deine Freundschaften bedeutet).

Besonders bedenklich ist die Filterblase jedoch, wenn es um politische Meinungen und Ansichten geht, denn wenn immer wieder Menschen mit denselben Interessen zusammengebracht werden, besteht die Gefahr der politischen Radikalisierung (zum Beispiel Rechtsextremismus). Das heißt, dass Gleichgesinnte zusammengeführt werden und auch immer zusammen bleiben und sich immer mehr in ihre geteilte Meinung hineinsteigern, sich austauschen und in die gemeinsame Richtung weiterentwickeln. Das ist schädlich für die Demokratie, weil man verlernt, sich mit den Meinungen anderer Menschen auseinander zu setzen.

Firewall

Eine „Firewall“ (Deutsch: „Brandmauer“) ist eine ➢Software, welche die Datenverbindungen zwischen Computern und Netzwerken wie dem Internet überwacht. In dem Programm wird festgelegt, unter welchen Bedingungen und nach welchen Regeln ➢Daten übertragen werden. Wenn die Daten nicht diesen Einstellungen entsprechen, wird die Übertragung blockiert. So kann verhindert werden, dass ➢Hacker oder Viren (➢Schadsoftware) in das Computersystem eindringen. Ohne eine Firewall solltest du dich lieber nicht im Internet

Forum ★

Das Wort „Forum“ kommt aus dem lateinischen und bezeichnete ursprünglich einen Marktplatz. Im Internet ist mit Forum (auch Web-Forum, Online-Forum oder ➢Community) ein Angebot gemeint, bei dem sich Personen zu verschiedenen Themen austauschen können. Bei einem Klick auf das jeweilige Thema öffnen sich meist sogenannte ➢„Threads“ (z.B. Unterthemen). Jemand schreibt oder fragt etwas und jemand anderes antwortet darauf. Für die meisten Foren musst du dir einen ➢Account anlegen, um mitdiskutieren oder Fragen stellen zu können. Um die Antworten der anderen zu lesen, braucht man sich meistens nicht selbst anzumelden. Es gibt unzählig viele Foren, die sich jeweils mit einem ganz bestimmten Thema beschäftigen. Sehr bekannte allgemeine Online-Foren für alle möglichen Themen sind beispielsweise „ASK.fm“ und „Gutefrage“.

FSK ★

„FSK“ steht für die „Freiwillige Selbstkontrolle der Filmwirtschaft“. Du findest diese Abkürzung zum Beispiel auf DVDs und Blu-rays, im Fernsehprogramm, im Kino oder Fernsehen, bevor ein Spielfilm beginnt, und an anderen Stellen, bei denen es um Filme geht. Denn es handelt sich um eine Kennzeichnung, ab welchem Alter der Film angeschaut oder gekauft werden darf. Für die Einstufung von Computerspielen, ist die ➢USK zuständig.

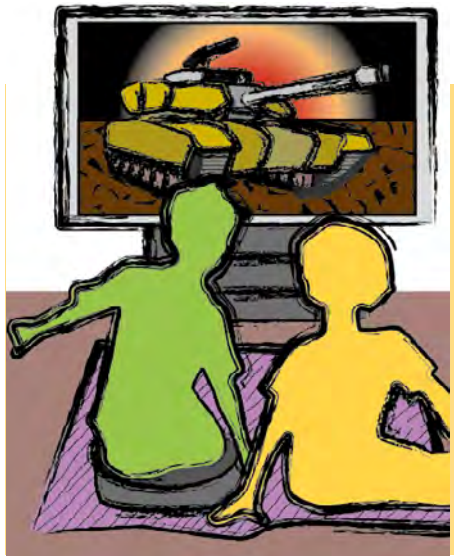
Es gibt in Deutschland fünf Altersfreigaben:

- FSK 0
- FSK 6
- FSK 12
- FSK 16
- FSK 18

Diese sind Teil des Jugendschutzgeset-

zes (JuSchG) und sollen vermeiden, dass Kinder Inhalte zu sehen bekommen, die nicht für ihr Alter geeignet sind, zum Beispiel Gewalt- oder Nacktszenen und Fäkalsprache (Schimpfwörter oder starkes Fluchen). Das muss nicht immer heißen, dass ein Film mit vielen Gewaltszenen erst für ältere Kinder freigegeben wird, denn es wird auch darauf geachtet, was die Botschaft hinter der Geschichte ist. Wenn beispielsweise im Film ganz klar betont wird, dass Gewalt schlecht ist und andere Lösungen für Probleme und Konflikte geboten werden, dann kann der Film eventuell auch für jüngere Kinder zugelassen werden, obwohl die Szenen recht brutal sind.

Die Produzent.innen von Filmen sind zwar nicht gesetzlich verpflichtet, ihre Filme von der Freiwilligen Selbstkontrolle prüfen zu lassen, aber in Deutschland dürfen nur Filme gezeigt werden, die vorher geprüft wurden, deshalb bleibt den Produzenten keine andere Wahl, als ihre Filme prüfen zu lassen, wenn sie diese bei uns zeigen möchten. Diese Regelung ist natürlich gut, um Kinder zu schützen, doch du musst immer bedenken, dass eine Art ➤Zensur betrieben wird und die Entfaltung von einzelnen Persönlichkeiten eingeschränkt werden kann. Das bedeutet: Wenn zum Beispiel eine Freigabe ab 12 Jahren erteilt wird (FSK 12), verpassen jüngere Kinder vielleicht Szenen, die zum kritischen Nachdenken angeregt hätten, ohne ihnen zu schaden. Jedes Kind ist individuell und kann das Gesehene ganz unterschiedlich verarbeiten. Die von der FSK festgelegten Freigaben sind in vielen Fällen gut überlegt, aber es gibt keine Garantie/Sicherheit, dass Zwölfjährige besser mit den Inhalten umgehen können als Mädchen und Jungen im Alter von 8 oder 10 Jahren. Und wenn beispielsweise einzelne Szenen herausgeschnitten werden, um eine niedrigere Altersfreigabe zu bekommen, dann werden außerdem die Filmemacher.innen zensiert und ihrer künstlerischen Freiheit beraubt.



AUFGABE: Schau dir mal gemeinsam mit deinen Eltern einen Film an, der für dein Alter freigegeben ist und achte dabei auf Gewalt- und Kampfszenen. Würdest du den Film auch jüngeren Kindern oder Geschwistern empfehlen? Wenn nein, wieso nicht? Würdest du eher eine höhere Altersgrenze ansetzen? Wenn ja, wieso? Rede mit deinen Eltern darüber. Und übrigens: Dein Bauchgefühl wird dir schon ganz genau sagen, welche Szenen besser und weniger gut für dich geeignet sind, denn du kennst dich selbst am besten.

GEHEIMDIENST ★

Geheimdienste oder auch Nachrichtendienste sind Organisationen oder Behörden, deren Aufgabe es ist, militärische, politische und wirtschaftliche Informationen über Personen und Länder zu beschaffen. Das heißt: Sie sammeln Informationen darüber, was andere Politiker.innen planen. Sie analysieren Konflikte und Kriege und bewerten, wie es sich auf das eigene Land auswirkt, wenn woanders auf der Welt etwas passiert. Die Mitarbeiter.innen dieser Organisationen recherchieren dafür in öffentlichen Dokumenten, aber sie spionieren auch heimlich andere Personen und Länder aus. Sie dürfen niemandem erzählen, was sie bei ihrer Arbeit herausgefunden haben und auch untereinander nur die nötigsten Informationen ihrer streng geheimen Projekte weitergeben. Die Methoden, wie Geheimdienste an verschiedene Daten kommen, wird in den meisten Fällen geheim gehalten, aber es gab auch schon viele Fälle, in denen bewiesen wurde, dass sie sich nicht an Gesetze gehalten haben, um an Informationen zu kommen.

Wichtig: Geheimdienste sammeln nicht nur Informationen von Politiker.innen und Personen, die bedeutsame Positionen und Jobs haben, sondern auch die ➤Daten von vielen anderen Bürgerinnen und Bürgern. Das ist ein großer Eingriff in die ➤Privatsphäre und das Grundrecht auf die informationelle Selbstbestimmung (➤Datenschutz). Das Wissen, das sie haben, gibt ihnen mehr Macht als die mächtigsten Einzelpersonen sie je haben könnten und das macht sie sehr gefährlich.

In Deutschland haben Geheimdienste eine ganz besondere Geschichte, denn

die „Geheime Staatspolizei“ (Gestapo) in der Nazi-Zeit und die „Staatssicherheit“ (StaSi) in der DDR, wurden von den damaligen Regierungen benutzt, um ihr Volk zu unterdrücken und zum Beispiel politisch anders denkende Menschen unter Druck zu setzen oder ins Gefängnis zu stecken. Heute haben wir in Deutschland drei große Nachrichtendienste: Den Bundesnachrichtendienst (BND) für Informationen aus dem Ausland, das Bundesamt für Verfassungsschutz (BfV) für Informationen innerhalb des Landes und den Militärischen Abschirmdienst (MAD), der zur Bundeswehr gehört. Außerdem gibt es noch verschiedene Nachrichtendienste für die einzelnen Bundesländer und andere Organisationen mit ähnlichen Aufgaben. Im Jahr 2013 veröffentlichte Edward Snowden, ein Mitarbeiter des US-amerikanischen Geheimdienstes NSA, geheime Dokumente und wurde somit zum ➤Whistleblower. Er hat der Öffentlichkeit erklärt und nachgewiesen, welche sensiblen Daten die NSA in Zusammenarbeit mit anderen Geheimdiensten (auch mit dem deutschen Bundesnachrichtendienst) illegal ausspioniert.

AUFGABE: Recherchiere nach dem „NSA-Skandal“ und schau dir an, welche Personen, Unternehmen und Online-Dienste von der Geheimdienst-Spionage betroffen waren. Google, Yahoo, Skype, das Online-Rollenspiel „World of Warcraft“ und die Spiele-App „Angry Birds“ sind nur einige von denen, die du sicherlich kennst.

GEMA

„GEMA“ ist die Abkürzung für „Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte“. Die „Vervielfältigungsrechte“ regeln das Recht/die Lizenz, um etwas weiterzuverbreiten. Die GEMA verwaltet in Deutschland die Nutzungsrechte für künstlerische Werke, wie Text und Musik. Der Begriff ist dir bestimmt schon einmal bei YouTube begegnet, denn eine Aufgabe der GEMA ist es, auf Urheberrechtsverletzungen zu reagieren. Stellt zum Beispiel jemand bei YouTube ein Video mit Musik ein, für die er/sie keine Lizenzen für die Weiterverbreitung gekauft hat, dann darf er/sie das Video nicht für andere zur Verfügung stellen.

GPS

„GPS“ (Global Positioning System) ist ein globales, also weltweites, Satellitensystem zur Navigation und Standortbestimmung.

Beinahe jedes Smartphone ist heutzutage mit einer GPS-Antenne ausgestattet. Die Satelliten befinden sich im Weltall, rund um die Erde, und senden ein Signal an dein Gerät. Dadurch kann bestimmt werden, wo auf der Erde du

dich befindest, und zwar sehr genau. Bei guten Empfangsbedingungen kann dein Standort auf etwa 20 Meter genau bestimmt werden. Je nachdem, wo du dich gerade befindest und wie viele Satelliten dein Signal empfangen (vier müssen es mindestens sein), kann es sein, dass die Positionsbestimmung ein wenig daneben liegt. Wie präzise die Positionsbestimmung in den meisten Fällen ist, merkst du an Navigationsgeräten im Auto (kurz: Navis), die dir ganz genau den Weg von A nach B angeben können.

Wichtig: Jemand, der auf deine GPS-Daten Zugriff hat, weiß dann also, dass du dich an einem bestimmten Punkt befindest. Besonders interessant sind deine Positionsdaten zum Beispiel für ➤Drittanbieter, um mehr über deine Gewohnheiten und dein Bewegungsmuster zu erfahren. Deshalb solltest du zum Beispiel bei der Installation von ➤Apps darauf achten, ob der Anbieter Zugriff auf deine Standortdaten haben möchte und ob er sie wirklich braucht. Aber auch Strafverfolgungsbehörden, zum Beispiel die Polizei, verwenden das GPS-System, um Verbrecher zu finden. Die Polizei holt sich diese Daten von deinem Mobilfunkanbieter und kann auch prüfen, wer sich zum Zeitpunkt einer Straftat in der Nähe des Tatortes aufgehalten hat (siehe auch ➤Datenschutz und ➤Vorratsdatenspeicherung)

AUFGABE: Schau dir die ➤App-Berechtigungen in deinem Handy an und überleg dir, welche App deinen Standort wirklich wissen sollte. Die Straßenbahn-App vielleicht schon (obwohl du auch den Namen der nächsten Haltestelle einfach aus dem Menü auswählen könntest). Aber bei Spielen zum Beispiel? Welches Spiel muss für seine Funktionen wissen, wo du bist? Wo immer du es nicht für nötig hältst, schalte die Standort-Berechtigung ab.

Hacker

Hacker sind Menschen, die sich mit Computern sehr gut auskennen. Ein Hack (im weiteren Sinne übersetzt mit „technischer Kniff") löst ein technisches Problem auf eine ungewöhnliche Weise, meistens durch eine Überarbeitung oder Erweiterung eines ➤Algorithmus. Das Wort „hacken" wird oft für Ereignisse verwendet, in denen sich jemand unerlaubt Zugriff zu einem System verschafft hat. Es gibt allerdings nicht nur kriminelle Hacker. Die guten Hacker probieren zum Beispiel Sicherheitslücken in Systemen (zum Beispiel Netzwerken) und Geräten zu erkennen und zu schließen. Diese Fähigkeit erfordert ein hohes Maß an IT-Wissen und Kreativität.

Viele große Unternehmen haben ihre eigenen Hacker und Haecksen, die einzig und allein versuchen, in das eigene System einzudringen. So können sie verhindern, dass böse Hacker die Lücke im System vor ihnen finden.

Kriminelle Hacker versuchen sich meist unerlaubt Zutritt zu einem System zu verschaffen, um ➤Daten zu klauen, die sie dann (beispielsweise an ➤Drittanbieter) weiterverkaufen oder um ➤Schadsoftware zu installieren, die ebenfalls deine Daten ausspioniert.

Happy Slapping

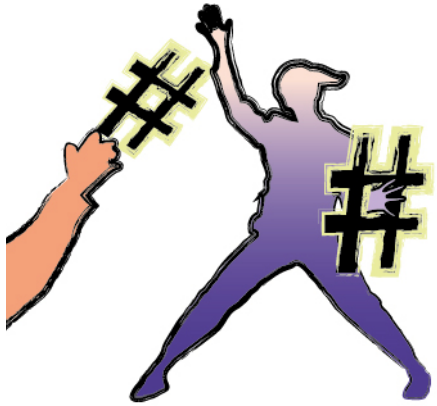
„Happy Slapping" heißt übersetzt „lustiges Schlagen" oder „fröhliches Zuschlagen". Gemeint ist damit die Verbreitung von Gewaltvideos über das Smartphone. Oft handelt es sich um größere Personengruppen, die eine Person fertig machen, während jemand das ganze Geschehen filmt. Das ist natürlich auf vielen verschiedenen Ebenen absolut verboten.

1. Es handelt sich um Körperverletzung, die je nach Schwere, zum Beispiel mit Geldstrafen oder Gefängnis, bestraft wird. Das ist nicht „happy", lustig oder fröhlich!
2. Es handelt sich um die Verbreitung von Gewaltdarstellungen, was ebenfalls verboten ist, da so ein Video die ohnehin schon geschädigte Person noch weiter erniedrigt.
3. Und letztendlich auch noch um die Verletzung des ➤Recht am eigenen Bild, denn das Opfer dieser Tat stimmt mit Sicherheit nicht zu, dass das Video verbreitet wird.

Hardware

Unter den Begriff „Hardware" fallen alle Teile, die in elektronischen Geräten verbaut sind, also die Teile, die man auch anfassen kann. Bei einem Computer wäre das zum Beispiel die Grafikkarte, die Tastatur, der Bildschirm, die Festplatte oder das Gerät insgesamt. Damit diese Teile alle zusammen funktionieren und zum Beispiel der Text, den du in die Tastatur eingibst, auch auf dem Bildschirm erscheint, werden Programme benötigt, welche diese Teile durch Befehle miteinander verbinden (➤Software).

Hashtag



„Hashtag" bezeichnet das Symbol Doppelkreuz (#) und wird im Internet für die Verschlagwortung genutzt. Somit kann man zum Beispiel in langen Texten nach bestimmten Wörtern suchen. Die Foto-Plattform „Instagram" und auch der Mikrobloggingdienst „Twitter" haben den Hashtag sehr populär gemacht.

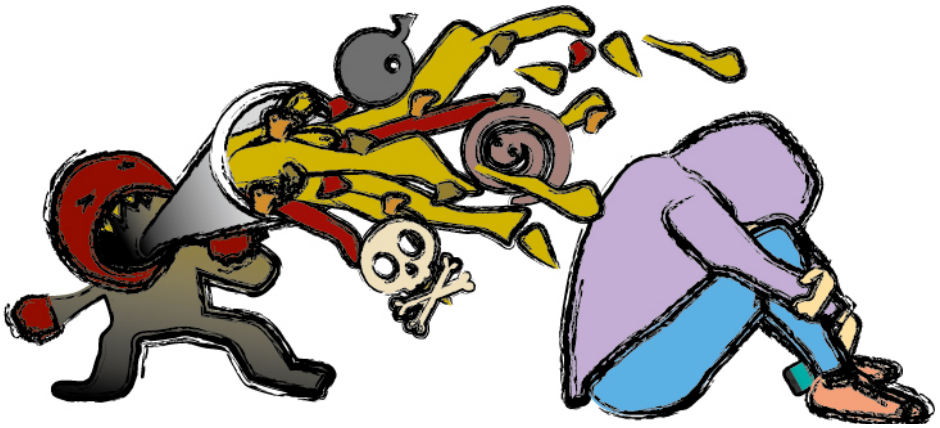
Hater

Als „Hater" (auf Deutsch: „Hasser") werden Menschen bezeichnet, die durch Sticheleien und blöde Bemerkungen Ärger verursachen oder ihren Hass verbreiten möchten. Der Begriff wird häufig bei blöden Kommentaren im Internet verwendet. Besonders berühmte Personen und YouTuber sind oft davon betroffen, dass jemand ihre Taten, Musik oder Videos nicht gut findet und öffentlich seinen/ihren Ärger darüber auslässt.

Wichtig: Nur weil jemand etwas nicht gut findet und seine klare Meinung äußert, ist er/sie noch kein Hater! Anderer Meinung zu sein, ist ja erstmal nicht schlecht, sondern der Beginn einer Diskussion. Du solltest aber immer zwischen konstruktiven Kritikern und Hatern unterscheiden. Konstruktive Kritik bedeutet, dass man seine kritische Haltung reflektiert begründen kann. Wenn die Bemerkungen nur dazu dienen, jemanden schlecht zu machen, dann kann von „Hatern" gesprochen werden. Wenn es um politische Themen geht, kann es sich auch um ➤Hate Speech (Hassrede) handeln.
Lass dich von blöden Kommentaren nicht verunsichern! Viele Hater tun dies nur aus Langeweile, aus Neid oder weil sie sich anonym stark fühlen!

Hate Speech

„Hate Speech" ist die englische Übersetzung von „Hassrede". Dabei geht es um fiese Kommentare, zum Beispiel Beleidigungen und Drohungen, im politischen Kontext, die Hass verbreiten. Durch diese Inhalte wird Intoleranz, Aggressi-



vität, Feindseligkeit oder Diskriminierung gegenüber anderen Personengruppen, Minderheiten oder zum Beispiel Menschen mit Migrationshintergrund ausgedrückt. Deshalb haben die meisten Hasskommentare einen rassistischen, frauen- oder fremdenfeindlichen Hintergrund.

