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

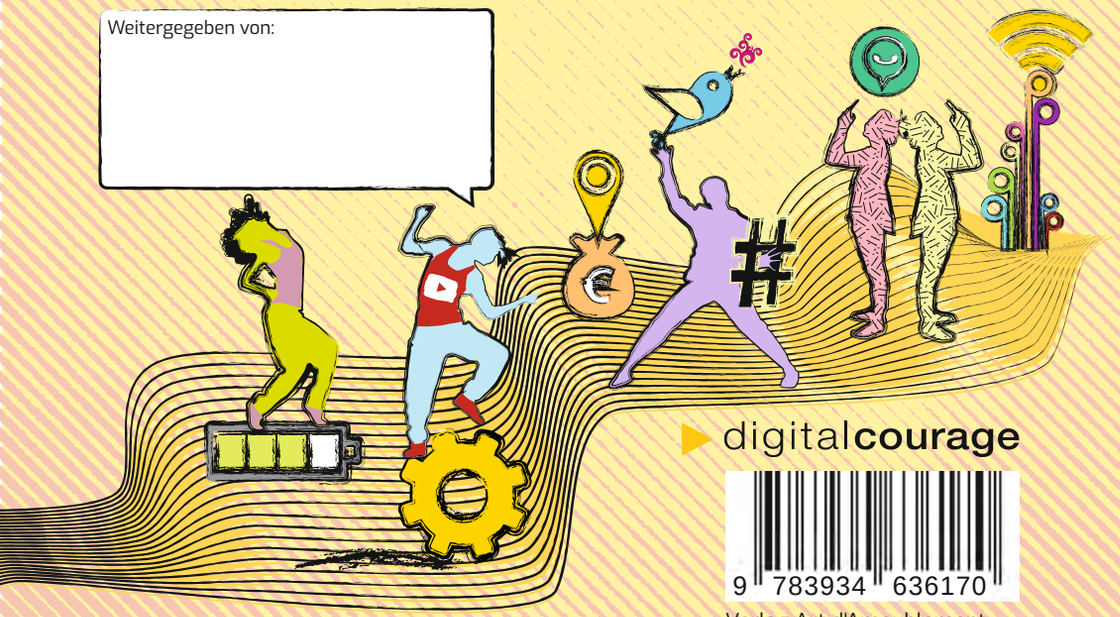
Du hast bestimmt schon von diesen Begriffen gehört, aber kannst du sie auch anderen erklären? Das können nur sehr wenige – und du kannst nun dazu gehören! Das #kids #digital #genial-Lexikon umfasst über 100 Begriffe rund um Netz, Digitalisierung und Mediennutzung.

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

9 783934 636170

Verlag Art d'Ameublement

digitalcourage (Hrsg.)

