DigiFit© Mach dich fit fürs Netz

Begleitheft zum Kartenspiel
Die Möglichkeiten und Risiken der digitalen Welt sind seit vielen Jahren wichtige Themen in der täglichen Arbeit mit Kindern und Jugendlichen. Sehr schnell stößt man aber an Grenzen und Graubereiche.
Welche Fotos soll/darf ich posten? Was geschieht mit meinen Daten? Sind Cybermobbing und Phishing legal? Und wie wollen wir als Gesellschaft mit all dem umgehen?

DigiFit ist ein Kartenspiel, das spielerisch zeigt, wie Kinder und Jugendliche ihre Privatsphäre schützen können. Im Spiel lernen sie mögliche Gefahren beim Nutzen digitaler Medien kennen. Dieses Begleitheft bietet Beispiele und Hilfestellungen für den analogen Umgang mit diesem Thema an. Das Spiel unterstützt Kinder und Jugendliche dabei, zu erkennen wie wichtig digitale Selbstbestimmung ist, und gibt ihnen praktische Tipps dazu.

Sonja Zechner ist als Schöpferin von DigiFit tief in die digitale Welt eingetaucht. Textliche Unterstützung hat sie vom Kinderbüro–Die Lobby für Menschen bis 14 durch Romana Rossegger, Sonja Buchegger und Jessica Braunegger bekommen. Dabei waren die Kinderrechte immer eine wichtige Grundlage. Die Herstellung und Verteilung des Spiels erfolgen durch Karli Printi.

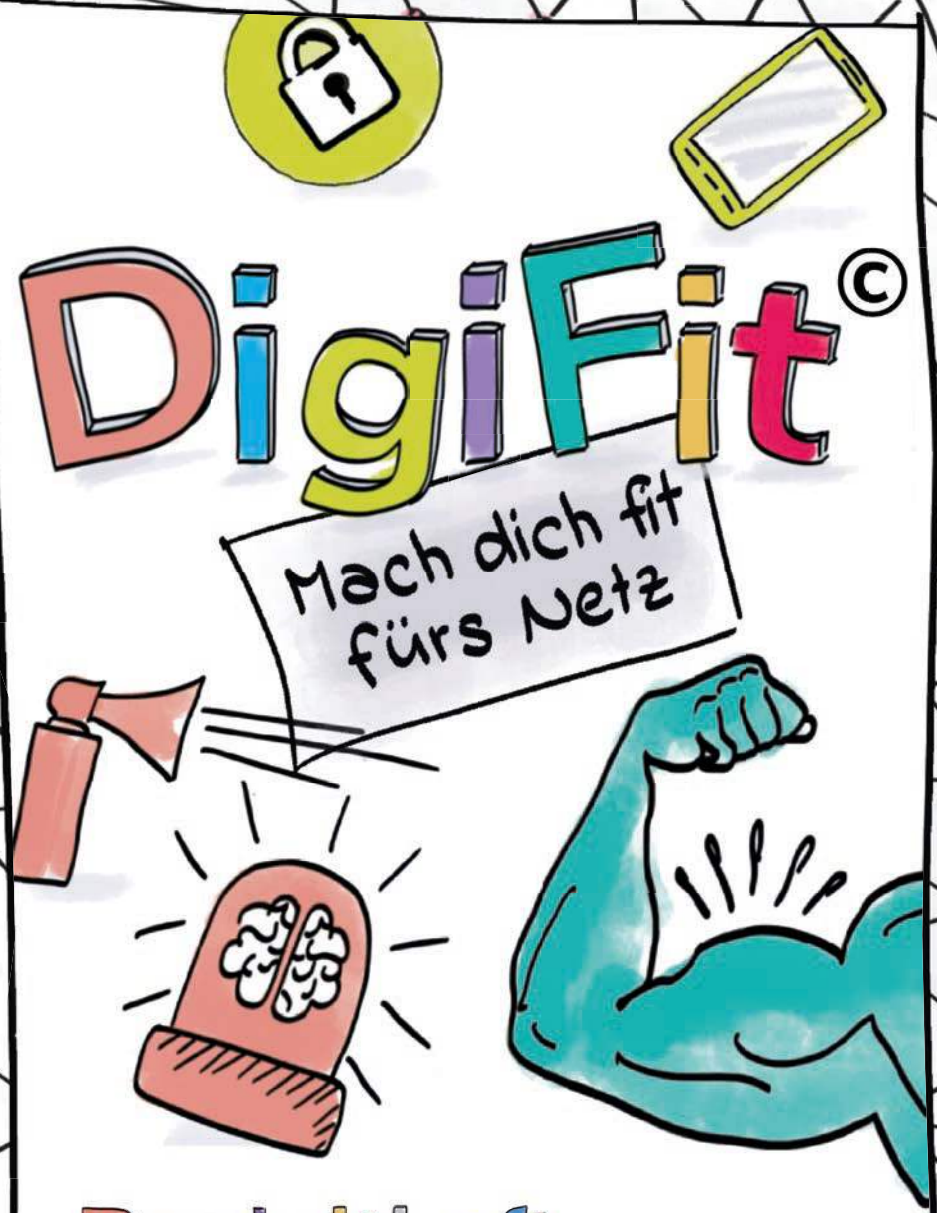
Ein herzliches Danke an alle Beteiligten für ihren kreativen Einsatz und an die vielen Expert:innen (Kinder und Erwachsene), die mit ihren Inputs, Anregungen und Kritiken Digifit erst möglich gemacht haben.