Das Internet und vor allem ➢Soziale Netzwerke bieten die Möglichkeit, solche Hassreden sehr leicht und schnell voranzutreiben. Dadurch, dass auf vielen Websites die Möglichkeit vorhanden ist, über Chats miteinander zu kommunizieren und Beiträge immer weiter zu kommentieren, gibt es oft viele Menschen, die diese Situation nutzen, um fiese Sachen zu schreiben. Dadurch, dass man im Internet oft anonym bleiben kann (➢Anonymität), fällt es den Menschen leichter, Beleidigungen zu schreiben, die sie ihrem Gegenüber wahrscheinlich nicht direkt ins Gesicht sagen würden. Anonym gemeine Sachen zu schreiben ist also nicht cool, sondern feige.

Wichtig: Wenn du zum Beispiel in einem Sozialen Netzwerk mitbekommst, dass jemand rassistische Aussagen von sich gibt oder eine ganz bestimmte Person fertig macht, weil sie zum Beispiel eine andere Hautfarbe oder Religion hat, dann solltest du diese Kommentare immer mit der Meldefunktion melden.

Hoax

Ein „Hoax" ist eine Falschmeldung, bzw. ein Scherz, der im Internet kursiert und über Massenmails und andere Nachrichten verbreitet wird, zum Beispiel über ➢Kettenbriefe. Oft wird dabei vor mit Viren infizierten ➢Links gewarnt (siehe ➢Schadsoftware), obwohl es diesen Virus gar nicht gibt. Diese Meldungen verunsichern die Menschen nur (➢Fake News).

Wie erkenne ich einen Hoax?

- Oft wird man aufgefordert, die Nachricht an möglichst viele Menschen zu verbreiten. In einer seriösen Meldung würde das niemand tun. Oder hast du schon mal in einem seriösen Zeitungsartikel die Überschrift gelesen „Bitte weitersagen"?
- Der Schaden, den der Virus angeblich anstellt, wird sehr stark dramatisiert. Manche Schäden sind gar nicht möglich, wie zum Beispiel dass ➢Hardware beschädigt wird.
- In vielen Fällen wird eine bekannte Firma als Quelle genannt, um die Meldung seriöser wirken zu lassen. Doch wenn du mal auf den Internetseiten dieser Firmen nachschaust, wirst du schnell feststellen, dass diese Firmen damit gar nichts zu tun haben.
- Die Zeitangaben in diesen Meldungen sind oft nicht nachzuvollziehen, zum Beispiel wenn da steht „seit gestern verbreitet sich ein Link…": Wann war denn gestern? Du weißt ja nicht, seit wann diese Meldung schon in Umlauf ist.

Auch Fake News sind eine Art Hoax, doch hier läuft es meistens umgekehrt: Es wird beispielsweise eine falsche Pressemeldung in Umlauf gebracht (zum Beispiel über einen Raub oder Mord), die große Aufmerksamkeit auf sich ziehen, doch hinter den Links verstecken sich eventuell wirklich Viren.

Bei Facebook ist noch eine andere Form des Hoax sehr beliebt: Es verbreiten sich Links, die in der Überschrift auf eine sensationelle Entdeckung oder eine andere spannende Nachricht aufmerksam machen, aber die Überschriften sind sehr allgemein gehalten, zum Beispiel „Du wirst staunen, wenn du das liest" oder „Unglaublich, was diesem Mann passiert ist". Um zu erfahren, worum es wirklich geht, soll man den Link anklicken. Oft wird dazu ein Foto abgebildet, auf dem der spannende Teil, um den es geht, abgeschnitten ist und der Eindruck entsteht, als müsse man den Link öffnen, um das ganze Bild zu sehen. Nach dem Öffnen der Seite passiert oft gar nichts, es erscheint lediglich eine leere Seite oder Werbung. Auch hinter diesen Links können sich Viren verstecken.

Wichtig: Grundsätzlich gilt: Öffne niemals einen Link, den dir jemand Fremdes geschickt hat und pass generell auf, welche Links du öffnest. Auch Freunde können dir virenverseuchte Links zuschicken, wenn sie es nicht besser wissen.

AUFGABE:
Wenn du am Computer den Mauszeiger über einen Link bewegst, ohne zu klicken, wird dir am unteren Bildschirmrand die ➢URL angezeigt, an der du oft schon erkennen kannst, was für eine Seite sich hinter der Verlinkung versteckt. Probier es aus! Kannst du erkennen, wohin dich ein Link weiterleiten will?

Hoster

Ein „Hoster“ (Deutsch: „Gastwirt“ oder „Veranstalter“) ist ein Anbieter, der Daten für Internetdienste speichert. Es gibt beispielsweise

- Webhoster (für ➤Webseiten),
- File-Hoster (für ➤Clouds oder andere Seiten, auf denen Dateien (Englisch: „Files“) gespeichert sind),
- oder E-Mail-Hoster.

Hotspot

Ein „Hotspot“ ist ein öffentlicher ➤WLAN-Zugang, zum Beispiel im Bus oder Zug, am Bahnhof, an Flughäfen, in Hotels oder in Cafés. Du kannst auch mit deinem eigenen Gerät einen Hotspot erzeugen, sodass andere deine Internetverbindung mitbenutzen können. Wenn du das tust, solltest du deinen Hotspot unbedingt mit einem Passwort schützen, damit keine fremden Menschen über deine Verbindung surfen, denn wenn sie zum Beispiel etwas Illegales im Internet machen, dann fällt die Straftat auf dich zurück. Außerdem teilst du auch dein Datenvolumen mit den anderen Surfern, die deine Verbindung nutzen.

Wichtig: Sei vorsichtig in öffentlichen WLAN-Netzen und nutze sie am besten gar nicht erst. Du kannst nie genau wissen, wer in deinem Umkreis den Hotspot mitnutzt und ermöglichst zum Beispiel ➤Hackern einen leichteren Zugriff auf dein Netzwerk.

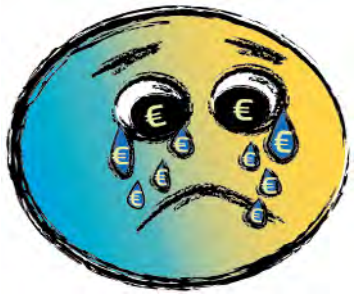
Impressum

In einem Impressum wird angegeben, wo etwas herkommt und wer dafür verantwortlich ist.

Bei einem Buch ist im Impressum beispielsweise der Autor angegeben sein, aber auch der Verlag, der das Buch gedruckt hat. Bei einer Internetseite muss im Impressum stehen, wer für die Seite verantwortlich ist, auch wenn viele Leute an der Internetseite mitarbeiten/mitschreiben. Denn wenn die Inhalte mal illegal oder strafbar sind, dann muss jemand dafür verantwortlich gemacht werden und es muss die Möglichkeit geben, diese Person zu kontaktieren. Zumindest im deutschen Recht ist das so.

Am häufigsten begegnet euch das Wort bestimmt im Internet, denn für Internetseiten besteht eine Impressumspflicht, außer es handelt sich um eine Seite, die ausschließlich für den privaten Gebrauch ist, zum Beispiel ein Online-Tagebuch/Blog. Aber sobald die Inhalte auch gezielt andere Menschen ansprechen sollen, Informationen verbreitet werden, die aus anderen Quellen kommen oder Werbung für etwas gemacht wird, muss ein Impressum angelegt werden. Dabei müssen zwei Wege zur schnellen Kontaktaufnahme angegeben sein, zum Beispiel E-Mail-Adresse und Telefonnummer.

In-App-Käufe



„In-App-Käufe“ sind die Käufe, die du innerhalb einer ➤App tätigst. Oft kannst du dir eine App, zum Beispiel ein Spiel, kostenlos herunterladen, doch nach ein paar Level kommst du nicht weiter, wenn du nicht dafür bezahlst. Oder du bekommst die Möglichkeit, besondere Level und Fähigkeiten in Spielen gegen Bezahlung freizuschalten oder einen Premium-Status freizukaufen, der dir mehr Funktionen bringt.

Wichtig: Die Preise dafür sind meistens nur sehr gering, zum Beispiel 79 Cent. Doch wenn du gerade richtig Spaß an dem Spiel hast und dir immer wieder Dinge dazukaufst, um besser zu sein, dann kann es passieren, dass du schnell den Überblick verlierst. Wenn du dich nur 10 Mal darauf einlässt, bezahlst du schon 7,90 Euro und am Ende kann dabei eine hohe Geldsumme entstehen, mit der du zunächst gar nicht gerechnet hattest. Außerdem darfst du solche Käufe gar nicht ohne deine Eltern durchführen. Andererseits: Wenn du ein Spiel wirklich gerne spielst, ist es auch fair, den Programmierern dafür ein bisschen was zu bezahlen. Aber pass auf, dass du den Überblick behältst!

Influencer ★

„Influencer“ (übersetzt: Beeinflusser), sind Personen, die – wie der Name schon sagt – andere Menschen beeinflussen Das geht auf verschiedene Arten – mit dem Wort „Influencer“ bezeichnet man aber meistens Menschen, die Werbung machen.. Besonders bei YouTube (aber auch in anderen ➤Sozialen Netzwerken) hat sich mittlerweile eine große Influencer-Kultur entwickelt: Verschiedene bekannte oder weniger bekannte YouTuber.innen stellen in ihren Videos Produkte vor und bekommen von den jeweiligen Firmen Geld dafür. Je nachdem, wie berühmt diese Personen sind und wie groß die Reichweite ihrer Videos und anderen ➤Postings ist (verlgeiche hierzu auch den Beitrag über ➤„viral“), verdie-

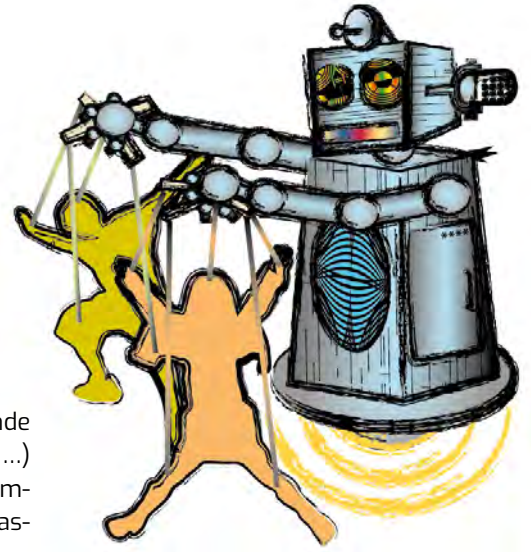
nen sie manchmal viel Geld damit. Es ist schwer eine allgemeine Zahl zu nennen- Schwer zu sagen, wie viel sie damit verdienen, aber man kann ganz grob rechnen, dass sie pro 1000 Views (also wenn das Video 1000 mal angesehen wurde), einen Euro verdienen. „Influencer“ oder „Influencerin“ ist keine Berufsbezeichnung, sondern ein Begriff aus dem Arbeitsbereich ➢„Marketing“. Werbung zu machen ist somit ihr Job. Wie sie dies machen, ist sehr unterschiedlich.

- ➢Unboxing-Videos: Wie der Name „unboxing“, also „auspacken“, schon sagt, wird gefilmt, wie ein Produkt aus seiner Verpackung genommen wird. Die Influencer versuchen dabei möglichst natürlich zu wirken, als wenn sie ganz normale Kund.innen wären, aber in Wirklichkeit haben sie sich vorher schon ganz genau überlegt, wie sie das Produkt besonders toll beschreiben und präsentieren, sodass alle Zuscher.innen das auch haben möchten.
- ➢Haul-Videos: „Hauls“ (übersetzt: Beute) sind Videos, in denen Produkte präsentiert werden, welche die Influencer schon vorher zugeschickt bekommen haben. Sie beschreiben die Vorteile der Produkte, aber oft auch, welche Erfahrungen sie damit bereits gemacht haben. Es kommt somit öfter vor, dass Influencer erst ein Unboxing-Video veröffentlichen und später ein Haul-Video.
- Product Placement (Produktplatzierung): Manchmal ist die Werbung gar nicht so offensichtlich. Im Hintergrund stehen zum Beispiel in einem Regal oder auf einem Tisch Produkte rum und in der Beschreibung des Videos werden die ➢Links angegeben, wo diese Dinge gekauft werden können. Diese Art der Werbung ist ganz nah an Schleichwerbung, also an heimlicher Werbung und der heimlichen Beeinflussung von Kaufentscheidungen dran.

Instant Messenger ★

„Instant Messenger“ (kurz: IM) sind Kommunikations- bzw. Nachrichten-Programme, wie z.B. WhatsApp oder der Facebook-Messenger. Sie werden oft fälschlicherweise als ➢Soziale Netzwerke bezeichnet, unterscheiden sich aber von Chats und Sozialen Netzwerken, da sie als ➢Software fest auf dem Gerät installiert werden müssen und somit nicht von jedem beliebigen Gerät abgerufen werden können. Die Nachrichten werden in Echtzeit übertragen, das heißt, dass du auch Leuten eine Nachricht schicken kannst, die gerade nicht online sind und sie lesen diese dann, wenn sie den Messenger wieder öffnen.

Internet der Dinge



„Internet der Dinge“ bezeichnet die technologische Entwicklung von der Vernetzung von alltäglichen Gegenständen. Dadurch können diese mit den Menschen, aber auch untereinander kommunizieren. Beispiele:

- Internetfähige Gebrauchsgegenstände (zum Beispiel sprechende Zahnbürsten)
- Internetfähiges Spielzeug (sprechende Puppen, Roboter, interaktive Bücher, ...)
- Gadgets (➢Wearables, wie Fitnessarmbänder, ➢Smart Watches, Sprachassistenten, wie Alexa, ...)
- Smart Home (per App regulierbare Heizungen und Jalousien, sprechende Zahnbürsten, ...)
- Smart Cars (Autos, die sich zum Beispiel selbst einparken oder erkennen, wenn du am Steuer müde wirst)
- Smart Cities (elektronische Fahrkarten für Bahnen, Ampeln, die sich nach Verkehrsaufkommen richten, ...)

Diese Dinge erledigen verschiedene Aufgaben von alleine oder sollen zumindest den Menschen bei bestimmten Aufgaben entlasten.

So vorteilhaft es auch sein mag, dass du mit einer Puppe sprechen kannst wie mit einer Freundin, oder, dass du schon auf dem Nachhauseweg die Heizung in der Wohnung einschalten kannst – du solltest bedenken, dass dabei Unmengen an ➢Daten entstehen und gespeichert werden. Zum Beispiel alles, was du der Puppe erzählst oder wann du jeden Tag nach Hause kommst und vielleicht sogar, welchen Weg du nimmst.

Es sieht zwar so aus, als würdest du mit der Puppe reden und eine Antwort bekommen, aber eigentlich meldet die Puppe an einen ➢Server bei der Firma, die die Puppe hergestellt hat, was du gesagt hast. Und dort wird jede deiner Aktionen gespeichert und verarbeitet. Damit versucht die Firma, dich bestmöglich zu analysieren, um ihre Produkte zu optimieren und dann mehr zu verkaufen.

Die „smarten“ Dinge kommunizieren nicht nur zwischen einem Sender und einem Empfänger, zum Beispiel zwischen einem Auto und seinem Besitzer, sondern auch untereinander. Es gibt nicht nur einzelne Gegenstände, sondern ganze Produkt- und Lebensbereiche, die „smart“ gemacht, also miteinander vernetzt werden. Intelligente Dinge überschneiden sich somit beispielsweise mit dem intelligenten Zuhause. Intelligente Fahrzeuge überschneiden sich mit intelligenten Städten. Es läuft darauf hinaus, dass eines Tages alles und jeder vernetzt sein wird.

Ein kleines **Gedankenexperiment**, wie sich das Internet der Dinge in Zukunft entwickeln könnte:

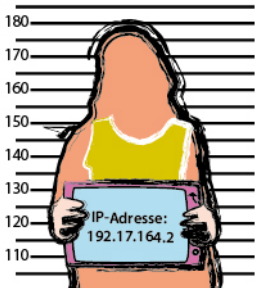
Angenommen der Kühlschrank in eurer Wohnung wäre mit dem Internet verbunden und registriert anhand von Codes und Chips an den Produkten, welche Lebensmittel darin enthalten sind. Außerdem trägst du ein Fitnessarmband, welches dir jetzt gerade nach dem Sport signalisiert, dass du einen Liter Wasser trinken sollst. Das Armband startet eine Abfrage an den Kühlschrank und der Kühlschrank teilt dem Fitnessarmband mit, dass kein Wasser mehr da ist. Diese Information leitet der Kühlschrank an deine Einkaufs-App weiter und du siehst auf deinem Smartphone, in welchen Läden auf deinem Heimweg gerade dein Lieblingswasser im Angebot ist. Zusätzlich bekommst du aber auch andere Produkte vorgeschlagen, die gerade stark reduziert sind, deshalb kaufst du auch noch Marmelade. Sobald du die Marmelade in den Kühlschrank stellst, petzt dieser das dem Fitnessarmband weiter. Das Armband rechnet aus, wie viele Kalorien du bereits verbrannt hast und wie viele Marmeladenbrote du heute Abend noch essen darfst…

Und was davon entscheidest du noch selbst? Die Marmelade hättest du gar nicht gekauft, wenn sie dir nicht in der App angezeigt worden wäre. Das Wasser wäre einen Laden weiter vielleicht noch billiger gewesen, aber der Laden hat keinen Vertrag mit deinem Einkaufs-App-Hersteller und wird deshalb nicht angezeigt. Ob du also wirklich einen Vorteil hattest, ist fraglich – aber alle Firmen wissen alles über dich und können dich beim nächsten Mal noch besser beeinflussen.

Wichtig: Gerade Gesundheitsdaten und Ernährung sind ganz sensible Daten und besonders geschützt. Manche Krankenkassen werten solche Daten schon aus und verlangen Geld, wenn du dich nicht absolut artig verhältst. Viele Folgen der Datensammelei, die das „Internet of Things“ macht, sind noch gar nicht absehbar. Wenn wir mit unseren Smartphones, die WLAN, Kamera und Mikrofon haben, in der Stadt - oder „smart City“ bewegen, werden wir selber zu mobilen Sensoren, mit denen wir und andere in unserer Nähe überwacht werden. Weiteres zu dem Thema kannst du im Eintrag zu „smart“ nachlesen. Weiteres kannst du im Beitrag zu „smart“.

IP-Adresse

Jedes Gerät mit einem Internetzugang hat eine eigene IP-Adresse (IP = Internetprotokoll), die aus Zahlen und Punkten besteht (zum Beispiel 93.184.216.34). Du kannst eine IP-Adresse mit deiner Wohnadresse vergleichen: Es lässt sich klar zuordnen, wem dieses Gerät gehört, bzw. über welches Gerät die Internetverbindung genutzt worden ist. Das ist zwingend notwendig, denn wenn Daten von einem Gerät auf ein anderes Gerät geschickt werden sollen, müssen die ➤Router (vergleichbar mit Postboten) wissen, an wen sie die Daten übermitteln sollen.



IT

„IT“ ist die Abkürzung von „Informationstechnologie“ und meint die Informations- und Datenverarbeitung auf elektronischem Weg. Eine etwas genauere Bezeichnung wäre deshalb „elektronische Informations- und Datenverarbeitung“ (EID). Die Begriffe IT und ➤EDV werden oft synonym verwendet, aber EDV ist nur ein Teil der IT.

Jugendmedienschutz ★

Das Wort „Jugendmedienschutz“ steht für den Schutz von Kindern und Jugendlichen bei der Nutzung von ➤Medien und orientiert sich an dem Jugendschutzgesetz (JuSchG). Dort ist beispielsweise die Kennzeichnung von Filmen (➤FSK) und Computerspielen (➤USK) mit einer Altersfreigabe festgelegt, um Kinder vor Inhalten zu schützen, die für ihr Alter gefährlich oder schädlich sein können, zum Beispiel Gewalt, Drogenkonsum und Pornographie.