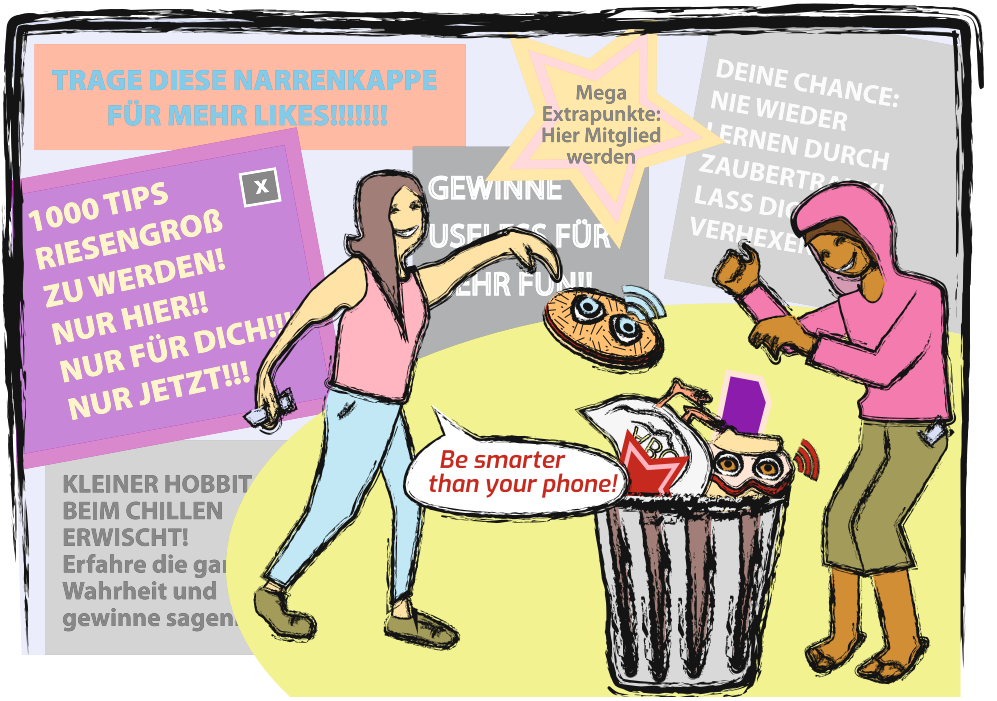
Jessica Wawrzyniak

#KIDS #DIGITAL #GENIAL

Schütze dich und deine Daten!

Das Lexikon von App bis .zip

Verlag Art d'Ameublement



Online-Werbung

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

- 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 z.B. zu ➤In-App-Käufen anregt. Manche Spieler. innen werden auch damit gelockt, dass sie Extrapunkte bekommen, wenn sie nur auf die Werbung klicken.

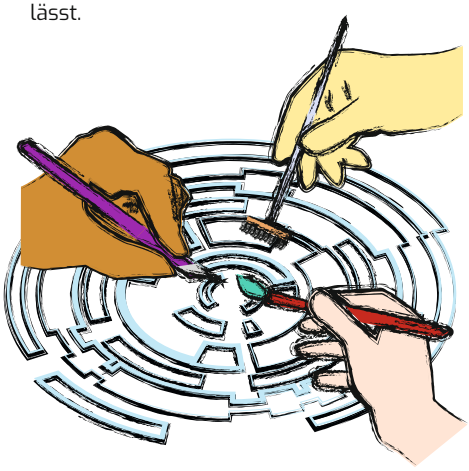
So kannst du dich vor lästiger Werbung schützen:

- **Werbeblocker einschalten:** Stell in den ➢Browser-Einstellungen ein, dass Pop-ups nicht zugelassen werden und installiere einen Ad-Blocker (Werbeblocker), wie z.B. „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 vs. kostenlose 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 z.B. 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 jeder, der Lust hat, 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 herausfinden, 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"
- ...

Opt-in/out

Opt-in und -out sind Bezeichnungen für Auswahlmöglichkeiten. Wenn du dir beispielsweise einen ➢Account für einen Online-Dienst einrichtest (z.B. für ein Spiel oder ein Profil in einem ➢Sozialen Netzwerk), musst du oft noch weitere Felder anklicken, z.B. 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").

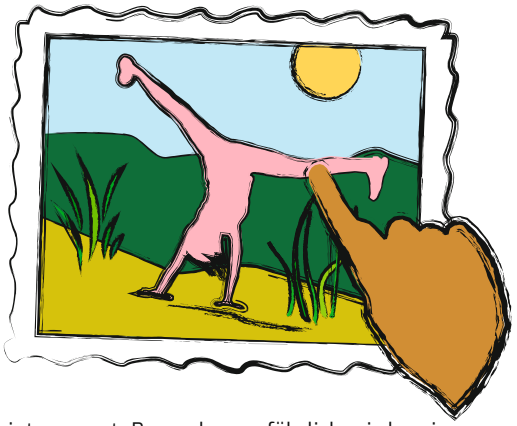
Du musst dir also solche Auswahlfelder immer genau anschauen und die Texte ganz genau lesen, um zu sehen, ob du ein Häkchen setzen oder entfernen solltest. Sonst kann es sein, dass du aus Versehen Dingen zustimmst, die du gar nicht möchtest. Manchmal wird auch mit (doppelten) Verneinungen getrickst, sodass du z.B. 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/etc. 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 z.B. 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 Medikamenten und Therapien behandelt werden.