Wir wünschen allen Spielenden viel Spaß und lehrreiche Momente!

Du hast Anregungen, Fragen oder weiter Spielideen?
Dann sende uns eine E-Mail an **office@kinderbuero.at**.

Das Entwicklungsteam Sonja Z., Sonja B., Romana, Jessica und Thomas

Impressum: Graz © 2022 | Herausgeber: Verein Kinderbüro® – Die Lobby für Menschen bis 14 | Konzept, Grafik und Layout: Sonja Zechner | Text: Sonja Buchegger, Romana Rossegger, Thomas Plautz, Jessica Braunegger | Druck: Karli Printi GmbH® | Vertrieb: www.karlisshop.at



Begleitheft zum Kartenspiel

Konzept | Grafik | Layout:
Sonja Zechner B.A.
Brunnengasse 9
A-8063 Eggersdorf bei Graz
www.sonjazechner.com

Herausgeber:
Verein Kinderbüro® – Die Lobby für Menschen bis 14
Karmeliterplatz 2/3
8010 Graz
www.kinderbuero.at

Vertrieb:
Karli Printi GmbH®
Kärntner Straße 565
A-8054 Graz
www.karlisshop.at

Druck:
Karli Printi GmbH®
Kärntner Straße 565
A-8054 Graz
www.karliprinti.at

©Copyright Kinderbüro 2022 Alle Rechte vorbehalten
„DigiFit“ ist eine registrierte Marke. Sämtliche Bestandteile sind urheberrechtlich geschützt. Jegliche Verwendung, Vervielfältigung und Veröffentlichung von Inhalten des Spiels (auch nur in Auszügen oder auch in digitaler Form) bedarf der vorherigen schriftlichen Genehmigung durch das Kinderbüro.

Vorwort

Für Kinder und Jugendliche ist die digitale Welt heute so selbstverständlich wie Zähneputzen oder Telefonieren. Sie scheinen den virtuellen Raum bereits von klein auf intuitiv zu verstehen. Kinder und Jugendliche bewegen sich selbstverständlich und offen in dieser Welt.

Die Digitalisierung hat den gesellschaftlichen Fortschritt beschleunigt und unzählige Aufgaben erleichtert oder überhaupt erst möglich gemacht. Zugleich hat sie uns als Einzelpersonen aber auch gläserner, abhängiger und manipulierbarer gemacht.

Wie bei vielen (technischen) Entwicklungen gilt auch in diesem Zusammenhang: Der Umgang mit den Möglichkeiten entscheidet über Nutzen oder Risiko, über Mehrwert oder Gefahr.

Das vorliegende Spiel will auf lustige, unterhaltsame und reale Weise das Bewusstsein für den Umgang mit den digitalen Möglichkeiten stärken. Außerdem soll es für Themen wie digitale Sicherheit, persönliche Rechte, vor allem Kinderrechte, und einen achtsamen Umgang mit persönlichen Daten sensibilisieren, ohne zu belehren. Es soll nicht nur Kinder, sondern auch Erwachsene ansprechen und das gemeinsame Erleben im Spiel mit Spaß und guter Laune fördern.

Das vorliegende Begleitheft dient der Vertiefung in einzelnen Bereichen. Es gibt genauere Einblicke in digitale Themen mit vielen nützlichen Hinweisen und Links zu weiterführenden Quellen.

Euer Entwicklungsteam, Sonja Z., Sonja B., Romana, Jessica und Thomas

Hier findest du den
Link zum Begleitheft
und **zur Spielanleitung**:

www.kinderbuero.at

Info

Wie ist dieses Begleitheft zu verwenden?

Das Spiel kannst du auch ohne Begleitheft spielen, damit du schnell und unkompliziert starten kannst. Wenn du zu einem der sechs Themenbereiche mehr Infos, Anregungen und Tipps „einfach zum Nachdenken“ möchtest, nimm dieses Begleitheft zur Hand und mach' dich schlau!

Jedes Thema ist in eine kurze Geschichte verpackt, die zum Nachdenken und Darüber-Sprechen anregt. Neben nützlichen Informationen sind auch weiterführende Links (siehe *"Weitere Informationen"*) und die Beschreibung der entsprechenden Spielkarten enthalten.

Dieses Begleitheft ist für Pädagog:innen und Eltern sehr gut geeignet, um mit Kindern und Jugendlichen die einzelnen Themen zu besprechen und zu vertiefen.

Ab wann dürfen Kinder WhatsApp, Instagram und Co. nutzen?

Lily, Max und ihre Freund:innen verwenden WhatsApp, TikTok und andere digitale Medien wie selbstverständlich. Offiziell ist das Nutzen von sozialen Netzwerken in Österreich erst ab 14 Jahren erlaubt. Das gilt, obwohl du laut Facebook und Instagram nur 13 Jahre alt sein musst, um sie zu nutzen. Diese Altersbeschränkungen gibt es aus gutem Grund, daher solltest du dich daranhalten.

In der Praxis gibt es viele Kinder, die diese Kanäle nutzen, obwohl sie jünger sind. Wenn du schon gegen die Altersbeschränkung verstößt, solltest du unbedingt deine Eltern um Erlaubnis bitten, bevor du einen dieser Dienste verwendest. Ein soziales Netzwerk gemeinsam zu erkunden, klare Regeln zu vereinbaren und Risiken anzusprechen ist wichtig. So wirst du bessere Erfahrungen mit digitalen Medien machen und deine Eltern wissen, dass du online sicher unterwegs bist.