Um Kinder vor ungeeigneten Inhalten im Internet zu schützen, werden beispielsweise Filterprogramme auf Computern und Smartphones eingesetzt, die schädliche Inhalte herausfiltern (zum Beispiel „JusProg“). Die meisten Jugendschutzfilter arbeiten mit „Blacklists“ („schwarzen Listen“), auf denen ➤Webseiten aufgeführt sind, die Kinder nicht besuchen sollten. Diese werden dann automatisch gesperrt, wenn die ➤Software erkennt, dass ein Kinder-Account angemeldet ist (➤Account). Auch ➤Kinder-Suchmaschinen arbeiten nach diesem Prinzip. Zu gefährlichen Seiten gehören neben den oben genannten Beispielen auch Webseiten, auf denen Themen wie Essstörungen (zum Beispiel Magersucht oder Bullimie) und Selbstverletzung als etwas Gutes dargestellt werden. Außerdem auch Seiten, die zum Eintritt in Sekten und politisch radikale Gruppen einladen, sowie in gesellschaftliche Gruppen, die sehr fragwürdige politische oder ideologische Weltanschauungen haben.

Jugendmedienschutz umfasst aber noch viel mehr als technische und gesetzliche Einschränkungen. Der beste Schutz ist nämlich, wenn du selbst einschätzen kannst, welche Inhalte gefährlich und unangebracht sind, aber das ist so schwer, dass auch Erwachsene das nicht immer selbst einschätzen können. Auch technische Filter, die mit ➤Algorithmen arbeiten, können Fehler machen können und beispielsweise nicht alle gefährlichen Seiten sperren, dafür aber Seiten, die gar nicht so gefährlich sind. So ist beispielsweise die Videoplattform „YouTube“ an vielen Schul-

computern gesperrt, da dort gefährliche Videos gefunden werden können, aber gleichzeitig werden mit so einem Verbot auch lehrreiche und informative Videos gesperrt. An dem Beispiel lässt sich gut erkennen, dass Filterprogramme sich schnell im Bereich der ➤Zensur bewegen, also unter Kontrolle von vergleichsweise wenigen Menschen und Behörden gehalten werden, die bestimmen, was Kinder sehen dürfen und was nicht. Es gehört somit zum Jugendmedienschutz dazu, dass Kinder lernen, wie sie selbstständig, verantwortungsvoll und kritisch mit Medien umgehen können, selbst wenn sie auf ungeeignete Inhalte stoßen (➤Medienkompetenz).

Kettenbrief

Ein Kettenbrief ist eine Nachricht, die du an viele andere Menschen schickst, damit diese die Nachricht wieder an viele Menschen verschicken und sich die Nachricht möglichst weit verbreitet. Gerade bei Messenger-Diensten wie WhatsApp sind Kettenbriefe sehr beliebt. Dabei gibt es schöne Kettenbriefe wie zum Beispiel

> „Schicke diese Nachricht an 10 Menschen, die du lieb hast."

Aber auch sehr böse Kettenbriefe in denen etwas steht, wie:

> „Wenn du diese Nachricht nicht an 13 Leute weiterschickst, wirst du morgen von einem Auto überfahren."

Außerdem verbreiten sich auch Falschmeldungen über Kettenbriefe (➤Hoax), wie zum Beispiel „Schicke diese Nachricht an 5 Freunde, dann färben sich deine WhatsApp-Häkchen rot" oder „Wenn du diese Nachricht nicht an all deine Kontakte verschickst, wirst du bei WhatsApp gesperrt".

Wichtig: Du brauchst dir bei gruseligen Kettenbriefen keine Sorgen zu machen, dass dir, deiner Familie oder deinen Freunden etwas passiert, wenn du sie nicht weiterschickst. Die Geschichten sind alle ausgedacht! Schicke sie auf keinen Fall weiter, denn das ist unnötig und macht anderen Angst.

Künstliche Intelligenz

Künstliche Intelligenz (KI) ist ein sehr ungenauer Begriff. Früher versuchte die KI-Forschung Computerprogramme zu entwickeln, die wie ein Mensch lernen und Sprache verstehen. Heute wird mittels KI versucht Tätigkeiten, die Menschen im Moment noch besser erledigen können, durch Computer ausführen zu lassen. Beispiele dafür sind Gesichtserkennung und Übersetzungsprogramme.

Link

„Link" ist die Abkürzung von „Hyperlink". Wörtlich übersetzt heißt das so viel wie „Über-Verknüpfung", aber im übertragenen Sinne sind damit Querverweise gemeint.

Wenn du also einen Text im Internet liest und in diesem Text auf andere Internetseiten verwiesen wird, dann handelt es sich um Links. Wenn du zum Beispiel zu deiner Freundin sagst „Sag mir mal den Link vom Blog #Kids #digital #genial", dann meinst du eigentlich die ➤URL der ➤Webseite.

Linux

„GNU/Linux" oder kurz „Linux" ist ein freies ➤Betriebssystem. Das bedeutet, dass der ➤Quellcode der ➤Software offen zugänglich ist (➤Open Source). Es gibt viele verschiedene Versionen (Distributionen), zum Beispiel Debian und Ubuntu. Der Pinguin ist das typische Logo und Markenzeichen von Linux.

Login/Logout

„Login" und „Logout" sind die englischen Bezeichnungen für „Anmeldung" und „Abmeldung". Dabei kann es sich, zum Beispiel um die An-/Abmeldung aus Programmen oder ➤Sozialen Netzwerken handeln, bzw. überall, wo du einen ➤Account angelegt hast. Du solltest dich immer aus allen Programmen und Diensten abmelden, wenn du diese im Augenblick nicht nutzt, denn dann sind deine Daten besser geschützt und für ➤Hacker schlechter zugänglich.

Malware

„Malware" ist das englische Wort für ➤Schadsoftware.

Marketing ★

„Marketing" bezeichnet einen Berufsbereich, in dem es darum geht, Produkte oder Dienstleistungen zu vermarkten, also - wie es der Name schon sagt - auf den Markt zu bringen und zu verkaufen. Mit „Markt" ist natürlich nicht der Wochenmarkt auf dem Marktplatz in deiner Stadt gemeint, sondern alle Stellen, wo das entsprechende Produkt gekauft werden kann, zum Beispiel in Läden oder Online-Shops. Zu Marketing gehört die Aufstellung von Kalkulationen, also auszurechnen, wie viel ein Produkt in der Herstellung kostet, zu welchem Preis es verkauft werden soll, welche Gewinne zu erwarten sind und auch die Forschung darüber, wie gut die Produkte den Kund.innen gefallen. Im Kern geht es deshalb

um die Entwicklung von Werbung, um Produkte bekannter zu machen. Diese Werbung kann sehr unterschiedliche Formen haben und es ist wichtig, dass du ein paar Marketing-Tricks kennst, um zu verstehen, wie Werbung Menschen beeinflusst und zum Kaufen anregt. Du kannst in diesem Lexikon noch mehr über ➤personalisierte Werbung, ➤Online-Werbung und ➤Influencer-Marketing erfahren.

Wenn es darum geht, eine Person zu vermarkten, also beispielsweise eine Sängerin oder einen Schriftsteller bekannter zu machen, dann ist von „PR" (Public Relations) die Rede, was übersetzt „Öffentlichkeitsarbeit" heißt. Darunter fällt beispielsweise zu überlegen, was in der ➤Presse stehen soll, also welche Informationen genutzt und veröffentlicht werden, um die Person beliebt zu machen oder schlechte Dinge zu verbergen.

Medien

Mit "Medien" meinen viele die öffentliche Presse, das Radio und Fernsehen. Doch "Medien" (Einzahl: Medium) haben noch eine andere wichtige Bedeutung. Sie speichern, übertragen/vermitteln und verarbeiten Informationen.
Beispiele für Medien:

- Buch, Zeitung, Zeitschrift, CD, DVD, Blu-ray, Fernseher, Radio, Spielekonsole, Computer, Laptop, Internet, Smartphone, Tablet, ...

Diese können nochmals unterteilt werden in analoge und ➤digitale Medien. Häufig werden diese als alte oder neue Medien bezeichnet.

- Analoge Medien: Buch, Zeitschrift, ...
- Digitale Medien: e-Book, Computer, Smartphone, digitales Fernsehen...

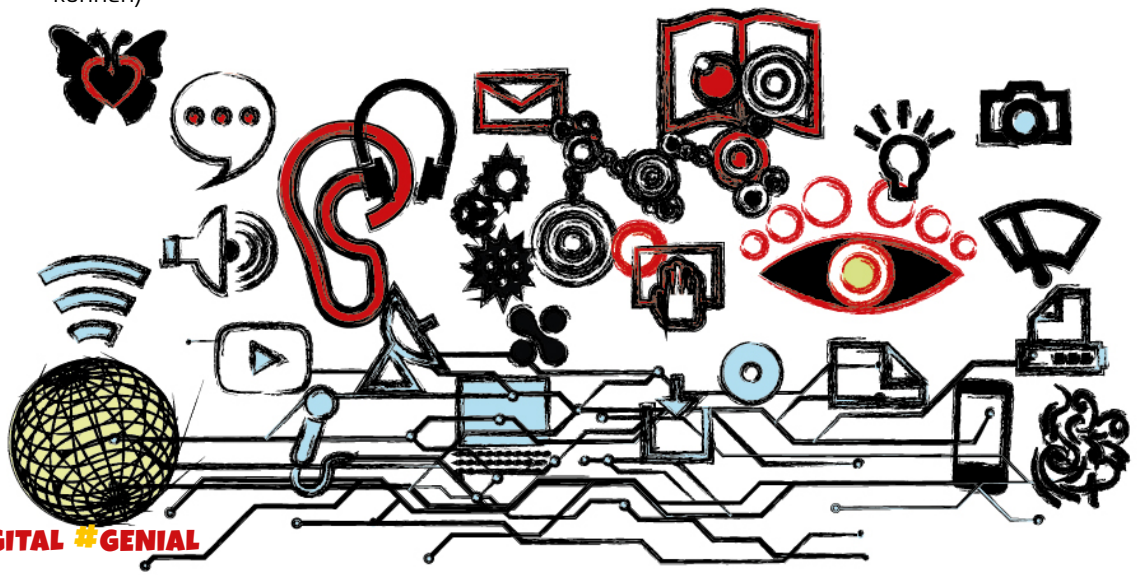
Außerdem können Medien auch nach Sinneskanälen kategorisiert werden:

- Auditive Medien (zum Hören): Kassette, CD, MP3, Radio, ...
- Visuelle Medien (zum Sehen): Foto, Zeitung, Zeitschrift, Buch, ...
- Audiovisuelle Medien (zum Hören und Sehen): Fernsehen, Video, ...
- Interaktive Medien (zum Interagieren): Computer, Internet, Smartphone, Tablet, ... (also Medien, die dir antworten können)

Medienkompetenz ★

„Medienkompetenz" bezeichnet die Fähigkeit, angemessen und sicher mit ➤Medien umgehen zu können. Der Pädagoge Dieter Baacke war einer der ersten, der diesen Begriff Ende der 1990er-Jahre verwendet hat und hat diesen in vier Bereiche unterteilt. Mittlerweile gibt es auch andere Erklärungen für Medienkompetenz, aber Baackes Beschreibung trifft den Begriff immer noch sehr gut:

1. Medienkritik: Dazu gehört das Wissen darüber, wie Medien auf Menschen wirken und dadurch zum Beispiel auch das Erkennen von Manipulationen. Hierbei geht es darum, sich vor den Nachteilen der Mediennutzung zu schützen. Im Vordergrund stehen die Inhalte in den Medien, nicht die Nutzung an sich.
2. Medienkunde: Damit ist das Wissen über die Funktionsweise gemeint, also wie beispielsweise ein Fernseher oder Computer funktioniert. Dazu gehört nicht nur technisches Wissen, sondern auch geschichtliches Wissen über die Entstehung und Weiterentwicklung von Medien, das Wissen wie Journalist.innen arbeiten und so weiter.
3. Mediennutzung: Dieses Wort meint die Nutzung von Medien in einem angemessen Ausmaß. Dazu gehört die Selbsteinschätzung, ab wann der Konsum von Medien ungesund wird.
4. Mediengestaltung: Dieser Begriff umfasst die eigenständige Produktion von Medien, z.B. von einem Zeitungsartikel, einer Radiosendung, einem Fernsehbeitrag, einem Hörspiel, ..., und betrifft somit das „Selbermachen" von Medien und Medieninhalten.



AUFGABE: Denk mal über deine eigene Medienkompetenz nach:
Medienkritik: Glaubst du, was in der Zeitung steht? Hast du schon mal ein Produkt gekauft, das von YouTuber.innen empfohlen wurde? Hast du schon mal einen ➤Link angeklickt, ohne zu wissen, welche Seite sich dahinter verbirgt? Hast du schon einmal einer Person im Chat geantwortet, die du nicht kanntest? Hast du schon mal einen ➤Kettenbrief weitergeleitet?
Medienkunde: Weißt du, was der Unterschied zwischen dem Internet und dem ➤World Wide Web ist? Hast du mal die Entstehung von Fotos zwischen einer analogen und digitalen Kamera verglichen? Weißt du, wann es das erste Smartphone gab? Hast du schon mal den ➤Quellcode einer Website untersucht?
Mediennutzung: Hast du schon mal bis tief in die Nacht gechattet, obwohl du müde wurdest? Bist du schon mal wütend geworden, weil du ein Spiel unterbrechen musstest? Hast du dein Handy schon mal ausgeschaltet, um nicht von anderen gestört zu werden?
Mediengestaltung: Hast du schon mal ein Hörspiel produziert? Hast du mal einen eigenen Blogbeitrag verfasst? Hast du schon mal Fotos vor einem Green Screen gemacht? Hast du schon mal eine Programmiersoftware genutzt?

Meme ★

Der Begriff „Meme" (englisch ausgesprochen wie „Theme") wird heute dafür verwendet, ein Internetphänomen zu beschreiben, das in den letzten Jahren in ➤Sozialen Netzwerken entstanden ist: Das Verschicken von witzigen Bildern, Sätzen und sogenannten „Insidern", also Witze, die nur bestimmte Personen verstehen, weil sie sich dabei an eine bestimmte Situation erinnert fühlen. Es wimmelt überall davon. Ein Beispiel dafür wäre ein Bild von einem Gesicht mit aufgerissenen Augen und einem lustigen Satz wie „Wenn du in dein Portmonnaie schaust." Gemeint ist damit, dass man genau so guckt, wenn man bei einem Blick ins Portmonnaie darüber erschrocken ist, wie wenig Geld da drin ist. Über dem selben Bild könnte auch stehen „Dieser Moment, wenn dir klar wird, dass du verschlafen hast." Der Kreativität bei Memes sind kaum Grenzen gesetzt.

Aber wusstest du, dass das Wort schon in den 1970er-Jahren verwendet wurde? Das Wort „Mem" wurde von dem Wissenschaftler Richard Dawkins genutzt, um einen einzelnen Gedanken zu beschreiben. Er ging in seiner Bewusstseinstheorie, beziehungsweise „Memtheorie" („Mem" abgeleitet von „memory" = Erinnerung), davon aus, dass ein reiner Gedanke erst durch die Weitergabe an andere eine Bedeutung bekommt. Während der Weitergabe des Gedankens oder der Information an andere Menschen, verändert sich die Bedeutung des Inhalts. Du kannst dir die Veränderung des Begriffs ähnlich vorstellen, wie bei dem Spiel „Stille Post". Ob diese Theorie so stimmt, ist bis heute aber noch unklar, deshalb hat sich die Theorie nicht sehr weit verbreitet.

Aufgabe: Hast du in letzter Zeit Memes verschickt oder geschickt bekommen? Hast du den Witz immer verstanden? Haben andere den Witz genauso verstanden wie du? Denk mal darüber nach, ob dir Ähnlichkeiten zu der Theorie von Richard Dawkins auffallen. Hat die heutige Verwendung des Begriffs noch etwas mit der Theorie von damals zu tun?

Metadaten

„Metadaten" sind ➤Daten über Daten. („Drüberdaten") Wenn du zum Beispiel ein Foto mit deinem Handy machst, dann werden in diesem Foto Datum und Uhrzeit der Aufnahme gespeichert, aber auch mit welchem Gerät das Foto aufgenommen wurde und eventuell wo das Foto geschossen wurde. Unter Metadaten versteht man aber auch Datenbanken, zum Beispiel eine Liste über die Bücher in einer Bibliothek, in denen alle Autoren und Titel vermerkt sind. Man kann also sagen: Metadaten sind Informationen über andere Daten.

Multimedia

„Multi" ist das lateinische Wort für „viele" und „media" das englische Wort für ➤„Medien". Zusammengesetzt bedeutet es also „viele Medien". Die Bezeichnung wird verwendet, wenn ein ➤digitales Gerät mehrere Medien vereint, die unterschiedliche Sinne ansprechen, zum Beispiel lesen (visuell – mit den Augen) und hören (auditiv – mit den Ohren). Doch allein dieser Aspekt reicht noch nicht aus, um als multimedial bezeichnet zu werden: Es müssen auch verschiedene Interaktionsmöglichkeiten vorhanden sein, also Kommunikationswege zwischen dem Gerät und dem Nutzer/der Nutzerin, zum Beispiel über eine Fernbedienung oder Sprachsteuerung.

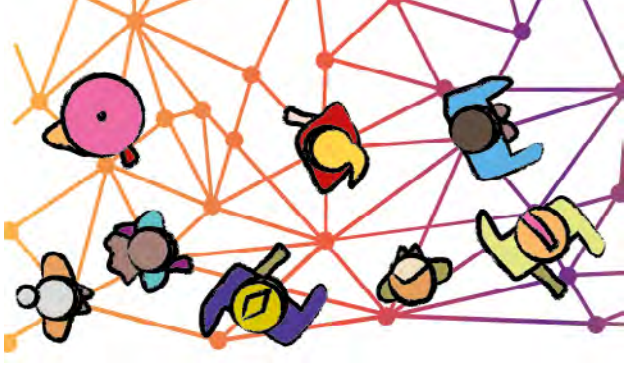
Netiquette

Das Wort „Netiquette" setzt sich zusammen aus dem englischen Wort „net" (Deutsch: „Netz" oder auch „Internet") und „Etiquette" (= respektvolles Benehmen) und wird für die Kommunikation im Internet, besonders in ➤Sozialen Netzwerken, verwendet. Denn im Internet soll man mindestens genauso respektvoll mit Menschen kommunizieren, wie im echten Leben, und daher einige Höflichkeitsregeln beachten.

Grundsätzlich gilt: Behandle andere so, wie du selbst behandelt werden möchtest, und bleib anderen gegenüber respektvoll. Denn du hast zwar nur einen Bildschirm vor dir, aber deine Nachrichten kommen bei realen Menschen an.

Netzneutralität

„Netzneutralität" (Englisch: „net neutrality") meint, dass Datennetze neutral sind (nicht zwischen Daten unterscheiden) und dies auch bleiben sollen. Es soll egal sein, welche ➤Daten über Computernetze oder das Internet übertragen werden. Netzbetreiber sollen keinen Einfluss darauf haben, welche Daten durch ihre Netze geschickt werden. Es könnte sonst beispielsweise passieren, dass ein Netzanbieter keine Video-Telefonie zulässt, weil die Übertragung mit einem größeren Datenaufkommen verbunden ist, als zum Beispiel das Verschicken von einem Bild. Oder vielleicht werden Daten von großen Firmen, die viel Geld



dafür bezahlen, als „wichtiger“ eingestuft als die Daten von Privatpersonen und deshalb schneller übermittelt. Dies würde auch bedeuten, dass einige Daten als „gut“ und andere als „schlecht“ eingestuft werden. Anbieter im Internet, deren Daten als schlecht eingestuft werden, würden demnach nachteilig behandelt werden. Es würde eine Diskriminierung von Daten stattfinden und somit eine Klassen-Teilung des Internets, wodurch das Internet seinen Charakter verlieren würde und ganz anders sein würde als jetzt – nicht mehr so frei und offen. Es gibt immer wieder Firmen oder Politiker.innen, die das Netz anders strukturieren wollen und Menschen, die sich dafür einsetzen, dass die Datenübertragung fair und neutral bleibt – die also für Netzneutralität kämpfen.