Im Internet haben Pädophile viele Möglichkeiten, ihre Fantasien auszuleben, da sie z.B. 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 z.B. 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, z.B. 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.

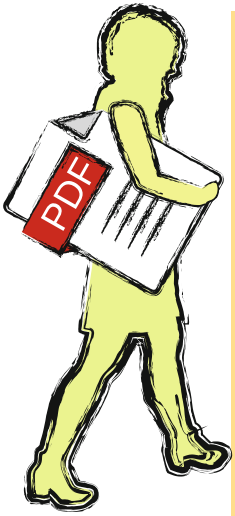
Dir kann auch jemand Geld auf dein PayPal-Konto überweisen, wenn du selber etwas verkauft hast. Dazu braucht der Käufer nicht deine Kontonummer, sondern nur deine E-Mail-Adresse, und PayPal kann dir die Zahlung dadurch zuweisen. Wenn du auf diesem Wege Geld bekommst, bezahlst du dafür jedoch eine Gebühr.

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. 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, bei dem genau abgebildet wird, was z.B. am Ende gedruckt werden 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 z.B. 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 z.B. 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!

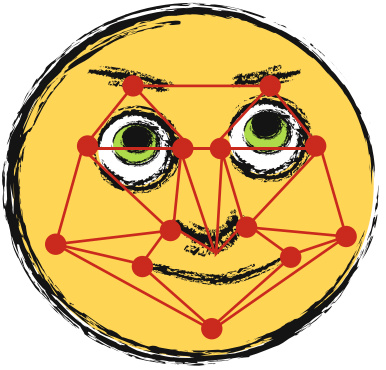
- Öffne ein Textbearbeitungsprogramm, z.B. „Libre Office".
- Schreib ein paar Zeilen darin.
- Klicke oben links auf „Datei".
- Speichere die Datei unter einem Namen ab.
- Wähle „Als PDF exportieren".
- Jetzt musst du dir nur noch merken oder nachsehen, in welchem Order das Dokument gespeichert wird, 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, z.B. „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 (z.B. durch das Klicken auf „Like"-Buttons), sondern auch durch dein Surfverhalten selbst. Es wird z.B. 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. 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



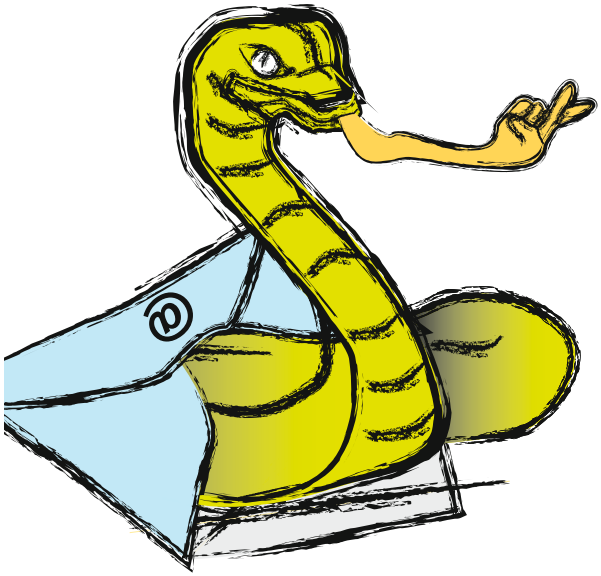
werden. So ist es beispielsweise bald möglich, dass du in einem Supermarkt an der Kasse stehst, von einer Kamera gefilmt wirst und dann an den digitalen Werbetafeln an der Kasse personalisierte Werbung angezeigt bekommst.

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, etc.), von Online-Shops oder anderen Unternehmen, bei denen es um Geld geht (z.B. ➢PayPal). Diese Seiten unterscheiden sich nur beim genauen Hinsehen vom Original.