Mehr Infos zum Thema findest du hier:
www.saferinternet.at

Lilly und Max

gehen dem Netz auf die Spur!

Lilly und Max sind schon lange befreundet. Obwohl Lilly schon 14 Jahre alt ist und Max erst 9 Jahre alt ist, verstehen sich die beiden wirklich gut.

Zusammen entdecken sie die vielen Möglichkeiten, die das Internet bietet. Sie machen aber auch Fehler und lernen, was sie tun können, um unangenehme Situationen zu vermeiden. Begleite Lilly und Max bei ihren digitalen Abenteuern!

DigiFit®

Mach dich
fit fürs Netz!

Medienkompetenzkarten

		Seite
Kritisch denken	Glaube nicht alles, was im Internet steht!	9
	Achte auf versteckte Kosten!	12
	Bevor du klickst, denk nach!	14
Rechtliches	Lade keine fremden Inhalte im eigenen Kanal hoch!	19
	Beachte "Das Recht am eigenen Bild"!	20
	Geh respektvoll mit anderen um!	21
Sichere Zugangsdaten	Schütze dein Passwort!	25
	Verwende einen Nickname!	26
	Bleibe sicher und geschützt!	27
Einstellungen der App	Deaktiviere In-App-Käufe!	31
	Poste keinen Standort!	32
	Kontrolliere deine Privatsphäre-Einstellung!	33
Ich in der digitalen Welt	Gib nicht zu viel preis!	37
	Das Internet vergisst nicht!	38
	Deine Daten gehören dir!	40
Regelmäßige Kontrolle	Schütze deinen Computer!	43
	Mache regelmäßig Updates!	44
	Kontrolliere regelmäßig deine Inhalte!	45

Hacker:innenkarten

Seite	
49	Filter
49	Öffentliches Netzwerk
50	Unseriöses Gewinnspiel
50	Viren
51	Influencer:innen
51	Grooming
52	Mobbing
52	Gestalte deine eigenen Hacker:innenkarten

Weitere Informationen

53	Links zu weiteren Informationen
55	Literaturverzeichnis
55	Stichwortverzeichnis

Spielanleitung

57	Links zur Anleitung und zum Begleitheft

Kritisch denken

Der Kettenbrief

Es ist ein typischer Samstag, Lilly und Max ist wieder einmal langweilig. Sie sitzen bei Max zuhause im Wohnzimmer und draußen regnet es aus Kübeln. Max wirkt nachdenklich. Er scheint sich über irgendetwas den Kopf zu zerbrechen.

Lilly: Was ist denn los, Max?

Max: Ich habe zum Geburtstag ein Smartphone bekommen, und bin nun auch endlich in der WhatsApp Gruppe meiner Klasse.

Lilly: Und? Das ist doch gut, oder etwa nicht?

Max: Ja schon, aber ich habe auf WhatsApp gestern diese Nachricht bekommen. Schau mal! Hast du davon schon einmal gehört?

Lilly *(lacht)***:** Ach Max! Mach dir keine Sorgen! Das ist ein kompletter Blödsinn! Das sind Nachrichten, die versendet werden, um anderen Angst zu machen! Denk doch mal nach! Glaubst du wirklich, dass ein Geist zu dir nach Hause kommt, nur wenn du diese Nachricht nicht an 15 weitere Personen versendest?

Max *(muss nun auch lachen)***:** Ja, du hast recht, aber es hat so echt geklungen.

Lilly: Das verstehe ich! So ist es mir auch gegangen, als ich so eine Nachricht zum ersten Mal bekommen habe. Im Internet gibt es Vieles, worauf du Acht geben musst, Max! Mir und meinen Freund:innen ist leider auch schon öfter etwas passiert. Aber damit du nicht die gleichen Erfahrungen machen musst, erzähl ich dir gern ein bisschen mehr darüber. Natürlich nur, wenn du möchtest!

Max: Ja bitte, unbedingt!

Fragen

Wie geht es dir, wenn du diese Geschichte hörst?

Hat eine Person, die du kennst, schon einmal so eine Nachricht bekommen?

Würdest du bei so einer Nachricht antworten?

Wenn ja, was würdest du schreiben?

Hier geht es um den kritischen Umgang mit Informationen und Angeboten aus dem Internet oder von einer App: Kann das stimmen? Von wem stammt das? Darf ich jedes Video anschauen? Soll ich das teilen? Was passiert, wenn ich diesen Link anklicke? Runterladen oder doch nicht?

Glaube nicht alles, was im Internet steht!

Warum werden falsche Nachrichten erstellt und verbreitet? Manche Verfasser:innen wollen bewusst provozieren, andere politischen oder finanziellen Nutzen ziehen. Viele verdienen mit außergewöhnlichen, nicht (ganz) der Wahrheit entsprechenden Geschichten ihr Geld. Oft werden Falschmeldungen verbreitet, weil sie einfach geglaubt werden. Daher ist es sehr wichtig, Inhalte zu hinterfragen und gegebenenfalls zu überprüfen.