Newsletter

„Newsletter“ bedeutet übersetzt Nachrichtenbrief. Es gibt Newsletter in gedruckter Form per Post und am häufigsten per E-Mail. Verschiedene Unternehmen, Geschäfte und Institutionen halten damit ihre Kundschaft und interessierte Menschen auf dem neusten Stand.

Doch bei Newslettern besteht häufig ➤Spam-Gefahr. Nicht immer sind die Empfänger.innen damit einverstanden, dass sie regelmäßig über neue Angebote informiert werden, wenn sie nicht darum gebeten haben. Daher müssen die Absender.innen der Newsletter erst eine Erlaubnis einholen, um den Neuigkeitenbrief regelmäßig verschicken zu dürfen. Diese Erlaubnis versteckt sich manchmal in den ➤AGB, wenn du dir z.B. einen ➤Account für einen Online-Shop anlegst. Im Optimalfall kannst du selber anklicken, ob du einen Newsletter bekommen möchtest (➤Opt-in), aber es kommt auch vor, dass das entsprechende Feld von vorne hinein angeklickt ist, und du das Häkchen entfernen musst, um den Newsletter nicht zu bekommen (➤Opt-out).

Wenn du einen E-Mail-Newsletter wieder abbestellen möchtest, musst du bis an das Ende der Mail scrollen, denn dort ist meistens ein ➤Link angegeben, unter dem du den Newsletter wieder abbestellen kannst oder zumindest eine Angabe, wie du die Zusendung des Newsletters stoppen kannst.

TIPP: Leg dir am besten eine E-Mail-Adresse an, die du nur für Newsletter verwendest. Wenn du diese Mails mit deinen anderen wichtigen E-Mails vermischst, kann es leicht passieren, dass wichtige Mails in der Menge untergehen. Außerdem weißt du dann immer auf einen Blick, welche Newsletter du bestellt hast.

Nickname

Ein „Nickname“ ist ein Spitzname, den man sich als Benutzernamen zulegt (und hinter dem man seinen Klarnamen verbirgt) wenn man sich einen ➤Account anlegt.

Online-Werbung

Es gibt viele verschiedene Formen der Werbung im Internet, die nicht immer klar als solche zu erkennen sind, zum Beispiel:

- Banner: Werden an verschiedenen Stellen in Apps oder auf Webseiten eingebaut und fallen häufig durch bunte, bewegte Bilder und Schrift auf.
- Pop-ups: Zusätzliche Fenster/Tabs, die sich öffnen, wenn du etwas anklickst.
- Overlays: Fenster, die sich öffnen und vor den eigentlichen Inhalt legen. Diese musst du mit [x] schließen. Teilweise wird das Symbol auch als Fake in das Bild eingebaut, sodass du die Werbung öffnest, wenn du darauf klickst und das richtige [x] ist etwas schwerer zu finden. Manchmal huscht auch eine Werbung ohne zu klicken von links nach rechts über den Bildschirm („Unterbrecherwerbung“). Nervig!
- Gesponserte Meldungen: Die Unternehmen bezahlen die Webseiten-Betreiber dafür, dass ihre Werbung gezeigt wird. Diese Werbung wird als „gesponsert“ gekennzeichnet und ist häufig bei ➤Sozialen Netzwerken wie Facebook oder Instagram zu finden. Sie ist oft leicht mit „normalen“ Postings zu verwechseln.
- Suchmaschinenwerbung: Die ersten Treffer in der Suchmaschine sind meist Werbeanzeigen und auch mit „Anzeige“ gekennzeichnet. Hier zahlen die Unternehmen Geld dafür, dass ihre Seite ganz oben genannt wird, wenn jemand nach bestimmten Begriffen sucht.
- In-Game-Werbung: Damit ist Werbung innerhalb von Spielen gemeint, die zum Beispiel zu ➤In-App-Käufen anregt. Manche Spieler.innen werden auch damit gelockt, dass sie Extrapunkte bekommen, wenn sie nur auf die Werbung klicken.

So kannst du dich vor lästiger Werbung schützen:

- **Werbeblocker einschalten:** Stell in den ➤Browser-Einstellungen ein, dass Pop-ups nicht zugelassen werden und installiere einen Ad-Blocker (Werbeblo-

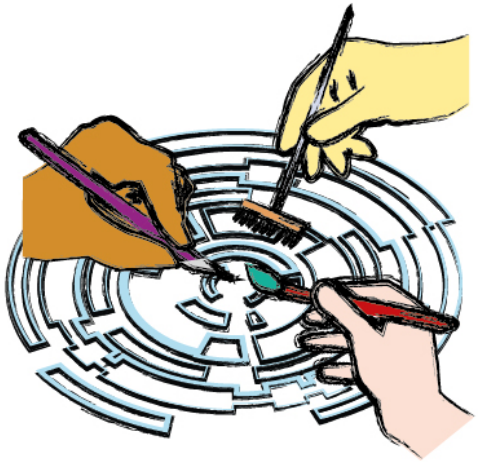
cker), wie zum Beispiel „u Block Origin“, damit Werbeanzeigen von vornherein unterbunden werden. Achte außerdem darauf, dass eine ➢Firewall aktiviert ist, die ebenfalls Werbung abwehren kann.

- **Coockies deaktivieren:** Manche Unternehmen wissen so gut über dich Bescheid, dass sie dir und nur dir bestimmte Werbung anzeigen. Das wissen sie meist über ➢Cookies. Deaktiviere die ➢Cookies im Browser, damit möglichst wenig Daten von dir gespeichert werden.
- **Kostenpflichtige Apps im Gegensatz zu kostenlosen Apps:** Kostenpflichtige Apps enthalten meist weniger Werbung, da sie sich nicht durch Werbeeinnahmen finanzieren müssen. Vielleicht lohnt es sich bei der ein oder anderen App, auch mal Geld auszugeben? Besprich das aber vorher unbedingt mit deinen Eltern!
- **Gewinnspiele:** Nimm nicht an Gewinnspielen teil, denn die sind oft nur Fake, sodass es gar nichts zu gewinnen gibt. Es geht bei Gewinnspielen fast immer darum, dass Unternehmen an deine persönlichen Daten, wie zum Beispiel deine E-Mail-Adresse, kommen, um dir dann noch mehr Werbung zuzuschicken.
- **Abonnements:** Kostenlose Geschenke sind oft mit Abo-Fallen, also mit versteckten Verträgen, verbunden. Du denkst, dass du etwas kostenlos bekommst, doch schließt aus versehen ein ➢Abonnement ab. Lies immer das Kleingedruckte (➢AGB)! Umsonst bekommst du sowieso gar nichts, denn oft musst du zumindest bestimmte Daten von dir eintragen, um ein Geschenk zu bekommen. Wenn du also nicht direkt mit Geld bezahlst, dann zumindest mit deinen Daten, die du den Unternehmen hinterlässt.

Open Source

Der Begriff „Open Source“ (Deutsch: „offene Quelle“) wird für Programme, also für ➢Software, verwendet, die ihren ➢Quellcode/Quelltext öffentlich darlegen, sodass alle, die Lust haben, an dem Programm mitarbeiten kann. Manchmal wird auch der Begriff „freie Software“ verwendet, doch die Nutzung von freier Software kann manchmal etwas kosten.

Vorteil: Wenn ein Programm so geschrieben ist, dass es bestimmte Daten von dir sammeln/auslesen kann, dann kann jemand, der/die ein bisschen Ahnung auf diesem Gebiet hat, dies anhand des öffentlichen Quelltextes schnell he-



rausfinden, die entsprechenden Befehle oder ➢Algorithmen herauslöschen/ändern und somit deine ➢Privatsphäre schützen.

Beispiele für freie Software, die du verwenden solltest:
„Libre Office“, statt „Microsoft Word“ (➢Microsoft), „OpenStreetMap“, statt „GoogleMaps“, „Gimp“, statt Photoshop, „VLC, statt „Mediaplayer“, …

Opt-in/out

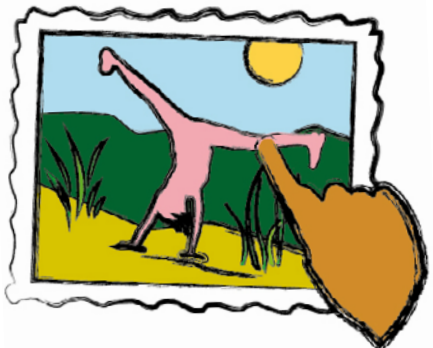
Opt-in und -out sind Bezeichnungen für Auswahlmöglichkeiten. Wenn du dir beispielsweise einen ➢Account für einen Online-Dienst einrichtest (zum Beispiel für ein Spiel oder ein Profil in einem ➢Sozialen Netzwerk), musst du oft noch weitere Felder anklicken, zum Beispiel ob du den ➢AGB zustimmst oder ob du einen ➢Newsletter bekommen möchtest. Wenn du die Felder selbst anklickst und auswählst, handelt es sich um das so genannte „opt-in“ (Option „aktiv rein“). Wenn die Felder schon vorher angehakt sind und du sie ausdrücklich abwählen musst, dann handelt es sich um „opt-out“ (Option „aktiv raus“).

Du musst dir also solche Auswahlfelder immer genau anschauen und die Texte ganz genau lesen, um zu sehen, ob du ein Häkchen setzen oder entfernen solltest. Sonst kann es sein, dass du aus Versehen Dingen zustimmst, die du gar nicht möchtest. Manchmal wird auch mit (doppelten) Verneinungen getrickst, sodass du zum Beispiel ein Feld auswählen musst, um einen Newsletter NICHT zu bekommen.

Außerdem gibt es noch das so genannte „Double-opt-in“, also ein doppeltes Opt-in. Dieses Verfahren begegnet dir beispielsweise beim Abonnieren von Newslettern oder wenn du eine Bestellung tätigst: Du bekommst dann zunächst eine Mail zugeschickt, in der du deine Anmeldung/Bestellung noch einmal bestätigen sollst. So sollte es jedenfalls sein, denn in Deutschland ist das Double-opt-in für Newsletter Pflicht. Gäbe es keine zusätzliche Bestätigungsmail, könnte zum Beispiel jede Person jede E-Mailadresse für jeden Newsletter anmelden. Da wäre jede Menge ➢Spam vorprogrammiert.

Pädophilie

„Pädophilie“ ist eine psychische Erkrankung, bei der Erwachsene erotische Fantasien mit Kindern (und sogar mit Babys) entwickeln. In den meisten Fällen handelt es sich um Männer, die sich Zuneigung oder sexuelle Praktiken von/mit Kindern wünschen (sowohl mit Mädchen als auch mit Jungen). Aber auch Frauen können pädophil sein. Die Krankheit fällt in den Bereich der Sexual- und Persönlichkeitsstörungen und kann mit Therapien behandelt werden. Die sexuelle Orientierung aber bleibt.



Nicht alle Pädophile werden zu Straftäter.innen, aber im Internet haben sie grundsätzlich viele Möglichkeiten, ihre Fantasien auszuleben, da sie zum Beispiel sehr einfach an Fotos von Kindern herankommen und diese Fotos regen ihre Fantasie an. Daher ist es für sie besonders interessant, wenn du Urlaubsfotos von dir hochgeladen hast, auf denen du zum Beispiel nur im Bikini oder in einer Badehose zu sehen bist. Aber auch ganz normale Profilfotos sind für Pädophile interessant. Besonders gefährlich wird es jedoch, wenn ihnen die Fotos irgendwann nicht mehr ausreichen und sie versuchen, Kontakt zu dir aufzunehmen, zum Beispiel über einen Chat. In den meisten Fällen geben sie natürlich nicht ihren richtigen Namen und ihr richtiges Alter an, denn das, was sie da tun, ist nicht erlaubt! Außerdem würdest du wahrscheinlich nicht freiwillig mit einer älteren Person schreiben. Durch regelmäßiges Schreiben gewinnt die Person langsam dein Vertrauen und verlangt vielleicht irgendwann Nacktfotos von dir oder schlägt eventuell sogar ein Treffen vor. Die erste Stufe dieser Kontaktaufnahme nennt sich ➢Cybergrooming.

Deshalb darfst du dich auf gar keinen Fall alleine mit fremden Personen treffen, die du im Internet kennengelernt hast! Sag auf jeden Fall immer einem Erwachsenen Bescheid, auch schon dann, wenn dir ein Kontakt komisch vorkommt.

PayPal

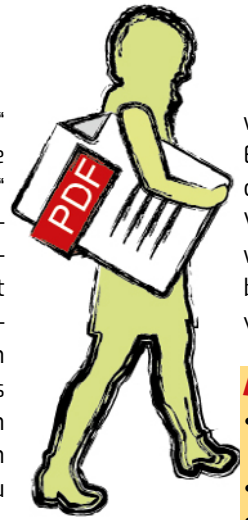
„PayPal" ist ein Online-Bezahlsystem, das wie ein Zwischenhändler bei Online-Käufen funktioniert, sodass du mit deinen Kontodaten anonym bleibst. Du meldest dich bei PayPal mit einer E-Mail-Adresse und deinen Kontodaten an, und wenn du irgendwo einkaufen möchtest, dann zieht PayPal das Geld von deinem Konto ein und überweist es an denjenigen weiter, der dieses Geld bekommen soll. Somit hinterlegst du deine Kontodaten nur bei PayPal und nicht in zahlreichen verschiedenen Online-Shops.

Es kann Dir auch jemand Geld auf dein PayPal-Konto überweisen, wenn du selber etwas verkauft hast. Dazu braucht der Käufer nicht deine Kontonummer, sondern nur deine E-Mail-Adresse, und PayPal kann dir die Zahlung dadurch zuweisen. Wenn du auf diesem Wege Geld

bekommst, bezahlst du dafür jedoch eine Gebühr.

Wichtig: Du verteilst deine Kontodaten somit nicht an verschiedenen Stellen, bei denen du nicht ganz sicher sein kannst, ob sie dort sicher sind, aber dafür sammelt PayPal viele Daten von dir und verkauft diese Informationen an weitere Firmen. In den meisten Fällen bekommt PayPal nicht nur die Information darüber, wann und in welchem Warenwert du eingekauft hast, sondern auch eine Liste der einzelnen Artikel, die du bestellt hast. So sensible Daten über dich, solltest du nicht mit solch einem großen Unternehmen teilen.

PDF



Die Abkürzung „PDF" steht für „Portable Document Format" (Deutsch: „(trans)portables Dokumentenformat"). Es handelt sich um ein Dateiformat, das auf jedem Computer und als Ausdruck von jedem Drucker immer gleich aussehen soll. Du brauchst aber ein Programm, das PDF-Formate öffnen kann.

Wenn du ein Textdokument mit einem Schreib-Programm schreibst und es danach mit einem anderen Text-Programm öffnen willst, dann kann es passieren, dass sich die Formatierung verschiebt oder Schriftarten anders angezeigt werden. Dies sollte bei einer PDF-Datei nicht passieren. Aber dafür lässt sich die Datei auch nur schwer bearbeiten, wenn zum Beispiel Rechtschreibfehler drin sind.

Es gibt aber auch Programme, mit denen PDF-Dokumente bearbeitet werden können. Das Datei-Format leistet somit keinen endgültigen Kopier- oder Missbrauchs-Schutz.

Außerdem sind PDF-Dokumente meist relativ klein in Bezug auf die Dateigröße, was zum Beispiel den Versand über E-Mails erleichtert. Die Dokumentgröße, die erschwerte Manipulation und der Verzicht auf Papier, sind der Grund dafür, wieso viele Arbeitgeber nur noch Bewerbungen per E-Mail und im PDF-Format verlangen.

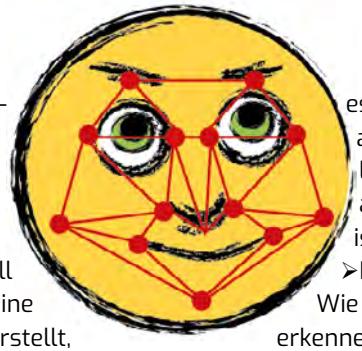
AUFGABE: Erstelle eine PDF-Datei!

- Öffne ein Textbearbeitungsprogramm, zum Beispiel „Libre Office".
- Schreib ein paar Zeilen darin.
- Klicke oben links auf „Datei".
- Speichere die Datei unter einem Namen ab.
- Wähle „Als PDF exportieren".
- Jetzt musst du dir nur noch merken oder nachsehen, in welchem Order das Dokument gespeichert wird, damit du es wiederfindest.
- Vergleiche die Textdatei und die PDF-Datei – sind sie gleich groß?

Es gibt auch Programme, mit denen du verschiedene PDF-Dokumente zu einem einzigen Dokument zusammenführen kannst, zum Beispiel „PDF Chain" oder „PDF Blender". Schau dir die Programme mal mit deinen Eltern an und probier sie aus. Sie werden dir in Zukunft ganz bestimmt nützlich sein.

Personalisierte Werbung

Personalisierte Werbung nennt man Werbung, die genau auf dich und deine Interessen zugeschnitten ist. Du gibst beim Surfen im Internet viele Daten von dir preis, nicht nur, was deine direkten Interessen betrifft (zum Beispiel durch das Klicken auf „Like"-Buttons), sondern auch durch dein Surfverhalten selbst. Es wird zum Beispiel oft gespeichert, wie lange du auf einer Seite surfst oder ob du dabei von unterwegs oder von zu Hause aus surfst. Außerdem können



➤Algorithmen erkennen, ob du viel oder wenig Geld hast, ein Mädchen oder ein Junge bist und noch vieles mehr. Aus all diesen Daten wird eine Profilanalyse von dir erstellt, die Unternehmen dabei hilft, dir Werbung anzuzeigen, die dich interessieren könnte. Klingt gut? Nein, ist es überhaupt nicht! Vielleicht würden dir ja ganz andere Dinge gefallen, wenn du nicht genau diese Werbung angezeigt bekommen würdest. Mädchen bekommen durch diese Analyse zum Beispiel eher Produkte mit Prinzessinnen-Aufdruck angezeigt und Jungen Produkte zu Fußball, aber es stimmt überhaupt nicht, dass nur Jungen sich für Fußball interessieren. Du wirst dadurch also gelenkt und manipuliert, um möglichst viel Geld auszugeben. Außerdem ist es ein Eingriff in deine ➤Privatsphäre.

Wie du Werbung im Internet erkennen und dich davor schützen kannst, kannst du im Beitrag über ➤Online-Werbung nachlesen.

Personalisierte Werbung kann allerdings auch schon über Kameras und Gesichtserkennung, also außerhalb des ➤WWW, realisiert werden. So ist es beispielsweise bald möglich, dass du in einem Supermarkt an der Kasse stehst, von einer Kamera gefilmt wirst und dann an den digitalen Werbetafeln an der Kasse personalisierte Werbung angezeigt bekommst.

Petition

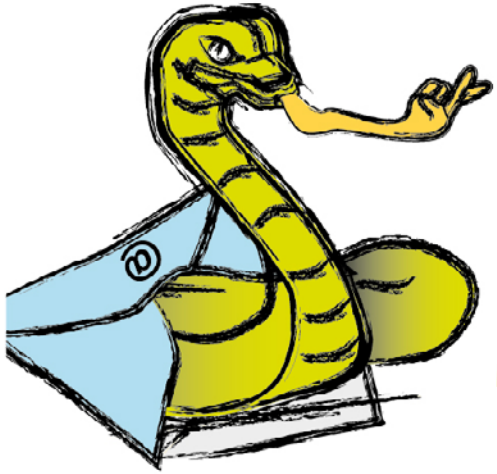
Eine „Petition" ist ein Schreiben in Form einer Bitte oder einer Beschwerde von vielen Menschen, die bei einer Behörde oder einer ähnlichen zuständigen Stelle eingereicht wird. Die Menschen, die diese Bitte oder Beschwerde unterstützen möchten, unterschreiben das Schriftstück und stehen somit mit ihrem Namen für das Anliegen ein. Man kann sich auch online an Petitionen beteiligen, doch hier muss auf jeden Fall vorher gut geprüft werden, ob es sich um eine rechtskräftige Petition handelt und was mit den persönlichen Daten passiert, die man auf der entsprechenden Seite einträgt.