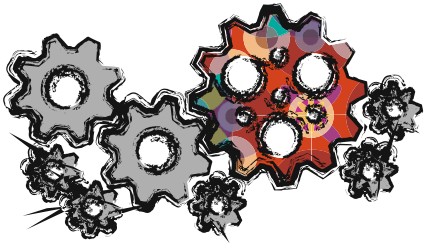
Du bekommst dann eine Mail, z.B. von einer Bank, mit einem ➢Link und der Bitte, dich einzuloggen und dir wichtige Informationen durchzulesen. Oder du sollst dich einloggen, weil angeblich jemand eine hohe Summe von deinem Konto abgebucht hat. Die Vorwände sind unterschiedlich, aber es geht immer nur 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

(z.B. mit vielen Zahlen drin). Noch auffälliger ist es, wenn du mit dem Unternehmen eigentlich gar nichts zu tun hast, weil du z.B. bei einer ganz anderen Bank bist. Du solltest diese Mails dann einfach löschen, dann kann nichts passieren.

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 z.B. in deinem ➢Browser installieren und sozusagen in dem Programm zusätzlich einstöpseln. Ein nützliches Plug-in für den Browser ist beispielsweise ein Werbeblocker (wie z.B. 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.



Prepaid

„Prepaid" ist Englisch und bedeutet „vorausbezahlt". Es handelt sich dabei also um eine Zahlungsvariante, z.B. 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 z.B. 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.

Privatsphäre

Deine Privatsphäre ist dein persönlicher, nicht-öffentlicher Bereich, indem du dich frei entfalten kannst. Solange du nichts Illegales/Strafbares oder Gefährliches machst, braucht es niemanden zu interessieren, was du in privaten Momenten und privaten Räumen tust. Die privatesten Bereiche sind z.B. Toiletten und Duschen, Umkleidekabinen, Schlaf-/Kinderzimmer und andere Wohnräume.

Privatsphäre gehört zu den Grundrechten jedes Menschen. Auch Kinder haben ein Recht auf Privatsphäre!

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 Videoka-

meras 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.

Push-Benachrichtigung

Wenn du ➢Apps auf deinem Smartphone oder Tablet benutzt, ist dir bestimmt schon einmal die Frage begegnet "Möchten Sie Push-Nachrichten erhalten?". Damit sind die Benachrichtigungen gemeint, die auf deinem Sperr- oder Startbildschirm des Smartphones erscheinen. Diese können teilweise nützlich sein, um zu sehen, wenn du eine neue Nachricht von Freunden oder von deinen Eltern bekommen hast. Sie können aber auch sehr 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, z.B. 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 (z.B. 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.

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 z.B. 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

#KIDS #DIGITAL #GENIAL

Schütze dich und deine Daten!

Das Lexikon von App bis .zip

#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!

- Über 100 Begriffe
- Leicht verständliche Texte
- Tipps und Tricks zum Umgang mit privaten Daten
- Kleine Aufgaben und Denkanstöße
- Für den Einsatz im Unterricht geeignet
- Gehört in jeden Schulranzen!

Hinweise zum Einsatz des Lexikons im Unterricht unter:
kidsdigitalgenial.de/unterricht

- Mengenrabatt bei Klassensätzen:
  Einzelpreis 2,45 €
  ab 11 Stk. je 2,27 €
  ab 26 Stk. je 2,23 €
- Versandkostenfrei

Bitte das ausgefüllte Formular per Brief schicken an Digitalcourage e.V., Marktstraße 18, 33602 Bielefeld oder **online bestellen** im Digitalcourage-Shop unter shop.digitalcourage.de/kids-digital-genial.
Auch im Buchhandel erhältlich: ISBN: 9-783934 -636170

Ich bestelle _____ Exemplare
der Broschüre #kids #digital #genial.

Liefer- und Rechnungsadresse:

Institution: _____

Name: _____

Straße/Hausnr.: _____

Adresszusatz: _____

PLZ: _____ Ort: _____

E-Mail: _____

[ ] Ja, ich möchte weitere Informationen von Digitalcourage e.V. erhalten.

digitalcourage