Stichworte

- **Falschmeldungen (Fake News)**
  Sind erfundene oder gefälschte Geschichten/Nachrichten oder veränderte Geschichten/Nachrichten, die nur noch teilweise der Wahrheit entsprechen.
- **Hoax**
  Ist eine Falschnachricht im Internet, die absichtlich als solche verbreitet wird. Das können Scherzmeldungen und Kettenbriefe über Fake Fotos bis hin zu „Horrormeldungen“ sein.
- **Seriöse Quelle**
  Erstellt Informationen/Nachrichten, die vertrauenswürdig sind z.B. Wissenschaftler:in, Universität, Ministerium.

Sei skeptisch! Nimm Infos nicht immer für wahr an! Schicke sie nicht weiter, ohne nachzudenken! Achte zuerst auf ihre Herkunft und Glaubwürdigkeit.

Diese Tipps helfen dir dabei, Falschmeldungen zu erkennen:

- Achte auf **reißerische Formulierungen** und emotionale Sprache. Das können Hinweise auf mögliche Fake News sein. Wie zum Beispiel: “Schlimm, was hier passiert ist!”, “Wahnsinn! Unfassbar diese Story!”. Dazu gehören auch schockierende Bilder. Oft geht es auch um Bedrohungen und mögliche katastrophale Szenarien, die Angst und Unsicherheit auslösen (sollen).
- **Click-Bait-Videos oder -Schaltungen** versuchen mit sensationellen Inhalten, dramatischen Bildern und reißerischer Sprache zu ködern (“bait” ist englisch für “Köder”). Solche weisen ebenfalls auf unseriöse Seiten oder Nachrichten hin. Videos enden mit einem Cliffhanger (einem offenem Ausgang) und zum Weiterschauen musst du extra klicken. Die versprochenen Inhalte gibt es aber oft gar nicht – man läuft nur Gefahr, sich damit Schadsoftware einzufangen. Diese Sensationsnachricht bzw. das Video sind nur „Köder“, damit du draufklickst - also lass es lieber sein! Überprüfe, ob Behauptungen, Zahlen oder Statistiken mit **Quellenangaben** belegt werden.
- **Hörensagen** ist meist keine verlässliche Informationsquelle.
  Sei hellhörig, wenn Sätze mit “Ich habe gehört, ...” oder “Eine Bekannte hat gesagt, ...” beginnen.
- Schau ins **Impressum** der Website oder der App. Dort steht, wer sie erstellt hat. So kannst du einschätzen, ob es sich um eine zuverlässige Quelle handelt. Sei jedenfalls vorsichtig, wenn es kein Impressum gibt.
- Gib die Autor:innen in eine Suchmaschine ein! **Expert:innen** erkennt man daran, dass sie an einem anerkannten Institut oder einer Hochschule arbeiten und zum gesuchten Thema arbeiten und/oder forschen. Achte auch auf eine neutrale Sprache: Vertrauenswürdige Fachleute vermitteln ihr Wissen so objektiv und neutral wie möglich.
- Auf glaubwürdigen Websites oder Apps finden sich zu einem Thema **mehrere Meinungen oder Standpunkte**.
- In unseriösen Nachrichten wird häufig **verallgemeinert:** “Wir sind ...!” oder “Alle Menschen ...”

- Viele Fake News sind in **Verschwörungstheorien** verankert. Diese sprechen von verborgenen Mächten, von Nutznießer:innen oder Sündenböcken. Sie unterteilen die Welt ausschließlich in Gut und Böse. Selbsternannte „Expert:innen“ erklären ihre Theorien mit emotional aufgeladener Sprache, “rütteln wach” und liefern vermeintliche “Beweise”, die nicht belegt werden. Sie stellen ihre Sichtweise als die “einzig gültige Wahrheit” dar.

- **Vergleiche** die Meldungen/Nachrichten mit Auskünften von anderen Websites oder Apps. Was schreiben angesehene Medien darüber?

- Finde heraus, wann die Information erstellt wurde. Ist sie **aktuell?** Ältere Infos könnten sich zwischenzeitlich geändert haben.

- Immer wieder werden auf sozialen Netzwerken (wie WhatsApp, aber auch Facebook oder Instagram) sogenannte **Kettenbriefe** versendet. Diese fordern dazu auf, die Nachricht an weitere Leute zu versenden („Schicke diese Nachricht an mindestens 10 Personen weiter!“). Sie drohen, dass etwas Schlimmes passiert (wie beispielsweise eine Krankheit, ein Unfall oder das Erscheinen eines Monsters), wenn du das nicht tust. Ganz wichtig: **Die angedrohten Gefahren sind nicht real!** Schicke vor allem gruselige Kettenbriefe nicht weiter, um nicht noch mehr Kinder unnötig zu ängstigen.

- **Im Zweifelsfall** die Nachrichten/Meldungen nicht teilen und weiterverbreiten! Sprich mit einer (erwachsenen) Person deines Vertrauens, wenn du dir unsicher bist!

- Achtung: Nicht nur Inhalte werden gefaked! Manchmal geben sich Menschen auch als jemand Anderes aus. Sie erstellen **Fake-Profile** und wollen so dein Interesse, dein Vertrauen und schließlich deine Daten oder mehr!

Achte auf versteckte Kosten!

Lesen, schauen, spielen. Toll, was das Internet alles bietet. Aber nicht jeder Klick hat rein informative, praktische oder unterhaltsame Folgen. Unbedachte Klicks haben oft unerwünschte psychische, rechtliche, technische und somit schädliche Konsequenzen.