Phishing

„Phishing" bezeichnet eine Betrugsmasche im Internet, hauptsächlich über E-Mails. Dabei werden Internetseiten konstruiert, die genauso aussehen, wie die eines seriösen Unternehmens, meist von einer Bank (Sparkasse, Volksbank, Deutsche Bank und so weiter), von Online-Shops oder anderen Unternehmen, bei denen es um Geld geht (zum Beispiel ➤PayPal). Diese Seiten unterscheiden sich nur beim genauen Hinsehen vom Original.

Du bekommst dann eine Mail, zum Beispiel von einer Bank, mit einem ➤Link und der Bitte, dich einzuloggen und dir wichtige Informationen durchzulesen. Oder du sollst dich einloggen, weil angeblich jemand eine hohe Summe von deinem Konto abgebucht hat. Die Vorwände sind unterschiedlich, aber es geht immer nur darum, dass du dich auf der gefälschten Seite mit deinem echten Benutzernamen und Passwort anmeldest, damit das dann ausgelesen werden kann. Solltest du mal auf einen Phishing-Trick reinfallen, musst du unbedingt schnell dein Passwort ändern und solltest dein Konto sperren lassen.

TIPP: Achte genau auf den Absender der Mail. Oft kannst du die Betrugsmasche direkt erkennen, wenn der Absender aus dem Ausland ist, oder ein privater Name, statt dem Namen der Bank. Häufig sind auch viele Rechtschreibfehler enthalten oder die Mail-Adresse des Absenders sieht komisch aus (zum Beispiel mit vielen Zahlen drin). Noch auffälliger ist es, wenn du mit dem Unternehmen eigentlich gar nichts zu tun hast, weil du zum Beispiel bei einer ganz anderen Bank bist. Du solltest diese Mails dann einfach löschen, dann kann nichts passieren.



Phubbing ★

„Phubbing", das sich aus „phone" und „snubbing" zusammensetzt („Telefon" und „jemanden vor den Kopf stoßen") ist ein Wort, das ausgedacht wurde, um das unhöfliche Verhalten zu beschreiben, wenn jemand sich in einer Gruppe von Leuten nur mit dem Smartphone beschäftigt. Das Wort ist für eine australische ➤Marketing-Kampagne verwendet worden und deshalb kein weit verbreiteter oder wissenschaftlicher Begriff. Trotzdem taucht er immer wieder mal auf, wenn es darum geht, dass Menschen zusammen an einem Tisch sitzen und nur auf ihr Smartphone schauen, oder andere Menschen sogar gezielt ignorieren, um etwas auf ihrem Smartphone zu lesen.

AUFGABE: Bist du schon einmal ignoriert worden, weil jemandem das Smartphone in dem Moment wichtiger war? Wie hast du dich dabei gefühlt? Hast du vielleicht selbst schon Leute vernachlässigt, um etwas an deinem Smartphone zu erledigen? Mach mal zusammen mit einer Freundin oder einem Freund ein Experiment und lasst eure Smartphones in der Tasche, wenn ihr euch verabredet. Ihr könnt danach miteinander darüber sprechen, ob ihr zukünftig öfter darauf verzichten wollt.

Plug-in

Ein „Plug-in“ (vom englischen „to plug in“ = „einstöpseln“), oder auch Add-on, ist eine Zusatzfunktion für eine bereits installierte ➤Software. Ein Plug-in ist demnach selbst auch eine kleine Software und du kannst diese zum Beispiel in deinem ➤Browser installieren und sozusagen in dem Programm zusätzlich einstöpseln. Ein nützliches Plug-in für den Browser ist beispielsweise ein Werbeblocker (wie zum Beispiel u Block Origin), der verhindert, dass dir Werbung über Pop-Up-Fenster angezeigt wird. Du musst bei der Installation von Plug-ins allerdings vorsichtig sein, da nicht jedes Plug-in sinnvoll ist und weil es vorkommen kann, dass in ihnen ➤Schadsoftware integriert ist. Außerdem sammeln manche Plug-ins viele Daten von dir.

Posting ★

Das Wort „Post“ oder „Posting“ meint das Abschicken oder Bereitstellen von etwas. Hier ist damit das Verfassen und Abschicken eines Beitrages/einer Nachricht zum Beispiel in einem ➤Sozialen Netzwerk oder ➤Forum gemeint. Das können Texte, Bilder oder Videos sein. Der Begriff etwas „posten“ (englisch ausgesprochen) wird mittlerweile für die Veröffentlichung verschiedener Texte im Internet verwendet, egal, ob es sich dabei um private Bilder, Beiträge auf den eigenen Seiten, journalistische Texte, Blog-Beiträge, Kommentare oder ➤Links handelt. Besonders im Marketing-Bereich, zum Beispiel bei ➤Online-Werbung, ist häufig von „Crossposting“ (über Kreuz posten) die Rede. Damit ist gemeint, dass ➤Links zu ein und derselben ➤Webseite in verschiedenen Sozialen Netzwerken verbreitet werden, um mehr Leser.innen auf die Seite hinzuweisen. Mehrere Postings hintereinander, die sich aufeinander beziehen, werden als ➤Thread (Erzählstrang) bezeichnet.

Aufgabe: Bei Instagram werden täglich etwa 95 Millionen Bilder gepostet. Bei Twitter werden 6000 Tweets pro Sekunde abgesetzt. Bei Snapchat werden täglich fast vier Milliarden Snaps verschickt. Bei Facebook sind es 60 Millionen Bilder pro Tag (die Zahlen stammen aus verschiedenen Statistiken etwa Ende des Jahres 2017). Wie viel postest du täglich? Beobachte deine eigenen Postings mal über eine Woche und überlege, was sie dir und anderen bringen. Übermittelst du damit wichtige Informationen? Vertreibst du dir damit die Langeweile? Könntest du auf den ein oder anderen Post auch verzichten?

Prepaid

„Prepaid“ ist Englisch und bedeutet „vorausbezahlt“. Es handelt sich dabei also um eine Zahlungsvariante, zum Beispiel in Form einer Guthabenkarte. Viele benutzen Prepaid-Karten für das Handy, statt einen Vertrag zu festen Konditionen abzuschließen. Sobald das Guthaben aufgebraucht ist, muss es wieder aufgeladen werden, sonst können kostenpflichtige Funktionen, wie zum Beispiel Telefonanrufe, nicht genutzt werden. Dadurch kann man, anders als bei einem Vertrag, bei dem man ein Mal im Monat eine Rechnung bekommt, begrenzen, wie viel Geld man ausgegeben will. Man ist außerdem nicht an eine bestimmte Laufzeit gebunden und hat auch kein ➤Abonnement abgeschlossen. Wenn du beispielsweise mal deine Handynummer ändern möchtest, dann geht dies viel einfacher, als wenn du darauf warten musst, dass du den Vertrag kündigen kannst.

Presse ★

„Presse“ ist ein Oberbegriff für Nachrichtenmedien. Früher waren damit Zeitungen, Plakate, Bücher und alle ➤Medien gemeint, die mit Druckerpressen hergestellt wurden. Später kamen Radio und Fernsehen als Nachrichtenmedien hinzu, danach auch das Internet. Somit bezeichnet „Presse“ heute alle Medien, die eine große Masse an Menschen mit journalistischen Inhalten erreichen (Massenmedien) – egal, ob sie noch auf Papier erscheinen oder nur noch elektronisch.
In Deutschland haben wir heute zum Glück die Presse-, Meinungs- und Informationsfreiheit, die im Grundgesetz festgesetzt sind. Das heißt wir alle – und insbesondere Journalist.innen – dürfen unsere Meinung in schriftlichen Texten, Gesprächen, Ton- und Videoaufnahmen und in anderen Kunstwerken (zum Beispiel Comics oder Bildern) frei äußern, ohne dafür bestraft zu werden, auch wenn wir eine schlechte Meinung von etwas haben. Dies gilt natürlich nicht für Inhalte, die Menschen unnötig/unbegründet schaden (zum Beispiel beleidigen) oder ganz bewusst Lügen verbreiten (Verleumdung oder ➤Fake News). Welche Freiheiten es gibt, ist aber in jedem Land unterschiedlich. Mehr dazu kannst du im Beitrag über ➤Zensur lesen.

Privatsphäre

Deine Privatsphäre ist dein persönlicher, nichtöffentlicher Bereich, indem du dich frei entfalten kannst. Solange du nichts Illegales/Strafbares oder Gefährliches machst, braucht es niemanden zu interessieren, was du in pri-

vaten Momenten und privaten Räumen tust. Die privatesten Bereiche sind zum Beispiel Toiletten und Duschen, Umkleidekabinen, Schlaf-/Kinderzimmer und andere Wohnräume.

Privatsphäre gehört zu den Grundrechten jedes Menschen. Auch Kinder haben ein Recht auf Privatsphäre! Auch vor deinen Eltern und Geschwistern darfst du Geheimnisse haben. In gewisser Hinsicht machen deine Geheimnisse dich zu der Person, die du bist.

Leider gibt es einige Technologien, die in die Privatsphäre des Menschen eindringen, indem sie Daten, also Informationen über dich sammeln, die sie gar nichts angehen. ➢Cookies zum Beispiel helfen Firmen, dich durchs Internet zu verfolgen (➢Tracking) oder Videokameras mit Gesichtserkennung erkennen dich immer, wenn sie dich erwischen, auch wenn du vielleicht gar nicht zugestimmt hast.

Außerdem kannst du grundsätzlich davon ausgehen, dass Informationen, die du über dich im Internet verbreitest, ab dem Moment, indem du sie abschickst, nicht mehr privat sind. Die meisten Sozialen Netzwerke bieten in ihren Einstellungen ein paar Möglichkeiten an, um die Privatsphäre zu schützen und diese solltest du auf jeden Fall richtig einstellen!

Schütze deine Privatsphäre! Wieso du dies unbedingt tun solltest, erfährst du unter ➢Datenschutz.

Proprietäre Software ★

„Proprietär" bedeutet „in Eigentum befindlich", also jemandem gehörend. Wenn das Wort in Bezug auf ➢Software verwendet wird, was häufig der Fall ist, dann ist damit das Gegenstück zu Freier Software oder ➢Open Source gemeint. Das bedeutet, dass der ➢Quelltext, also der Bauplan einer Software, einer Person oder einer Firma gehört und gar nicht oder nur teilweise öffentlich verraten wird, ähnlich wie bei einem Geheimrezept. Das bedeutet natürlich auch, dass schwerer herauszufinden ist, ob sich beispielsweise eine ➢Schadsoftware als „Zutat" in dem Programm befindet.

Push-Benachrichtigung

Wenn du ➢Apps auf deinem Smartphone oder Tablet benutzt ist
dir bestimmt schon einm
Frage begegnet "Möchte
Push-Nachrichten erhal
Damit sind die Benachr
gungen gemeint, die auf
nem Sperr- oder Startl
schirm des Smartpho
erscheinen. Diese können teilweise nützlich sein, um zu sehen, wenn du
neue Nachricht
on Freunden
oder von deinen
Eltern bekom-
men hast. Sie
önnen aber auch
ehr nerven, wenn

du beispielsweise immer darüber informiert wirst, wenn irgendjemand deiner Freunde etwas Neues gepostet hat, die App irgendeine neue Funktion für dich bereithält oder ➢Online-Werbung eingeblendet wird; und das 20 mal am Tag.
Du kannst diese Push-Benachrichtigungen in den App-Einstellungen ausschalten und das solltest du auch tun! Lass dich nicht dauernd stören und schalte die Benachrichtigungsfunktion nur für wirklich wichtige Dinge ein, zum Beispiel wenn Du auf eine dringende Nachricht wartest. Außerdem verbraucht die Funktion viel Akkukapazität, da die App die ganze Zeit im Hintergrund laufen muss, um dir die Benachrichtigungen im richtigen Moment anzuzeigen.

QR-Code

QR steht für „Quick Response", also „schnelle Antwort". QR-Codes funktionieren ähnlich wie Strichcodes und können mit bestimmten Geräten und Programmen ausgelesen werden. Die weißen und schwarzen Punkte ergeben einen Code, den ein Mensch nicht einfach lesen kann, doch Computer können diesen Code (Binärcode) entschlüsseln.

Wichtig: Wenn du dir einen QR-Code-Reader, also einen QR-Code-Leser auf dein Smartphone lädst, kannst du deine Kamera an den Code halten und diesen auslesen. Du kannst dir aber nie sicher sein, was sich dahinter verbirgt und somit auf einen Link, bzw. Seite geleitet werden, die du gar nicht sehen wolltest (zum Beispiel Werbung) oder auf der sich ein Virus verbirgt.

AUFGABE: Erstelle einen QR-Code. Dafür brauchst du gar nicht zwangläufig eine App, denn das kannst du auch im Browser tun, indem du in der Suchmaschine nach einem entsprechenden Programm suchst. Link einfügen, QR-Code generieren, fertig.

Quelltext/Quellcode

Jede Software und auch jede Internetseite hat einen ➢Quelltext, der sozusagen als Bauplan dient. Dort sind alle Befehle festgehalten, die bestimmen, wie das Programm oder die Seite funktionieren oder aussehen soll.
Bei vielen Programmen ist der Quelltext geheim, damit nicht einfach jemand den Plan klauen oder bearbeiten kann. Einige Programme fallen jedoch in den Bereich ➢„Open Source" und stellen ihren Quelltext öffentlich zur Verfügung, damit andere diesen Bauplan auch verwenden und weiterentwickeln können.

AUFGABE:
Schau dir mal so einen Quelltext an, indem du auf einer Internetseite einfach auf die rechte Maustaste klickst und „Quelltext anzeigen" oder „Element untersuchen" auswählst. Kannst du etwas daraus erkennen? Schau genau hin.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Recht am eigenen Bild

Das Recht am eigenen Bild besagt, dass jeder Mensch selber entscheiden darf, wofür das eigene Bild verwendet wird. Das heißt, du kannst einer Veröffentlichung deines Bildes auch widersprechen und der oder die andere muss sich daran halten.

Wichtig: Bevor du zum Beispiel ein Bild von dir und Freunden im Internet hochlädst oder bei WhatsApp, Snapchat oder sonst wo verschickst, musst du immer nachfragen, ob das für die Personen auf dem Foto in Ordnung ist. Wenn 100 Personen auf dem Foto sind, dann musst du auch alle 100 Personen fragen, solange die Gesichter einzeln erkennbar sind (zum Beispiel durch Heranzoomen).

Wenn du in der Öffentlichkeit fotografierst, lässt es sich nicht vermeiden, dass auch fremde Menschen auf dem Bild sind, die du natürlich meist nicht alle fragen kannst. Wenn du beispielsweise in einem Fußballstadion oder vor einer Sehenswürdigkeit ein Foto machst, dann darfst du die Bilder nicht öffentlich zur Verfügung stellen. Für die Presse gibt es da Sonderregelungen.

Wenn du noch nicht 18 Jahre alt, also noch nicht volljährig bist, dann müssen deine Eltern entscheiden, ob deine Fotos veröffentlicht werden dürfen. Aber die letzte Entscheidung liegt natürlich immer bei dir! Wenn du nicht möchtest, dass Fotos von dir veröffentlicht werden, dann müssen sich auch deine Eltern daran halten.

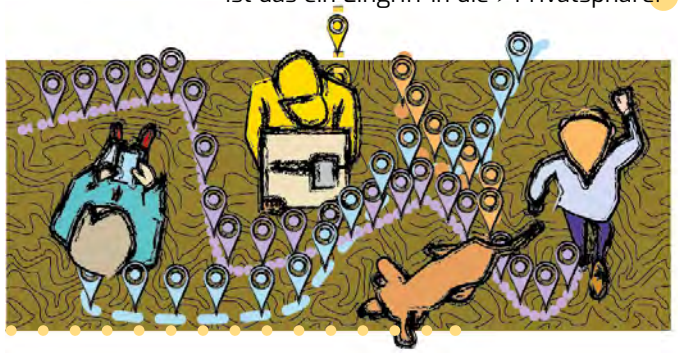
AUFGABE: Sprich mit deinen Eltern darüber, welche Fotos von euch ihr veröffentlicht sehen wollt und welche nicht. Habt ihr unterschiedliche Ansprüche an eure Privatsphäre? Findet ihr die gleichen Fotos voneinander peinlich oder unproblematisch, oder gehen eure Meinungen sehr weit auseinander?

RFID-Chip

RFID steht für „radio-frequency identification", also die Identifikation über elektromagnetische Wellen. Meist befindet sich ein RFID-Code in einem kleinen Chip, der von speziellen Geräten ausgelesen werden kann. Jeder Chip hat eine eigne Nummer, über die er klar erkannt/zugeordnet werden kann. Solche Chips sind sehr klein und werden oft im Alltag verwendet, zum Beispiel

- in verschiedenen Waren und Kleidungsstücken, um die Produktionswege zu überwachen und Diebstahl zu vermeiden (deshalb piept es zum Beispiel, wenn jemand etwas im Laden klaut),
- in Reisepässen, Personalausweisen, Kundenkarten, Kreditkarten und anderen auslesbaren Karten, um Personen zu identifizieren,
- oder auch um Tiere zu identifizieren, zum Beispiel entlaufene Hunde (als Implantat im Körper).

Wichtig: Durch RFID-Chips ist es auch möglich, Menschen zu überwachen und zum Beispiel Bewegungsprofile zu erstellen. Denn viele Menschen tragen die RFID-Chips in ihrer Geldbörse (in Kredit- und Kundenkarten) oder an der Kleidung mit sich herum. Wenn diese Daten ausgelesen werden, ist das ein Eingriff in die ➤Privatsphäre!



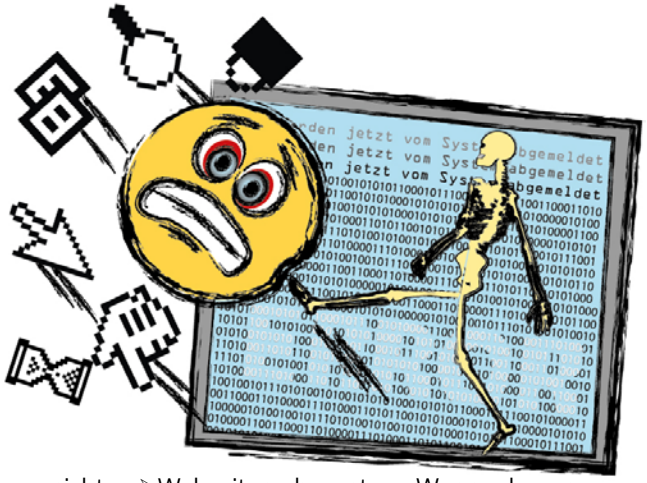
Router

„Router" bauen eine Datenverbindung zwischen verschiedenen Geräten auf. Du kannst dir Router wie Postboten in verschiedenen Städten vorstellen: Wenn eine Verbindung von A nach B aufgebaut werden soll, dann landen die übertragenen Daten bei dem Postboten (Router), der diese dann auf die Empfänger im zuständigen Bereich aufteilt (auf die Geräte). Der Router arbeitet dabei mit ➤IP-Adressen, die ihm genau sagen, wer die Daten sendet oder empfangen soll.

Schadsoftware

Schadsoftware bezeichnet Computerprogramme, die dafür gemacht sind, schädliche Funktionen auszuführen. Dazu gehört zum Beispiel das Manipulieren oder Löschen von Dateien, das unerlaubte Sammeln von Daten oder die Zerstörung von Programmen.
Es gibt verschiedene Klassifikationen. Einige davon sind:

- Spyware: Der Name ist abgeleitet vom englischen „to spy", also „(aus) spionieren". Es handelt sich dabei um Programme, die unerlaubt Daten von dir sammeln. Im schlimmsten Fall aktiviert das Programm deine Kamera oder dein Mikrofon, sodass du direkt beobachtet oder abgehört werden kannst.
- ➤Trojaner: Ein Trojaner tarnt sich als ein gutes Computerprogramm (zum Beispiel als ein ➤Plug-in) und fällt das System dann von innen an.
- ➤Virus (Plural: Viren): Diese schleichen sich in ein Computerprogramm rein, indem sie sich selbst in das Programm oder in eine Datei hineinkopieren. Somit können sie auch auf verschiedenen Wegen, zum Beispiel über USB-Sticks, übertragen werden.
- ➤Wurm: Ein Wurm funktioniert wie Viren, verbreitet sich allerdings über Netze, wie zum Beispiel das Internet.