Stichworte

- **Download**
  Dateien, also einzelne Programme, Filme, Musikstücke oder Bilder werden aus dem Internet auf den Computer, das Tablet oder das Handy kopiert, also dauerhaft gespeichert.

Bevor du einen Link zu einem Foto oder Video anklickst, denke über die folgenden Punkte nach:

- Auf YouTube, Instagram und Co gibt es merkwürdige, verstörende oder gar beängstigende Fotos oder Videos. Die meisten dieser Plattformen sind für Erwachsene gemacht. Daher sind viele **Inhalte für Kinder unpassend.** Besuche Plattformen von Erwachsenen nur gemeinsam mit Erwachsenen! Sie können dich vor unpassenden Inhalten schützen und/oder dir erklären, was die Inhalte bedeuten.

- Klick nicht gleich auf Download! Sei vorsichtig beim **Herunterladen von Dateien**! Dabei könntest du dich strafbar machen. Gibt es beispielsweise die aktuellen Hits aus den Charts gratis, solltest du sie nicht downloaden. Musik, Filme, Videospiele und andere Werke aus Kunst oder Wissenschaft sind normalerweise auf der ganzen Welt geschützt. Ohne Zustimmung der Urheber:innen oder der Besitzer:innen der Schutzrechte darfst du sie nicht kopieren und verbreiten. Urheber:innen sind: Künstler:innen, Verfasser:innen, Produzent:innen, Autor:innen, Erfinder:innen oder Ähnliches. Also Finger weg von **Tauschbörsen**, die mit kostenlosen Angeboten locken!

- Die meisten Video- und Audiodienste sind kostenpflichtig (Beispiele: Netflix, Amazon Prime, Apple iTunes, Sky online sowie Spotify, Tidal, YouTube Music etc.). Es gibt aber auch Plattformen mit freien Inhalten. Frei nutzbare Bilder, Musik und Videos fallen zum Beispiel unter die CC-Lizenz (Creative Commons). Aber auch solche unterliegen diversen **Nutzungsbedingungen**, die du jedenfalls einhalten solltest.

- Achtung vor Betrug! Mit unbedachten Klicks kannst du dir auch eine **Schadsoftware (Malware)** einfangen. *Siehe auch "Schütze deinen Computer!"*

- Überlege gut, ehe du auf einen Link klickst, etwas herunterlädst oder auch E-Mail-Anhänge öffnest! Frage im Zweifelsfall eine (erwachsene) Person deines Vertrauens, bevor du das machst!

Bevor du klickst, denk nach!

Unüberlegte Klicks können auch zu versteckten bzw. unerwünschten Kosten führen, also negative finanzielle Folgen haben. Eine weitere Gefahr ist das unbedachte Bekanntgeben deiner Daten. Besondere Vorsicht gilt bei Apps und Online- und/oder Gewinn-Spielen, die mit speziellen Tricks zum Kaufen oder einem Abschluss eines kostenpflichtigen Abonnements verführen.

Stichworte

- **Versteckte Kosten, In-App-Kauf**
  Sind Käufe von Diensten oder Funktionen, die getätigt werden, während man eine App nutzt.

- **In-Game-Kauf**
  Sind Käufe, die getätigt werden, während man ein Spiel spielt, d.h. du kaufst Dienste bzw. Funktionen direkt im Spiel.

- **Abo (Abonnement)**
  Ist ein Vertrag mit der Verpflichtung etwas über einen längeren Zeitraum zu nutzen und dafür zu zahlen.

- **Gewinnspiel**
  Ist die Aufforderung zur Teilnahme an einem Spiel, bei dem ein Preis in Aussicht gestellt wird. Gewinner:innen werden durch Zufall ermittelt, meist via Verlosung.

- **Datenklau**
  Ist das Beschaffen von personenbezogenen oder geheimen Daten, wobei den Datenbesitzer:innen nicht bewusst ist, was weiter mit ihren Daten passiert.

- Oft gibt es Spiele gratis zum Download oder Online-Spielen. Während des Spielens sollst du dann immer wieder neue Funktionen, Superkräfte oder Spielleben dazu kaufen, damit du leichter, schneller oder überhaupt weiterspielen kannst **(In-App-Kauf oder In-Game-Kauf).** Oft wird richtig viel Druck ausgeübt, damit du etwas kaufst! Zeige Spiele immer einer erwachsenen Person, bevor du sie nutzt bzw. herunterlädst! Schau genau auf verführerische Kaufangebote im Spiel!

- **Befristete Gratis-Angebote:** Beispielsweise bietet dir eine App gratis die neuesten und besten Infos zu einem Thema wie deine Lieblingssänger:in – allerdings nur für eine Woche. Danach musst du für die Infos monatlich bezahlen. Besprich Gratis-Angebote aller Art mit deinen Eltern oder einer anderen erwachsenen Vertrauensperson!

- Vorsicht auch bei **gratis Testabos**, die können nach Ablauf einer Frist automatisch in ein kostenpflichtiges Abo übergehen. Besprich Testabos mit einer erwachsenen Person, bevor du eines abschließt. Schau genau auf Fristen und Nutzungsbedingungen!