Hinweise auf Schadsoftware sind zum Beispiel:

- unvorhergesehene Meldungen auf dem Bildschirm,
- komische Töne (zum Beispiel wie beim Einstecken eines USB-Kabels),
- Programme, die sich wie von alleine öffnen oder schließen,
- Netzwerkverbindungen, die sich aufbauen, obwohl du das gar nicht wolltest,
- Freunde bekommen Nachrichten von dir, die du nie verschickt hast,
- das Gerät stürzt häufig ab oder lässt sich nicht starten,
- das Öffnen von Programmen dauert lange,
- Dateien und Ordner verschwinden einfach oder werden verändert,
- das Licht neben der Laptopkamera leuchtet manchmal, obwohl du die Kamera gar nicht benutzt,
- ...

Wichtig: Du solltest darüber nachdenken, dir ein Anti-Viren-Programm herunterzuladen, aber darauf achten, dass dieses auch vertrauenswürdig ist und nicht selber deine Daten sammelt. **Das beste Anti-Viren-Programm ist jedoch der eigene Verstand!** Öffne keine ➢Links, bei denen du nicht weißt, was sich dahinter versteckt. Lade dir keine ➢Apps von ➢Webseiten herunter. Wenn du am Computer surfst, dann solltest du dir keine Programme von Webseiten herunterladen, die du nicht verstehst (zum Beispiel in einer fremden Sprache), oder die auf einer Seite angeboten werden, die nicht besonders vertrauenswürdig aussieht (zum Beispiel weil sie sehr viel Werbung enthält). Schau auf jeden Fall vorher in das ➢Impressum.

Wenn du E-Mails bekommst, dann öffne den Anhang nur, wenn du genau weißt, von wem die E-Mail kommt und was in dem Anhang drin ist. Wenn dir Freunde geheimnisvolle ➢Links oder Dateien schicken, dann kannst du auch nachfragen, was sich dahinter verbirgt. Denn wie oben beschrieben, kann es auch passieren, dass deine Freunde unbeabsichtigt Links verschicken, weil sie selber einen Virus auf ihrem Gerät haben. Manchmal wissen sie gar nichts davon, dann solltest du sie warnen, dass ihr Computer vielleicht befallen ist.

Server

Egal, was du im Internet machst: Sobald du eine Seite aufrufst, kommuniziert dein Gerät (Computer, Tablet, Smartphone) immer, bei jedem Klick, mit einem anderen Gerät, nämlich mit einem Server, auf dem alle Daten gespeichert werden.

Beispiele:

- Wenn du zum Beispiel mit einem Klick eine Webseite öffnen möchtest, dann sendest du die Information an den Server, dass du die Inhalte der Seite aufrufen möchtest.
- Wenn du dich bei einem Spiel oder ➢Sozialen Netzwerk anmelden möchtest, dann tippst du deinen Benutzernamen und dein Passwort ein und schickst diese eingegebenen Daten an den Server, wo sie überprüft werden und der Befehl zum Einloggen erteilt wird.
- Wenn du eine Nachricht, ein Foto, eine E-Mail oder eine Sprachnachricht verschicken möchtest, dann schickst du diese von deinem Gerät an einen Server, und von dort werden sie an den Empfänger geleitet.

Auf einem Server werden also Daten gespeichert oder zugänglich gemacht. Daher muss zunächst zwischen ➢Hardware und ➢Software unterschieden werden.

- Server- (Hardware): Ist ein Computer, auf dem große Datenmengen gespeichert werden. Server, die ausschließlich Daten aus dem Internet, also von Internetseiten, speichern, werden „Hoster" genannt. Ein einzelner Hoster verwaltet meistens mehrere Clients.
- Server- (Software) oder „Client",: Ist ein Computerprogramm, das den Zutritt zu einer ➢Datenbank gewährt. Ein Client (Deutsch: „Kunde") kommuniziert dabei mit einem Server oder Hoster.

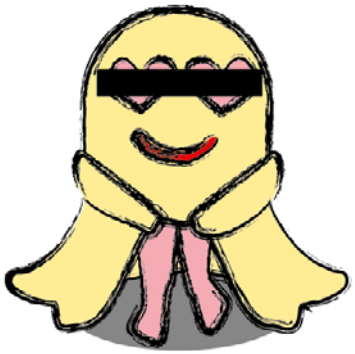
Sexting

Das Wort „Sexting" setzt sich aus „Sex" und „Texting" zusammen. Es bezeichnet den einvernehmlichen Austausch von erotischen Nachrichten, Bildern und Videos zwischen zwei Personen. Wichtig dabei ist, dass dieser Austausch von beiden Parteien gewollt ist, denn wenn eine Person diese Nachrichten oder Bilder nicht bekommen möchte, heißt das nicht mehr Sexting, sondern wir befinden uns schon im Bereich der sexuellen Belästigung, bzw. wenn eine Person so ein Foto nicht anfertigen möchte und sie dazu gedrängt wird, im Bereich der sexuellen Nötigung.

Einige Jugendliche tauschen erotische Texte und Bilder mit ihrem Partner oder ihrer Partnerin als Vertrauensbeweis aus, oder um zu flirten. Das ist nichts Schlimmes und jede.r darf selbst entscheiden, ob er oder sie das möchte. Doch dabei kann auch einiges schief gehen: Der/die Partner.in könnte das Vertrauen leider missbrauchen und die

Fotos Freund.innen oder Fremden zeigen. Zudem können die Bilder auch auf anderen Wegen in falsche Hände gelangen, zum Beispiel wenn jemand diese auf deinem Gerät sieht oder sich dein Gerät mit einem anderen Gerät synchronisiert (➤Synchronisation), zum Beispiel wenn du dein Handy zum Laden an den Computer anschließt. Außerdem besteht auch die Möglichkeit, dass dein Gerät gehackt wird (➤Hacker).

Wichtig: Am besten verzichtest du ganz auf solche Art Bildaufnahmen! Wenn du allerdings trotzdem Bilder von dir machst, auf denen du nackt oder in Unterwäsche zu sehen bist, dann musst du unbedingt darauf achten, dass dein Gesicht nicht zu erkennen ist und auch sonst nichts auf dem Bild mit dir in Verbindung gebracht werden kann (Narben, Muttermale, Piercings, Tattoos, eindeutige Kleidungsstücke oder dein Zimmer im Hintergrund…). Gerade, wenn du Fotos im Spiegel machst, solltest du überprüfen, was sich noch alles spiegelt. Wenn solche Bilder in Umlauf geraten, kann dies ganz schlimme Folgen für dich haben, denn es könnte dich jemand mit diesen Bildern erpressen oder wegen der Bilder mobben (➤Cybermobbing).



Wenn du solche Bilder von dir gemacht hast, bist du aber noch lange nicht schuld, wenn sie in Umlauf geraten. Schuld ist daran immer die Person, die sie in Umlauf gebracht hat. Außerdem sind Mädchen, die solche Fotos machen, keine „Schlampen“ und Jungs nicht „cool“ – solche Bewertungen sind unfair! Mädchen werden meist schlimmer beschimpft als Jungs, aber das Geschlecht macht es nicht besser oder schlechter.

Smart ★

„Smart“ ist ein Adjektiv, also ein Wie-Wort, das (sowohl im Englischen als auch im Deutschen) eingesetzt wird, um etwas als intelligent oder elegant zu beschreiben. Deshalb wird das Wort oft verwendet, wenn es um künstliche Intelligenz (KI) geht, also wenn Computer und Roboter schlaue Dinge tun, obwohl sie kein Gehirn haben wie Menschen. Künstliche Intelligenzen können aber noch viel mehr leisten als Menschen, zum Beispiel besser rechnen, mehr Informationen speichern oder verknüpfen und dadurch schneller/besser arbeiten.

Ist also von „smarten“ Dingen/Gegenständen die Rede, dann ist gemeint, dass diese zu einer künstlichen Intelligenz werden, zum Beispiel durch eingebaute Chips (das können ➤RFID-Chips sein) oder Sensoren (kleine Fühler und Knöpfe, die ohne Berührung funktionieren). Die Gegenstände werden beispielsweise mit Computersystemen, dem Internet oder ➤Bluetooth vernetzt und sind oft

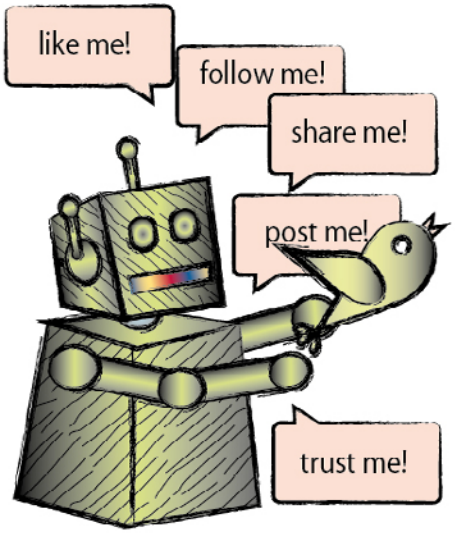
über Fernbedienungen von ganz anderen Orten steuerbar. Häufig kann auch ein Tablet oder Smartphone als Fernbedienung eingesetzt werden. Beispiel: Ein Fernseher, der mit dem Internet verbunden werden kann, wird zum Smart TV.

Das Smartphone gehört, wie der Name schon sagt, ebenfalls zu diesen „intelligenten Dingen“: Das ursprüngliche Mobiltelefon oder Handy ist nun durch die Verbindung mit dem Internet und durch die Sensoren, die das Touchpad steuern, zum „smart phone“, also zum intelligenten Telefon, geworden. Wie du aber weißt, ist das Smartphone heutzutage wie ein kleiner Computer und das kann mit allen Dingen geschehen, die auf diese Weise intelligent gemacht werden. Viele dieser smarten Technologien sind mit dem Internet verknüpft, wodurch der Begriff ➤Internet der Dinge“ entstanden ist.

Mit der „smarten“ Vernetzung von ganz vielen Dingen in verschiedenen Lebensbereichen haben Datenschützer. innen große Bedenken. Wenn dein Kühlschrank weiß, was du isst, können dabei ➤Daten gesammelt werden, ob du dich gesund ernährst. Wenn du deine Rollläden über das Internet rauf und runter fahren kannst, dann kann das vielleicht auch gehackt werden (➤Hacker) und Einbrecher können sich sozusagen selbst die Tür aufmachen. Und wenn du alle Filme nur noch online über dein Smart TV abrufst (➤Streaming), weiß der Anbieter, wie viel du fern siehst und ob du vielleicht etwas gesehen hast, was für dein Alter noch gar nicht freigegeben war (vergleiche ➤FSK).

AUFGABE: Such Zuhause mal alle Geräte, die „Smart“ heißen und besprich mit deinen Eltern, welche Funktionen sie haben. Braucht ihr diese Funktionen wirklich? Welche Daten fallen dabei an? Und wer bekommt diese Daten? Könnt ihr manches davon vielleicht auch einfach abschalten, um nicht nur Strom, sondern auch Daten zu sparen?

(Social) Bot



„Bot" ist eine Abkürzung vom englischen „robot", also Roboter. Damit sind automatisierte Programme gemeint. Wenn du zum Beispiel einen Begriff in die Suchmaske einer Internetseite oder Suchmaschine eingibst, dann prüft so ein Programm automatisch das Internet auf diesen Suchbegriff, ohne dass ein Mensch diese Arbeit übernimmt.

Diese praktische Funktion kann allerdings auch missbraucht werden. Denn so können beispielsweise auch E-Mail-Adressen automatisch gesucht und gefunden werden, die für Werbezwecke genutzt werden. Wenn deine E-Mail-Adresse von so einem Bot ausgelesen wird, bekommst du beispielsweise viele Mails, die du gar nicht haben wolltest (➤Spam). Deshalb solltest du deine private E-Mail-Adresse nie öffentlich im Internet angeben.

Ein „Social Bot" ist dasselbe wie ein Bot, also ein automatisiertes Programm. Doch „Social Bots" sind, wie der Name schon sagt, „sozial" und können mit Menschen in Kontakt treten. Ein Beispiel dafür wäre eine automatische Antwort auf eine E-Mail. Diese automatischen Antworten können so gut programmiert werden, dass eine natürliche Person eine Unterhaltung mit einem Social Bot führen könnte, ohne es zu merken.

Social Bots werden in ➤Sozialen Netzwerken eingesetzt, um Kommunikation anzuregen. Sie zu erkennen ist sehr schwer, aber es gibt ein paar Punkte, auf die du achten kannst, wenn du vermutest, dass du es mit einem Social Bot zu tun hast.

1. Prüfe das Profil der Person. Es ist zumindest ein Indiz, wenn das Profil erst kürzlich angelegt wurde. In manchen Sozialen Netzwerken gibt es die Möglichkeit, das eigene Profil zu verifizieren, also die Echtheit zu beweisen (vor allem bei Plattformen, auf denen es um das Kennenlernen von Personen geht). Achte also darauf, ob ein Profil als echt anerkannt wurde.
2. Prüfe, wie aktiv die Person kommuniziert. Wenn es ungewöhnlich viele Nachrichten/Interaktionen in kürzester Zeit gegeben hat, dann ist das ein Indiz dafür, dass hier versucht wird, Kommunikation anzuheizen, und dass ein Computer dahinter steckt.
3. Achte darauf, wie schnell die Person auf Nachrichten reagiert. Wenn die Antwort auf eine Frage binnen weniger Sekunden schon da ist, ist dies ein Grund, skeptisch zu werden. Social Bots brauchen nur einen Bruchteil einer Sekunde, um zu antworten. Einige sind so programmiert, dass eine Antwort extra wenige Sekunden verzögert wird, um keinen Verdacht zu erregen. Braucht dein Gegenüber für einen Text mit fünf Wörtern genauso lange wie für einen Text mit 50 Wörtern, dann ist das verdächtig.
4. Achte auf die Inhalte der Nachrichten. Ein Social Bot ist programmiert und kann zwar die geschriebenen Worte einigermaßen erkennen, analysieren und eine annähernd passende Antwort präsentieren, doch oft sind die Antworten nicht vollkommen passend, schneiden das Thema nur leicht an oder sind sehr allgemein gehalten.

Software

Eine „Software" ist ein Computerprogramm. Dieses steuert genau, was zu tun ist, und wird von der ➤Hardware lediglich ausgeführt. Alle Apps und alle Programme auf digitalen Geräten sind von irgendjemandem programmiert und die einzelnen Befehle im ➤Quellcode festgehalten worden. Dieses Programmieren können alle lernen, die sich dafür interessieren, doch es gibt auch Berufe, die sich nur damit beschäftigen, zum Beispiel Softwareentwickler.innen. Es kommt auch häufig vor, dass ➤Admins oder andere Personen aus der ➤IT-Branche so fit in dem Bereich sind, dass sie kleinere Softwares programmieren können.

Soziales Netzwerk

Ein „Soziales Netzwerk" im Internet ist ein „Treffpunkt", wo sich viele Menschen (eine ➤„Community") miteinander austauschen und interagieren, also gegenseitig aufeinander reagieren. Daher kann man in vielen Sozialen Netzwerken chatten, Fotos/Videos austauschen, diese kommentieren oder auch über Video-Telefonie miteinander reden. So können die Nutzer.innen auch über weite Entfernungen in Kontakt treten.

Soziale Netzwerke sammeln meistens viele Daten von dir! Wenn du dich auf einer Plattform registrierst, dann solltest du als erstes die Einstellungen prüfen und alle Unterpunkte so einstellen, dass du möglichst wenig von dir preisgibst! Überleg dir auch vorher, ob es unbedingt sein muss, dass du dich dort anmeldest und ein Profil anlegst, das du mit persönlichen Daten füllst.

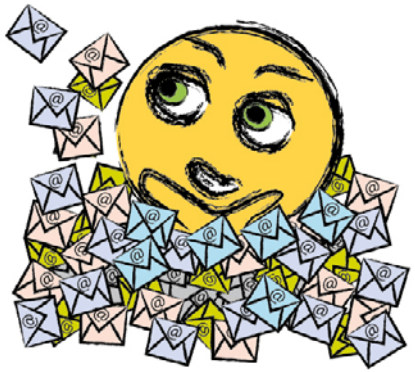
Gefahren: Besonders auf diesen Plattfor-

men begegnen sich viele (fremde) Menschen und es entwickeln sich verschiedene Gruppen (zum Beispiel Menschen mit gleichen politischen Interessen oder Fan-Gruppen von Stars). Daher gibt es leider auch ➤Cybermobbing, ➤Hater oder ➤Hate Speech.

Soziale Netzwerke gibt es aber auch außerhalb des Internets, denn der Begriff bedeutet eigentlich, dass Menschen miteinander in Verbindung treten/vernetzen. Deswegen „soziales" Netzwerk

TIPP: Wenn von dem Sozialen Netzwerk im Internet die Rede ist, dann wird das „s" von „sozial", wie bei einem Eigennamen, meist groß geschrieben. So kann man die beiden unterscheiden.

Spam



„Spam" (Englisch: „Abfall") sind unerwünschte Nachrichten, wie zum Beispiel E-Mails. Oft enthalten diese Nachrichten Werbung, Gewinnbenachrichtigungen von Gewinnspielen, an denen man nie teilgenommen hat, oder andere Inhalte, in denen sich ➤Schadsoftware befinden kann. Sei deshalb immer vorsichtig, wenn du nicht weißt, von wem eine Mail ist!

Es gibt auch Programme, die automatische Spam-Mails generieren und verschicken. Wenn du deine Mail-Adresse irgendwo öffentlich angegeben hast, ist es für diese Programme kein Problem, deine Mail-Adresse automatisch auszulesen und dir Spam-Mails zu schicken. Gib deine E-Mail-Adresse also nie öffentlich an und wenn es doch unbedingt sein muss, dann ersetze das „@"-Zeichen durch „[at]". Jeder weiß dann, dass das @-Zeichen gemeint ist, aber Computer und Bots (vgl. ➤(Social) Bots) können das Zeichen nicht automatisch auslesen. Spam-Nachrichten können aber auch beispielsweise per SMS verschickt werden, wenn jemand deine Handynummer hat.

TIPP: Durch einen falschen Klick, eine Bestellung in einem Online-Shop, die Teilnahme an einem Gewinnspiel oder durch die Installation von einer App/einem Programm, bestellt man sich oft aus Versehen einen ➤Newsletter mit, der einem dann regelmäßig zugeschickt wird.

Staatstrojaner

Staatstrojaner sind Spionage-Programme (vgl. ➤Schadsoftware), die von Ermittlungsbehörden (Polizei, Staatsanwaltschaft,...) und Geheimdiensten (zum Beispiel Bundesnachrichtendienst (BND) oder Verfassungsschutz) heimlich auf Geräten installiert werden, also auf Computern, Laptops, Smartphones und so weiter.

Mit dem Staatstrojaner bekommen Behörden also die Möglichkeit, private Nachrichten von Menschen auszulesen oder abzuhören, was ein großer Eingriff in die Privatsphäre ist. Er wird als Schutzmaßnahme getarnt, um beispielsweise Verbrechen aufzuklären oder zu verhindern. Es ist jedoch die Aufgabe des Staates, für Sicherheit zu sorgen, indem er Sicherheitslücken schließt und nicht ausnutzt! Deshalb sind sehr viele Menschen gegen den Einsatz von Staatstrojanern.

Weitere Informationen über die Funktionsweise der Schadsoftware und über den Wortherkunft, kannst du im Beitrag ➤Trojaner nachlesen.

Stalking

„Stalking" beschreibt das Verfolgen, Beobachten und teilweise auch das Belästigen einer Person. Dies ist strafbar, deshalb können Stalker angezeigt werden und dürfen sich, wenn sie verurteilt wurden, der Person dann zum Beispiel nicht mehr nähern. Stalking im Internet ist allerdings nicht so leicht zu erkennen. Du weißt nicht, wer sich auf deiner Seite rumtreibt, deine Fotos anschaut und kontrolliert, an welchen Orten du dich verlinkt hast. Du weißt nicht, wer bei WhatsApp immer wieder deinen Online-Status prüft.

Wichtig: Stalker haben oft eine psychische Erkrankung. Sie sind von einer Person besessen. Oft suchen sie entweder die Nähe der Person, weil sie zum Beispiel in diese verliebt sind, manchmal aber auch, weil sie der Person schaden möchten. Wenn du merkst, dass dich jemand ständig, heimlich oder auch offensichtlich verfolgt und du die Person nicht kennst oder diese nicht damit aufhört, obwohl du sie darum gebeten hast, dann solltest du das auf jeden Fall deinen Eltern erzählen und eventuell mit ihnen gemeinsam zur Polizei gehen.

Standortdaten „Standortdaten" beschreiben die genaue Position, an der du dich befindest. Dein Standort kann zum Beispiel über eine ➤GPS-Ortung bestimmt werden.

Streaming

„Streaming" (Deutsch: „strömen") bezeichnet die Datenübertragung von Dateien (Videos, Filme, Musik und so weiter), ohne die ganzen Dateien auf dem eigenen Gerät zu speichern, wie es zum Beispiel bei ➤Downloads der Fall ist. Beim Streaming wird immer nur ein ganz kleiner Teil der Datei für den Moment des Abrufs gespeichert und dann sofort wieder gelöscht.

Was bei Sportveranstaltungen bereits altbekannt ist, nun aber auch Einzug in

private Lebensbereiche findet, ist das Live-Streaming. Dabei wird der Stream einer Sendung live im Internet übertragen, oder es wird eben ein beliebiger Moment im Alltag mit der Kamera begleitet und live im Netz übertragen. So eine Funktion bietet beispielsweise auch Facebook an.

Wichtig: Bedenke, dass du nichts mehr zurück nehmen kannst, was du in einem Live-Stream gesagt oder getan hast! Achte außerdem darauf, dass man nicht erkennt, wo du dich aufhältst (zum Beispiel anhand des Hintergrunds).

Außerdem: Wer Filme zum Streamen zur Verfügung stellt und nicht die Lizenzen dazu hat, macht sich ganz klar strafbar. Das ist auch nichts Neues. Aber seit April 2017 ist Streaming in den meisten Fällen illegal, wenn du nicht dafür bezahlst. Wenn du also auf einen aktuellen Film stößt, der kostenlos gestreamt werden kann, dann solltest du lieber die Finger davon lassen, denn wenn das herauskommt, kann es sehr teuer für sich werden.

Suchmaschine

Eine Suchmaschine ist ein Programm, das dir dabei hilft, Seiten im Internet zu finden. Die meisten Menschen verwenden dazu „Google", deshalb hat sich mittlerweile der Begriff „googeln" für „im Internet suchen" etabliert. Es gibt aber noch viel mehr Suchmaschinen und Google ist eine Suchmaschine, die sehr viele Daten von dir sammelt, während du am Surfen bist. Das solltest du zum Schutz deiner ➤Daten unbedingt vermeiden (➤Datenschutz)! Bessere Suchmaschinen sind zum Beispiel „startpage.com" oder „duckduckgo.com".

Es gibt auch Suchmaschinen, die extra für Kinder sind, und die solltest du auch nutzen, denn sie blockieren Seiten, die nicht für die Augen von Kindern gedacht sind. Zum Beispiel gibt es

- http://www.blinde-kuh.de
- http://www.fragfinn.de (auch als App für Smartphones und Tablets verfügbar)

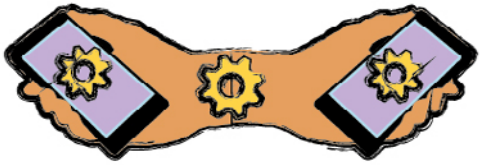
Sie funktionieren nach dem „Whitelist-Prinzip", das heisst dir werden nur Seiten angezeigt, die explizit freigegeben sind und auf einer „weißen Liste" stehen. Seiten, die nicht auf dieser Liste stehen, können nicht abgerufen werden. Daher muss dir immer bewusst sein, dass diese Suchmaschinen eigentlich Zensur betreiben. Das bedeutet: Jemand anderes entscheidet, was du lesen sollst oder nicht, und so bist du natürlich eingeschränkt, was deine Entwicklung in verschiedene Richtungen betrifft.

Synchronisation

„Synchronisation" bedeutet „Abgleich". Du kannst beispielsweise ➤Daten zwischen verschiedenen Geräten synchronisieren/abgleichen, sodass du dieselben Daten auf mehreren Geräten speichern kannst. Dies macht man meistens über ➤Bluetooth, USB-Kabel oder über das Internet, bzw. über ➤Clouds. Gerade Geräte der Marke „Apple" sind darauf ausgelegt, dass man einen Datenabgleich zwischen verschiedenen Geräten machen kann, zum Beispiel zwischen einem iPhone, iPad und MacBook.

Auch ➤Apps wollen häufig Daten synchronisieren, zum Beispiel möchte WhatsApp deine Kontaktliste mit deinem Telefonbuch abgleichen (was verboten ist, wenn du nicht jede einzelne Person aus deiner Kontaktliste gefragt hast, ob du das darfst). Aber nicht immer geht bei Apps klar hervor, ob eine Synchronisation sinnvoll ist. Oft wollen die Anbieter einfach nur Daten von dir.

Außerdem kann es schlimme Folgen haben, wenn du deine Daten versehentlich mit einem anderen Gerät synchronisierst, zum Beispiel wenn du dein Handy nur zum Laden des Akkus an einen fremden Computer anschließt und du aus Versehen alle deine Bilder auf dem fremden Gerät speicherst.



Telekommunikationsdaten

„Telekommunikationsdaten" sind Verbindungsdaten zwischen Festnetztelefonen, Handys, Smartphones, und auch Daten über die Verbindung dieser Geräte. Also zum Beispiel deine Telefonnummer, die Nummer, die du anrufst, Länge des Gesprächs, dein Standort während des Gesprächs, Datum und Zeitangabe des Gesprächs und so weiter.

Diese Daten werden bei den jeweiligen Anbietern gespeichert (➤Vorratsdatenspeicherung).

Thread

„Thread" ist das englische Wort für „Strang" und wird im Internet genutzt, um eine Hierarchie, also eine Ordnung von über- und untergeordneten Elementen darzustellen. Meistens begegnet dir das Wort wahrscheinlich in ➤Blogs und ➤Foren, wo ein „Thread" einen Knotenpunkt, also ein Thema

abbildet, auf das dann geantwortet werden kann. Man kann einen Thread also als einen Erzählstrang oder Gesprächsfaden bezeichnen, der dabei hilft, den Gesprächsverlauf der einzelnen Beiträge (➤Postings) zu überblicken.
Beispiel:
„Der Sommer ist toll!"
– Re: „Das finde ich nicht."
– Re: Re: „Wieso denn nicht?"
– Re: Re: Re: „Ist zu warm."
– Re: „Finde ich auch!"
In Foren und Blogs wird meistens auf das „Re:" („referenz" = Betreff) verzichtet, damit die Gespräche besser lesbar sind. Bei E-Mails wird der Bezug in der Betreffzeile allerdings oft verwendet. Manchmal steht da auch „Antw." für Antwort.

Tracking

„Tracking" bedeutet auf Deutsch „Verfolgung" oder „Ortung" und kann ganz unterschiedliche Formen haben: Eine Paketsendung zu verfolgen, kann zum Beispiel sinnvoll sein (Wann kommt es an und wann muss ich Zuhause sein?) und seine Pizza-Lieferung zu orten hat zugegeben einen gewissen Charme und Spaßfaktor. Es gibt aber auch Formen des Trackings, die überflüssig sind, zum Beispiel wenn dich jemand trackt, um zu wissen, wo du bist oder wo du deine Zeit verbringst. Meistens funktioniert so eine „Verfolgung" über das ➤GPS in deinem Smartphone. Es gibt zahlreiche ➤Apps, mit denen Eltern ihre Kinder überwachen können oder Liebespaare gegenseitig kontrollieren können, wo sich die Partnerin oder der Partner gerade aufhält. Besonders schlimm ist Tracking, wenn du ohne dein Wissen von Apps getrackt wirst, die deine Bewegungsprofile (wann, wo und wie lange du an einem Ort warst), an ➤Drittanbieter weiterverkaufen und Geld mit diesen sehr privaten Informationen verdienen.

AUFGABE: Schau mal in die ➤App-Berechtigungen deiner Apps, ob Bewegungsdaten von dir gesammelt werden. Du wirst dich wundern, welche Apps deine Bewegungsdaten sammeln, obwohl dies gar nicht nötig ist (zum Beispiel Musikerkennungs-Apps).

Wichtig: Mit einem Smartphone in der Tasche, kannst du es kaum noch vermeiden getrackt zu werden. Du solltest dein GPS-Signal immer ausschalten und auch dein WLAN. Anhand der Stellen, an denen sich dein Handy in ein WLAN einwählt, können ebenfalls Bewegungsmuster erstellt werden. Dies wird zum Beispiel bereits teilweise in Supermärkten so gemacht: Die Betreiber werten beispielsweise aus, wie lange du vor welchem Regal gestanden hast, welche Produkte dich somit interessieren und welche Produkte schlechter ankommen. Auch viele Webseiten sind daran interessiert, deine ➤Metadaten auszuwerten und deine Aktivitäten zu verfolgen, was ebenfalls eine Art des Trackings ist. Sie wollen zum Beispiel wissen, von welcher Seite du auf ihr Angebot aufmerksam gemacht wurdest. Das geht sie aber nichts an. Du solltest daher in den Einstellungen deines ➤Browsers ein Häkchen bei folgender Datenschutz-Einstellung setzen: „Websites mitteilen, meine Aktivitäten nicht zu verfolgen".

Trojaner

Ein Trojaner ist eine Form von ➤Schadsoftware. Der Begriff ist abgeleitet vom „trojanischen Pferd" und ist auf eine Geschichte in der griechischen Mythologie zurückzuführen. In dieser geht es darum, dass die Griechen unter der Herrschaft von Odysseus ein riesiges, hölzernes Pferd gebaut haben, dass sie der Stadt Troja geschenkt haben. Die Bewohner der Stadt haben das Geschenk angenommen und dieses Pferd durch ihre hohen Stadtmauern in die Stadt hinein transportiert. Doch im Inneren des Holz-Pferdes hatten sich Krieger versteckt, die somit ohne große Mühe in die Stadt eindringen und diese bekriegen konnten. Und genauso funktioniert ein Trojaner in einem Computersystem: Er tarnt sich als ein gutes Computerprogramm (zum Beispiel als ein ➤Plug-in) und fällt das System dann von innen an. (Siehe auch: ➤Staatstrojaner.)

Unboxing ★

„Unboxing“ bedeutet „auspacken“ und ist ein Begriff des Social-Media-Marketings, beziehungsweise des Influencer-Marketings (➢Marketing). Es handelt sich dabei um Werbevideos, in denen ein Produkt vor der Kamera ausgepackt und präsentiert wird. Mehr dazu kannst du im Beitrag über ➢„Influencer“ nachlesen.

Update

„To update“ bedeutet nichts anderes als „aktualisieren“. Wenn beispielsweise eine neue Version einer App verfügbar ist, wird dir angeboten, diese zu aktualisieren. Manchmal ist die alte Version auch gar nicht mehr verwendbar. Ganz viele ➢Apps und ➢Softwares werden immer wieder weiterentwickelt und verbessert. Es kommen neue Funktionen dazu, oder es werden zum Beispiel Sicherheitslücken geschlossen, durch die Kriminelle einbrechen und Daten klauen können. Daher solltest du dafür sorgen, immer die neusten Updates zu installieren.

Wichtig: Verwechsle nicht „Update“ mit ➢„Upgrade“.

Upgrade

Upgrades sind meistens Erweiterungen für Programme, die du schon nutzt. Teilweise wurden aber nur unnötige Funktionen hinzugefügt, die dich Geld kosten. Sie werden dir beispielsweise in Spielen angeboten, um Vorteile gegenüber anderen Mitspieler.innen zu bekommen (siehe auch ➢In-App-Käufe). Um zu entscheiden, ob ein „Upgrade“ sinnvoll ist, solltest du den Begleittext gut lesen und entscheiden, ob du dieses Upgrade haben willst oder nicht.

Urheberrecht

Das Urheberrecht regelt, wem künstlerische Werke gehören, wer sie verwenden und wer sie weiterverbreiten darf. Darunter fallen zum Beispiel Texte, Fotos, Lieder und jegliche Art von Kunstwerken. Der Schaffer oder die Schafferin eines Werks nennt sich „Urheber.in“.

Über das Urheberrecht kannst du im Beitrag ➢Creative Commons mehr erfahren.

URL

„URL“ ist die Abkürzung von „Uniform Resource Locator“. Übersetzt heißt das „einheitlicher Ressourcenzeiger“ und meint den genauen Namen einer Webseite. Diese beginnt mit „http://“ oder „https://“, einem Netzwerkprotokoll, über das die meisten Webseiten im ➢World Wide Web (WWW) geladen werden. Durch dieses Protokoll, eine Art Sprache, ist es möglich, dass die Webseiten vom ➢Browser heruntergeladen und angezeigt werden können.

USK ★

USK ist die Abkürzung für „Unterhaltungssoftware Selbstkontrolle“. Du findest den Hinweis auf Computer- und Videospielen, denn sie geben an, ab welchem Alter ein Spiel für Kinder oder Jugendliche geeignet sind, so wie „FSK“ bei Filmen. Weitere Informationen findest du im Beitrag ➢FSK.

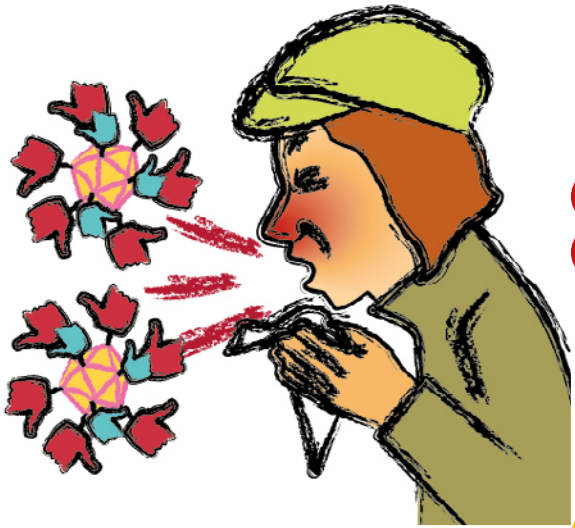
Video on Demand (VoD)

„Video on Demand“ bedeutet „Video auf Abruf“ und fasst beispielsweise Serien und Filme zusammen, die du im Internet über Mediatheken oder ➢Streaming-Portale abrufen kannst.

Es gibt dabei verschiedene Modelle, zum Beispiel Videos/Filme, die du kostenfrei anschauen/streamen kannst, Plattformen, bei denen du ein bezahltes ➢Abonnement abschließen kannst, Filme die du kostenfrei herunterladen kannst (ist jedoch selten der Fall) oder Filme, die du kostenpflichtig ➢downloaden musst. Informiere dich auf jeden Fall vorher, ob Kosten auf dich zukommen. Weitere Informationen kannst du im Beitrag ➢Streaming nachlesen.

Viral ★

„Dieser Post ging viral!“ ist ein Satz, der häufig von YouTuber.innen, aber auch in der gesamten Szene der ➢Sozialen Netzwerke genutzt wird. Gemeint ist damit, dass sich ein ➢Posting (egal ob Bild, Text oder Video) besonders schnell und weit verbreitet. Das Wort „viral“ kommt aus der Biologie und meint die Verbreitung eines Virus. Doch obwohl die Verbreitung



von medizinischen Viren und auch von technischen Computerviren (siehe auch ➢Virus in diesem Lexikon) etwas Negatives ist, wird die virale Verbreitung von Postings als etwas Positives angesehen und als Zeichen dafür, dass der Beitrag sehr beliebt ist. Ein Post verbreitet sich aber beispielsweise auch, weil er besonders interessant oder schockierend ist, deshalb sagt die Verbreitung nicht viel über die tatsächliche Beliebtheit aus. Um einen Beitrag besonders schnell zu verbreiten, wird häufig ➢Clickbaiting betrieben, also mit spannenden Überschriften gelockt, hinter denen sich teilweise gar nicht so spannende Texte oder sogar ➢Websites mit Kostenfallen und ➢Schadsoftware verbergen. Außerdem wird bei der Verbreitung von Postings auch häufig getrickst, indem Reichweite, also die Anzahl von lesenden Personen, dazu gekauft wird. Du fragst dich, wie das möglich ist? - Es gibt verschiedene ➢Algorithmen, die entscheiden, welche Posts du in Sozialen Netzwerken zu sehen bekommst und welche nicht. Wenn Reichweite dazugekauft wird, dann wird der Algorithmus so beeinflusst, dass der Beitrag für dich als wichtig eingestuft wird und er dir eher angezeigt wird als andere Beiträge.

Virtual Reality ★

„Virtual Reality“ (VR), auf Deutsch „virtuelle Realität“, bezeichnet die Wahrnehmung von der Wirklichkeit in einer Realität, die durch Computer geschaffen wird. Schwierig zu verstehen? Du hast bestimmt schon mal von Virtual-Reality-Brillen (VR-Brillen) gehört, die es mittlerweile auch für verschiedene Konsolen zu kaufen gibt. Es wird beispielsweise eine ganz andere Welt geschaffen und wenn du die Brille aufsetzt, fühlt es sich zumindest visuell (also für das Auge) so an, als wärst du mitten drin und ein Teil dieser Kulisse. Du kannst damit zum Beispiel an einer Achterbahnfahrt teilnehmen oder im Ozean tauchen, mit Fischen und Haien neben dir, obwohl du auf einem Stuhl sitzt und dich gar nicht bewegst, höchstens den Kopf um dich umzuschauen. Im Gegensatz zu ➢„Augmented Reality“ (erweiterte Realität), siehst du in dem Moment aber nichts mehr von der echten Realität, zum Beispiel von dem Zimmer, in dem du gerade sitzt. Es ist dabei sehr wichtig zu wissen, dass im Gehirn ganz viele Prozesse entstehen, wenn man sich in eine virtuelle Welt begibt und die Sinne versuchen, sich an die Gegebenheiten anzupassen. Wenn in der virtuellen Welt die Sonne scheint, kann es sein, dass dir warm wird, obwohl es in dem Raum, wo du dich befindest, gar nicht wirklich wärmer wird. Wenn du eine virtuelle Achterbahnfahrt mitmachst, kann es sein, dass dir sehr übel wird, weil die Bilder von Höhe, Tiefe oder Beschleunigung deinen Gleichgewichtssinn durcheinander bringen. Außerdem sind diese Prozesse für den Körper sehr anstrengend, was zu Kopfschmerzen und Müdigkeit führen kann. So spannend es auch ist, in nicht reale Welten abzutauchen, solltest du dies nie mehr als ein paar Minuten tun.

Virus Ein Virus (Plural: Viren) ist eine Form der ➢Schadsoftware.

Vlog „Vlog“ ist die Abkürzung für Video-Blog. Einige Blogger.innen verwenden Videos als Gestaltungsmittel für ihre ➢Blogs.

Vorratsdatenspeicherung

Was ist Vorratsdatenspeicherung (VDS)?

Zerpflücken wir mal das lange Wort: Vorrat – Daten – Speicherung. Es geht also darum, dass Daten auf Vorrat gespeichert werden. Das heißt, sie werden jetzt gerade noch nicht benötigt, aber vorsichtshalber aufbewahrt – man weiß ja nie, wofür sie mal gut sein können. Manche Politiker.innen sagen, Daten auf Vorrat zu speichern würde helfen, Verbrechen aufzuklären. Es gibt in Deutschland ein Gesetz, das unter anderem Telefonanbieter zur Speicherung verpflichtet. Das Problem: Dabei werden auch die Daten von Menschen gespeichert, die gar nichts Schlimmes tun wollen.