- Für die **Teilnahme an einem Online-Gewinnspiel** einer Website musst du dich meist durch viele verschiedene unübersichtliche Unterseiten und Eingabefenster durchklicken, Gewinnfragen beantworten und Kontaktdaten angeben. Wenn du schließlich deine Telefonnummer angibst, kann das zu einem versteckten Abo über deine Handyrechnung führen! Schau genau auf das Kleingedruckte! Nimm keinesfalls an Gewinnspielen teil, ohne dich vorher darüber zu informieren! Mach eine Suchmaschinenanfrage (z.B. Google-Suche) zum Gewinnspiel! Was schreiben Andere darüber? Hat jemand womöglich schlechte Erfahrungen damit gemacht? Im Zweifelsfall nimm nicht teil! Rede mit einer erwachsenen Person darüber!

- Oft **bezahlst du einen Dienst oder ein Spiel mit deinen Daten**. Um an der Verlosung zu einem tollen Preis teilzunehmen oder gratis ein Online-Spiel nutzen zu können, musst du Infos über dich, wie dein Alter, deine Adresse und deinen Standort bekannt geben. Die Betreiber:innen des Gewinnspiels oder die Spielehersteller:innen verkaufen diese Daten dann an Werbefirmen und verdienen damit Geld.

Hier kannst du dir Notizen machen

Ich möchte zu diesen Themen mehr erfahren. Auf Seite 53 unter „Internetquellen" finde ich weiterführende Links.

Rechtliches

Einmal im Netz, immer im Netz?

Lilly und Max sitzen im Garten und genießen in der Sonne ein leckeres Eis, Lilly erzählt:

Lilly: Letzten Sommer habe ich ein lustiges Tanzvideo gemeinsam mit meinen Freunden Mia und Mohammed gedreht. Es gab wieder einmal eine Challenge auf TikTok *(=Videoportal/App für Lippensynchronisation von Musikvideos)*. Wir haben unzählige Male neu aufgenommen. Nach einiger Zeit waren wir ganz erschöpft und haben beschlossen, es gut sein zu lassen. Die Videos haben wir mit meinem Handy aufgenommen, weil meine Kamera am besten war. Mia und Mohammed sind heim gegangen und ich habe mir unsere vielen Versuche angeschaut. Sie waren so lustig! Ich habe das beste Video ausgesucht und es gleich auf TikTok hochgeladen.

Lilly: Am nächsten Morgen in der Schule habe ich Mohammed und Mia fragen wollen, ob sie das Video schon gesehen haben. Beide haben sich seltsam verhalten. Der Unterricht hat aber angefangen, deswegen habe ich auf die Pause warten müssen, um nachzufragen.

In der Pause ist Mia sofort aus dem Klassenzimmer gestürmt und auch Mohammed ist nicht gut drauf gewesen.

Lilly: Mohammed, warte! Was ist denn los?

Mohammed: Ach Lilly, wieso hast du das Video einfach hochgeladen, ohne uns zu fragen?

Lilly: Aber ich habe gedacht, das ist ok. Ich habe mir alle Videos angeschaut und das beste hochgeladen. Wir haben schon total viele Likes, hast du gesehen?

Mohammed: Ja, und weißt du auch warum? Alle aus der Schule machen sich darüber lustig! Mia hat da zum Spaß noch das T-Shirt von ihrem Bruder mit dem blöden Spruch angehabt. Ist dir das nicht aufgefallen?

Lilly: Was?? Nein, das tut mir unglaublich leid! Ich hätte euch das Video vorher schicken sollen, um euch zu fragen. Ich werde es sofort wieder löschen.

Mohammed: Jetzt ist es zu spät, Lilly. Meine Cousine aus der Oberstufe hat mir im Unterricht das Video weitergeleitet. Irgendwer hat es schon kopiert und verschickt. Es ist sogar nochmals bearbeitet worden. Wenn Mias Eltern das herausfinden ... Die sind eh so streng, was das betrifft.

Lilly: Oh nein! Was habe ich nur getan? Aber wir müssen doch irgendetwas unternehmen können, oder?

Mohammed: Meine Cousine meinte, wir sollen zu unserem Vertrauenslehrer gehen.

Max: Das ist ja schrecklich! Was ist dann passiert? Hast du dich mit Mia wieder vertragen? Was ist mit dem Video passiert?

Lilly: Das Video ist zwar von TikTok gelöscht worden, aber weil andere es schon heruntergeladen gehabt haben, ist es noch da. Ist einmal etwas im Netz, kann es sehr schwer sein, das dort wieder wegzubekommen. Mia und ich haben uns wieder versöhnt, aber jetzt wissen wir, dass wir das so schnell nicht mehr ohne gegenseitige Zustimmung machen.

Fragen

Hast du schon einmal ungefragt ein Bild oder ein Video von jemandem gemacht?

Wie reagierst du, wenn ein Bild von dir ungefragt im Netz veröffentlicht wird?

Hast du schon mal versucht, ein Bild oder ein Video komplett aus dem Netz zu entfernen?

Wenn ja, wie hast du es gemacht?

Kinder und Jugendliche produzieren Inhalte für ihren Social Media Account und verwenden dafür gerne Musik, Videos oder verschiedene Bilder von anderen Internetseiten, oder sie verwenden Fotos und Bilder von anderen Menschen, ohne diese zu fragen. Ihnen ist oft nicht bewusst, dass sie damit gegen "Das Recht am eigenen Bild" verstoßen. Dabei ist es wichtig, Regeln für ein gutes Miteinander im Netz einzuhalten.

Lade keine fremden Inhalte im eigenen Kanal hoch!

Stichworte

- **Urheber:in**
  Ist Ersteller:in z.B. Fotograf:in, Videofilmer:in, Komponist:in, Autor:in.
- **Urheberrecht**
  Urheber:innen haben als einzige Personen das Recht, ihre Werke der Öffentlichkeit zugänglich zu machen, zu vervielfältigen, zu verbreiten, zu senden, zu verleihen und aufzuführen. Als Werke gelten beispielsweise Fotos, Videos, Musikstücke und Texte.

- Wenn du **Musik, Videos oder Bilder** für deine eigene Seite verwenden willst, die jedoch von anderen Personen gemacht worden sind, brauchst du deren Erlaubnis!
- Auch wenn du Musik für ein Video im Hintergrund verwenden willst, braucht es die Zustimmung der Urheber:innen des Musikstücks.

- Wenn du **Textstellen** (aus dem Internet) für deine eigene Website, ein Posting oder Ähnliches verwenden willst, dann darfst du sie nicht einfach kopieren! Schreibe sie um und/oder gib an, wer die Urheber:innen sind.

Beachte „Das Recht am eigenen Bild"!

Stichworte

- **Das Recht am eigenen Bild**
  Bilder von Personen dürfen nicht der Öffentlichkeit zugänglich gemacht werden, wenn dadurch berechtigte Interessen der:des Abgebildeten oder unter Umständen einer:eines nahen Angehörigen verletzt würden.

- Beachte immer das **Recht am eigenen Bild**! Das Veröffentlichen oder Verschicken von Fotos oder Videos, die andere Personen bloßstellen, ist gesetzlich nicht erlaubt!
- Fotos und Videos von anderen Menschen betreffen immer deren **Eigentum und Privatsphäre**. Überlege: Möchte ich, dass jemand so etwas von mir ohne mein Einverständnis veröffentlicht oder weiterleitet?
- Frag zur Sicherheit immer die Abgebildeten vor dem Posten oder Weiterschicken, ob sie damit einverstanden sind!

Geh respektvoll mit anderen um!

Stichworte

- **Respektvoll sein**
  Das bedeutet andere Menschen freundlich und höflich zu behandeln und Unterschiede zu akzeptieren.

- **Mach nicht mit, wenn eine Person gemobbt wird!** Rede mit einer erwachsenen Person darüber! *Siehe auch die Hackerkarte "Mobbing"*
- Verbreite oder veröffentliche keine Fotos, Videos etc. von anderen Personen ohne deren **Einverständnis**!
- Plaudere nichts **Persönliches** oder intime Dinge über andere aus!
- **Sei höflich!** Sag Bitte und Danke! Vermeide Schimpfworte und Beleidigungen!
- **Trage Unstimmigkeiten oder Streits nicht online aus!** Sprich lieber persönlich mit der anderen Person. Schriftliche Nachrichten werden oft falsch verstanden.

- Gruppenchats machen manchmal Druck! **Du darfst auch nein sagen.** Geh also auch respektvoll mit dir selbst um und nimm dich und deine Gedanken und Gefühle ernst! Mach nicht mit, wenn du nicht magst!
- **Auch außerhalb des Internets ist Respekt gefragt:** Leg dein Smartphone beim Essen weg! Benutze dein Handy bei Treffen mit anderen möglichst wenig! In Bim oder Bus nur leise telefonieren! In öffentlichen Einrichtungen nur im Notfall telefonieren und deine Töne deaktivieren!

Hier kannst du dir Notizen machen

Ich möchte zu diesen Themen mehr erfahren. Auf Seite 53

unter „Internetquellen" finde ich weiterführende Links.

Sichere Zugangsdaten

Im Freibad

Mia und Lilly sind wieder einmal im Freibad, wie fast jeden Tag in den Sommerferien. Es ist ein perfekter Tag! Sie haben Eis gegessen, sind von den Sprungtürmen gesprungen, sind die Rutschen gerutscht und haben sich auf dem warmen Fliesenboden aufgewärmt. Als sie zu ihrem Platz zurückkommen und ihr Eis fotografieren wollten, bemerkt Mia, dass ihr Handy weg ist! Wo ist es nur?

Mia: Ich gebe mein Handy immer in dasselbe Fach in meinem Rucksack. Das ist sehr eigenartig...

Lilly: Vielleicht ist es irgendwo hier unter den Badetüchern?

Sie suchen alles ab, finden es aber nicht. Sie fragen auch die Bademeisterin und den Mann am Einlass. Die Bademeisterin erinnert sich bei der Beschreibung des Handys. Sie meint, sie habe vorhin zwei Mädchen mit so einem Handy beim Volleyballplatz gesehen.

Mia: Lass uns nachsehen, vielleicht sind sie noch da!

Lilly und Mia laufen zum Volleyballplatz, aber es ist niemand da.

Mia: Warum sollte jemand mein Handy klauen?

Mia grübelt vor sich hin als sie wieder zu ihrem Platz zurückgehen. Drei Badetücher weiter liegen Karla und Emily, Mias Nachbarinnen. Sie sind schon zusammen in den Kindergarten gegangen. Die beiden bleiben stehen und grüßen die Nachbarskinder. Da sieht Mia plötzlich das Handy in Karlas Hand. Es kommt ihr sehr bekannt vor.

Mia: Hey! Das ist doch mein Handy! Wieso hast du mein Handy?