Welche Daten werden gespeichert?

Genau genommen handelt es sich dabei um die Speicherung von Daten, die bei der elektronischen Nachrichtenübertragung von Telekommunikations-Diensten gesammelt werden, also zum Beispiel von deinem Mobilfunkanbieter (Tele-

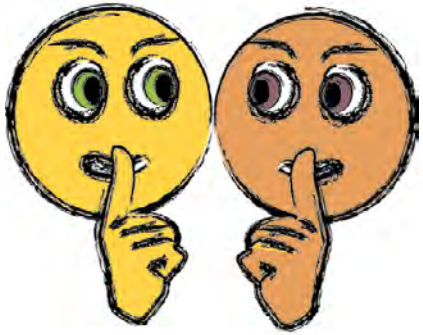
kom, Vodafone, ...). Auf deren ➤Servern wird unter anderem gespeichert, wann du eine Nachricht verschickt hast, wie lange du telefoniert hast, welche Nummer du angerufen hast, von wem du angerufen worden bist, wie lange das Gespräch gedauert hat, an welchem Ort du während des Telefonats gerade warst und wann du das Internet genutzt hast. Somit kann ziemlich genau nachvollzogen werden, wen du kennst und ein Bewegungsprofil erstellt werden. Diese Informationen verraten auch, welche Interessen oder Hobbys du hast, und lassen noch viel mehr Rückschlüsse auf deine Persönlichkeit zu.

Wer hat Zugriff auf diese Daten?

- Natürlich die Telekommunikations-Anbieter. Problem: Diese haben schon immer diverse Verbindungsdaten kurzfristig gespeichert, aber je länger sie speichern (müssen), desto genauer kann ein Profil über dich werden.
- Die Polizei, ➤Geheimdienste und die Regierung. Problem: Sobald der Verdacht besteht, dass du beispielsweise in Verbindung zu einer Straftat stehst, können diese Daten über dich angefordert werden. Das Schwierige an der Sache: Vielleicht warst du nur zufällig in der Nähe, wenn jemand eine Straftat begeht und du gerätst womöglich in das Visier der Ermittler. Eigentlich ist es die Aufgabe der Justiz (z.B. Anwälte), zu beweisen, dass du schuldig bist, aber nun musst du vielleicht selbst beweisen, dass du unschuldig bist. Solange du deine Unschuld nicht beweisen kannst, bleibst du unter Verdacht.
- Ein weiteres Problem: Diese Daten sind sehr wertvoll und daher auch für kriminelle Hacker sehr interessant. Es besteht also die Möglichkeit, dass Fremde an diese Daten herankommen und das ist auch in der Vergangenheit schon passiert.

Schlimm genug...
aber was ist außerdem schlecht daran?

- Zunächst: Vorratsdatenspeicherung ist ein massiver Eingriff in die ➤Privatsphäre! Es geht niemanden etwas an, wann du dich wo aufhältst und wer deine Freunde sind. Du solltest selber entscheiden können, welche Informationen du preisgibst.
- In manchen Berufen ist es wichtig geheim zu bleiben, zum Beispiel im Journalismus. Journalist.innen versuchen, an noch unveröffentlichte Neuigkeiten zu kommen und müssen dafür viel recherchieren. Wenn die Kommunikationsdaten mit anderen gespeichert werden, dann könnten geheime Informant.innen nicht mehr geheim bleiben. Dann steht nicht nur der Job, sondern auch die Sicherheit der Journalist.innen und auch der Informant.innen auf dem Spiel, insbesondere, wenn es sich um Kritik am Staat oder zum Beispiel an den Geheimdiensten handelt, die diese Daten selbst in die Hände bekommen. Das schadet der Demokratie.



Wearable

„Wearable" bedeutet auf Deutsch „tragbar" oder „anziehbar". Der Begriff bezeichnet also Gegenstände und Kleidung, die am Körper getragen werden können, und zwar solche, die als „smart" oder „intelligent" bezeichnet werden, weil sie mit dem Internet verbunden sind oder mit anderen Geräten interagieren/kommunizieren. Das kann zum Beispiel ein Fitnessarmband sein, eine intelligente Uhr (Smart Watch), die Google-Brille (Google Glasses) oder auch Lautsprecher, die in die Kapuze einer Jacke eingebaut sind. Wearables sind somit ein Teil des ➤Internets der Dinge, welche besonders nah am Menschen dran sind, viele persönliche Daten sammeln und ➤Big Data „füttern".

TIPP: Bevor du dein Taschengeld in besonders coole Wearable-Technik investierst, solltest du dir gut überlegen, ob es dir wert ist, dass du so viele persönliche Daten von dir einfach kostenlos für große Unternehmen zur Verfügung stellst.

Web ★

„Web" ist die Abkürzung für ➤World Wide Web. Das Wort wird oft für „Internet" eingesetzt, was aber falsch ist, da das World Wide Web nur einen Teil des gesamten Internets ausmacht.

Webseite

Eine „Webseite" ist eine Internetseite im ➤World Wide Web. Mit dem englischen Wort „Website", bezeichnet man mehrere Seiten, die aber alle zusammen gehören und vom gleichen Anbieter stammen. „Site" ist englisch und heißt so etwas wie „Landschaft". Jede Website und jede Webseite hat eine eigene Adresse/➤URL.

Whistleblower ★

„Whistleblower“ (übersetzt: Hinweisgeber) sind Personen, die ganz brisante Geheimnisse in den Bereichen Wirtschaft und Politik veröffentlichen, zum Beispiel Informationen über Datenmissbrauch, Korruption (Bestechung) oder Insiderhandel (Informationen, die heimlich ausgetauscht werden). Der Begriff wird vom englischen „whistle“ abgeleitet, was „pfeifen“ oder im weiteren Sinne „verpfeifen“, also „verpetzen“ bedeutet. Die Informationen, die Whistleblower enthüllen, sind meist von so großer Bedeutung, dass die Personen anonym bleiben müssen, um nicht verklagt zu werden, sich vor Feinden zu schützen oder ihren Job nicht zu verlieren.

Ein sehr bedeutender Whistleblower der heutigen Zeit ist Edward Snowden, der zuletzt als ➤Admin für den US-amerikansichen ➤Geheimdienst NSA gearbeitet hat. Im Jahr 2013 enthüllte er, welche Maßnahmen vor allem die amerikanischen und britischen Geheimdienste, aber auch diverse andere Geheimdienste, verwenden, um ➤Telekommunikationsdaten und die Kommunikation im Internet weltweit zu überwachen. Der BND (Bundesnachrichtendienst) als deutscher Geheimdienst, tauchte in den Dokumenten ebenfalls

als Partner auf. Dabei kam heraus, dass nicht nur Millionen von Bürgerinnen und Bürgern weltweit ausspioniert wurden, sondern auch die Gespräche von über 100 verschiedenen Staats- und Regierungschefs überwacht wurden, darunter auch über 300 Gespräche von Bundeskanzlerin Angela Merkel. Snowden verriet also streng geheime Informationen über Spionage und wurde somit innerhalb dieser Behörden selbst zum Spion. Um sich zu schützen, ist er aus den USA geflohen und kann nicht dorthin zurückkehren.

Snowden gab seine Informationen 2013 als erstes an die Dokumentarfilmerin Laura Poitras und Glenn Grennwald, einem Journalisten der Zeitung „Guardian“, weiter. Zusammen produzierten sie heimlich den Film „Citizenfour“, der nach Snowdens Decknamen benannt ist, den er verwendete, bevor er seine wahre Identität bekannt gab. Dass er seinen Namen veröffentlicht hat und wir auch wissen, wie er aussieht, ist auf seinen eigenen Wunsch geschehen. Er wollte, dass die Geheimdienste sich nicht damit heraus reden können, dass sie die Quelle der Informationen unbekannt und somit nicht glaubhaft ist.

AUFGABE: Schau dir sowohl den Dokumentar-Film „Citizenfour“ (2014), als auch den Spiel-Film „Snowden“ (2016) an, um mehr über Edward Snowdens Enthüllungen zu erfahren. Wie würdest du dich in so einer Situation verhalten? Findest du es gut, dass wir jetzt vieles wissen, was Geheimdienste tun und wie sie zusammenarbeiten? Oder hätte Edward Snowden alles geheim halten sollen, wozu er verpflichtet war?

Wiki

Wikis sind Internetseiten, die von den Nutzer.innen gelesen, aber auch verändert werden können. Sie dienen meistens dazu, um anderen Menschen etwas zu erklären, ähnlich wie ein Lexikon oder eine Bedienungsanleitung. Das bekannteste Wiki ist „Wikipedia“. Dadurch, dass alle möglichen Menschen an den Seiten mitschreiben können, wird es nicht gerne gesehen, wenn Wikipedia in Hausaufgaben, für Referate oder für andere wissenschaftliche Arbeiten verwendet wird. Die Inhalte könnten theoretisch auch falsch sein. Natürlich sind viele Dinge, die dort stehen, richtig und mit Quellen belegt. Es gibt also Verweise auf Bücher oder ➤Links, die beweisen, dass diese Information richtig und nicht ausgedacht ist.

AUFGABE: Gib mal dein Lieblingstier bei Wikipedia ein und schau dir die Seite ganz genau an. Da die meisten Wikipedia nur nutzen, um schnell etwas nachzuschlagen, fällt den Wenigsten auf, was es dort noch alles zu entdecken gibt. Du kannst beispielsweise bei jedem Artikel zwischen „Artikel“ und „Diskussion“ wählen. Schau dir mal an, was zu deinem Lieblingstier diskutiert wird.

World Wide Web (WWW)

Das World Wide Web (WWW) ist ein wichtiger Teil des Internet, das über viele ➤Webseiten verfügt, die mit ➤Links, bzw. Hyperlinks miteinander verknüpft sind. Es wird oft mit dem Internet gleichgesetzt, doch das WWW macht nur einen kleinen Teil des gesamten Internets aus. Andere Teile sind zum Beispiel E-Mail,

tig, denn du meinst damit wahrscheinlich eine Webseite.

Um das WWW nutzen zu können, benötigst du einen ➤ Browser/Webbrowser. Jede Website hat eine genaue Adresse, wie zum Beispiel www.kidsdigitalgenial.de, die über das Protokoll HTTP oder HTTPS („Hypertext Transfer Protocol Secure" = sicheres Hypertext-Übertragungsprotokoll) aufgerufen wird. Zusammen ergibt das dann die „URL" also den genauen Speicherort/die „Adresse" der Website im World Wide Web. In diesem Beispiel: https://kidsdigitalgenial.de.

Dateiaustausch (Filesharing), oder Internet-Telefonie (VoIP). Die Bezeichnung „Internetseite" ist somit nicht ganz rich-

Wurm In der ➤IT-Branche ist mit „Wurm" eine Art der ➤Schadsoftware gemeint.

Zensur ★

Wahrscheinlich kennst du das Wort „Zensur" als Begriff für Noten in der Schule. Es gibt aber noch eine andere Bedeutung, nämlich die Kontrolle oder der Verbot von Inhalten durch (staatliche) Behörden, zum Beispiel in den ➤Medien. Das heißt: Regierungen (die Chefs und Chefinnen der Länder) und große Firmen löschen oder verbieten Informationen, die andere nicht bekommen sollen. Sie verhindern die Verbreitung von Informationen, die ihnen oder anderen schaden könnten, die nicht in der ➤Presse auftauchen sollen und wollen die Kontrolle über Informationen behalten.

In Deutschland gilt die Presse- und Informationsfreiheit, die es Journalist.innen ermöglicht, ihre Meinung frei zu äußern, auch wenn sie eine schlechte Meinung von etwas haben. In der Türkei beispielsweise, also gar nicht weit von uns entfernt, werden viele Texte, Bilder und Videos verboten. Wer zum Beispiel etwas Schlechtes über türkische Politiker.innen oder über das Land schreibt, kann dafür verhaftet werden. Noch extremer ist die Zensur in China: Die Menschen in China bekommen seit Jahrzehnten nur die Informationen zu lesen, die die Regierung erlaubt. Auch wenn die Bürgerinnen und Bürger ➤Suchmaschinen im Internet nutzen, um Informationen zu bestimmten Themen recherchieren, finden sie nichts darüber oder nur Artikel, die aus einer Sichtweise geschrieben sind, die den chinesischen Politiker.innen gefällt. Die Menschen dort haben bei vielen politischen Themen also gar nicht die Möglichkeit, sich umfassend zu informieren und ihre persönliche Meinung wird gezielt in eine Richtung gelenkt, also manipuliert. Das Löschen der Beiträge im Internet übernehmen ganz viele Menschen, die dafür bezahlt werden und nichts darüber verraten dürfen. Wenn herauskommt, dass sie doch etwas verraten haben, werden sie in Gefängnisse gesperrt oder schlimmeres.

Auch bei uns hat es mal eine starke Zensur gegeben. In den „alten Bundesländern" im Westen Deutschlands, wurden noch bis in die 1950er-Jahre unerwünschte Bücher verbrannt, Filmaufführungen verhindert und Journalist.innen verfolgt. In Ost-Deutschland (ehemalige DDR) wurde die Presse noch bis in die späten 1980er-Jahre streng überwacht.

Auch wenn die Zensur durch Politiker.innen in Deutschland auf den ersten Blick mittlerweile abgenommen hat, heißt das aber noch lange nicht, dass es keine Zensur mehr gibt. Heute werden manchmal beispielsweise kinderpornographische Inhalte und brutale Gewaltvideos von den jeweiligen Internetanbietern gesperrt. Auch das Melden und Löschen von Hasskommentaren und anderen unangemessenen Inhalten in ➤Sozialen Netzwerken ist eine Form der Zensur. Hier ist besonders schwierig einzuschätzen, welche Inhalte noch zur freien Meinungsäußerung gehören und welche den Menschen wirklich schaden können.

Welche Inhalte im Internet gelöscht oder gesperrt werden, wird teilweise von Menschen entschieden, teilweise von ➤Algorithmen, die nach bestimmten Schlagworten suchen. Dabei passieren oft Fehler, denn nur weil jemand das Wort „Droge" schreibt, kann der Algo-

rithmus nicht beurteilen, ob hier Drogen verkauft werden oder ob jemand vor Drogen warnt. Pfiffige Menschen schaffen es, auch verbotene Dinge so zu beschreiben, dass kein Algorithmus das per Wortsuche heraus bekommen kann. Und wenn Menschen beurteilen, welche Inhalte gelöscht werden sollen, passieren ebenfalls Fehler, weil jeder Mensch ein anderes Empfinden von richtig/falsch und gut/böse hat, selbst wenn es einige eindeutige Fälle gibt. Ob alle Sperrungen gerechtfertigt sind, ist unmöglich zu kontrollieren. Selbst wenn es möglich wäre: Wer hätte dann das Recht, darüber zu entscheiden?

Wichtig: Angeblich soll uns Zensur vor Gewalt, Ausgrenzung und Straftaten schützen und außerdem vermeiden, dass sich jemand schlechtes Verhalten abguckt und nachmacht. Wir müssen in Zukunft aber ganz genau aufpassen, dass „Schutz" nicht zur Ausrede wird und dass wir dabei nicht die Informations- und Meinungsfreiheit verlieren, für die unsere Vorfahren gekämpft haben. Das kann schneller passieren als du denkst, denn auch China rechtfertigt die starke Zensur als „Schutz für das Land" und es gibt sehr viele Menschen, die das glauben und darauf reinfallen.

ZIP-Datei

Die Abkürzung „ZIP" kommt von „zipper", was auf Englisch „Reißverschluss" bedeutet. Es handelt sich dabei um ein Datei-Format, das du an der Endung „.zip" erkennst. Um eine ZIP-Datei zu öffnen, musst du diese mit einem geeigneten Programm (zum Beispiel mit „7-zip") „entpacken", denn das Besondere an dieser Datei ist, dass sie meist weitere Dateien enthält. Wenn beispielsweise viele verschiedene Dateien gleichzeitig per E-Mail verschickt werden sollen und die Dateien (zum Beispiel Fotos) sehr groß sind, also viel Speicherplatz benötigen, dann dauert das Versenden der Mail sehr lange, falls sie überhaupt versendet werden kann. In einer ZIP-Datei (sozusagen in einem Ordner) werden die einzelnen Dateien allerdings „komprimiert", also verkleinert. Wenn die Datei bei dem Empfänger angekommen ist, kann er/sie den Ordner entpacken und die komprimierten Dateien in ihre Ursprungsgröße zurück verändern („de- oder entkomprimieren"). Das Packen und Entpacken der Dateien kann man sich dabei bildlich wie das Öffnen und Schließen eines Reißverschlusses vorstellen.

Über die Autorin

Jessica Wawrzyniak ist studierte Medienpädagogin (MA) und im Verein Digitalcourage aktiv. Sie schreibt den Blog #Kids #digital #genial, der Kinder und Jugendliche in leicht verständlicher Sprache über Begrifflichkeiten der Digitalsierung, sichere Mediennutzung und Datenschutz aufklärt. 2017 nahm sie mit ihrem Blog an einem Bürgerprojekt-Wettbewerb im Kreis Münsterland und OWL teil. Unter dem Motto „Kompetent und fair in der digitalen Welt" sicherte sie sich eine finanzielle Förderung, welche die Umsetzung dieses Buchs ermöglichte.

Über Digitalcourage

Digitalcourage e.V. engagiert sich seit 1987 für Grundrechte, Datenschutz und eine lebenswerte Welt im digitalen Zeitalter. Wir mögen Technik, doch wir wehren uns dagegen, dass unsere Daten sinnlos gesammelt und verkauft werden. Digitalcourage ist gemeinnützig, das bedeutet, wir finanzieren uns durch Spenden und ganz viel Arbeit im Verein wird ehrenamtlich (ohne Bezahlung) getätigt.

Index

Blog:

#Kids #digital #genial

Tipps und Tricks im Umgang mit Medien und Datenschutz:

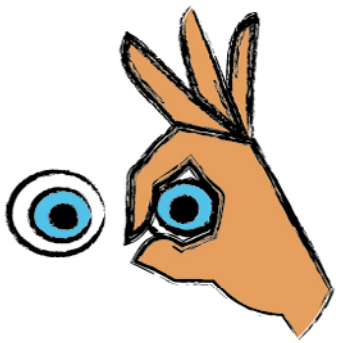
kidsdigitalgenial.de

Hinweise zum Einsatz des Lexikons im Unterricht:

kidsdigitalgenial.de/unterricht

Online bestellbar unter:

shop.digitalcourage kids-digital-genial



#KIDS #DIGITAL #GENIAL

Was ist ein „Browser“? Wie funktioniert ein „Algorithmus“? Und wofür sind „Cookies“ eigentlich da?

Du hast bestimmt schon von diesen Begriffen gehört, aber kannst du sie auch anderen erklären? Das können nur sehr wenige – und du kannst nun dazu gehören! Das #Kids #digital #genial-Lexikon umfasst über 100 Begriffe rund um Netz, Digitalisierung und Mediennutzung.

Du wirst das Internet, dein Smartphone und deine eigene Mediennutzung von einer ganz anderen Seite kennenlernen – mit Respekt vor persönlichen Daten und Privatsphäre.

Wieso bekomme ich unerwünschte Mails? Wie erkenne ich Fake News? Und was muss ich beim Veröffentlichen von Fotos beachten?

Endlich gibt es Antworten, auch auf Fragen, die du dir noch nie gestellt hattest. Und es gibt auch viele kleine Aufgaben zum Mitmachen und Mitdenken. Mach mit! Schütze dich und deine Daten!

#Kids #digital #genial findet Technik, Medien und das Internet super und unverzichtbar, aber den Schutz von privaten Daten genauso. Lerne mit ein paar Tipps und Tricks, wie beides zusammen geht und werde zum Profi im Netz!

digitalcourage

ISBN 978-3-934636-20-0 Verlag Art d'Ameublement
2. erweiterte Auflage | € 3,85 (D) | € 3,85 (Ö) | SFr 4,35 (CH)