Karla: Das ist deins? Ich habe es vorhin bei der Eisdiele liegen gesehen und habe gedacht, ich finde vielleicht heraus wem es gehört, wenn ich die Kontakte durchgehe!

Mia: Ach da habe ich es liegen gelassen, verflixt! Ich habe ja ein Foto für Snapchat damit machen wollen, genau!

Karla: Ich bin gerade dabei gewesen auf dein Instagram-Profil zu gehen, um vielleicht an den Fotos zu erkennen, wem das Handy gehört! Es ist sehr einfach gewesen!

Lilly: Du solltest dein Handy lieber mit einem PIN-Code sichern, Mia! Dann kommt auch niemand an deine Daten und Apps ran!

Karla: Bei Instagram, Snapchat, TikTok, WhatsApp und Co bist du ja ständig eingeloggt, da brauche ich nicht mal ein Passwort eingeben.

Mia ist froh, ihr Handy wieder zu haben! Sie schießen noch ein gemeinsames Selfie mit den Nachbarskindern. Mia richtet sich dann mit Lillys Hilfe gleich einen Sperrcode ein.

Fragen

Hast du so etwas auch schon erlebt?

Wie geht es dir, wenn du diese Geschichte hörst?

Hast du dein Handy mit einem sicheren Code gesperrt?

Was würdest du tun, wenn du ein fremdes Handy findest?

Zum Schutz deiner Privatsphäre oder vor Datenklau sind sichere Passwörter wichtig. Dein Computer, dein Tablet und dein Handy sind deine private Sache! Was du dort tust, geht niemanden etwas an. Daher schütze deine Daten, deine Geräte und deine Privatsphäre!

Schütze dein Passwort!

Stichworte

- **WLAN (Hotspot)**
  "Wireless Local Area Network", ist also ein drahtloses Lokal-Netzwerk. Über dieses Netzwerk kann ohne Kabel im Internet gesurft werden.

- **Phishing**
  Gefälschte Internetseiten, E-Mails oder SMS, verleiten die Internetnutzer:innen dazu, ihre Passwörter oder andere persönliche Daten bekannt zu geben.

- Achtung im **öffentlichen WLAN** bzw. bei öffentlichen Hotspots beispielsweise im Café oder Einkaufszentrum. Gib niemals ein Passwort ein, wenn du über ein öffentliches WLAN einsteigst! Cyberkriminelle könnten das WLAN nutzen, um deine Zugangsdaten auszuspionieren. Besuche im öffentlichen WLAN nur Websites, die HTTPS verwenden z.B. https://www.website.at (das s bei https steht für "secure", also sicher), aber sei auch hier vorsichtig. Mittlerweile können solche Zertifikate gefälscht werden.

- Achtung **Phishing**: Achte auf die Absender-Adresse! Sieht diese merkwürdig aus? Kommt dir der Betreff komisch vor? Auch unpersönliche Anreden ("Sehr geehrter Kunde"), eigenartige Formatierungen oder Formulierungen, Rechtschreib- und Grammatikfehler sowie fremdartige Zeichen, falsch aufgelöste oder gänzlich fehlende Umlaute können auf gefährliche E-Mails hinweisen. Das deutlichste Anzeichen für eine Phishing-Mail ist eine Aufforderung zur Bestätigung oder Aktualisierung von persönlichen Daten. Oft wird mit unangenehmen Folgen gedroht, wenn du die geforderten Daten nicht eingibst (z.B.: "Wenn Sie sich nicht anmelden, muss der Account gesperrt werden!" oder "Wenn Sie Ihr Passwort nicht aktualisieren, gehen wichtige Daten verloren.") Gib niemals einen PIN oder andere wichtige Daten ein! Seriöse Dienstleister:innen versenden niemals E-Mails mit solchen Aufforderungen!

- Wenn du dir nicht alle Passwörter und Zugangsdaten auswendig merken kannst: Bewahre sie nicht direkt neben dem Gerät auf, das du schützen möchtest. Schreibe deine Passwörter auf Zettel und verstecke diese an einem sicheren Ort.

- Deine Passwörter solltest du auch vor Freund:innen geheimhalten!

Verwende einen Nickname!

- Bleib **im Forum oder beim Chat** mit fremden Personen lieber anonym! Verwende einen Spitznamen *(= Nickname)* und gib nicht deinen richtigen Namen, deine Adresse oder Telefonnummer an! Du kannst nie wissen, mit wem du da plauderst und dich austauschst. Oft geben sich Menschen als jemand Anderes aus! Du weißt auch nicht, wer sonst noch mitliest und so an deine privaten Infos kommen könnte.

Bleibe sicher und geschützt!

- **Sichere Passwörter** sind solche, die man nicht erraten kann! Sie sollten am besten aus mindestens 8 Zeichen bestehen – Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen. Nimm zum Beispiel irgendeinen Satz, den du dir gut merken kannst, wie “Wie schützt denn du deine 2 Computer?” und verwende die Anfangsbuchstaben, Ziffern und das Sonderzeichen: “Wsddd2C?” als sicheres Passwort.
- Verwende für jedes Gerät und jeden Zugang **unterschiedliche Passwörter**! Es wäre zwar praktisch nur ein Passwort für alle Accounts zu haben, weil du dir nur eines merken musst, aber das wäre auch gefährlich. Wirst du gehackt, haben die Angreifer:innen Zugriff auf mehrere deiner Accounts.
- Dein Smartphone sollte mit einem **PIN-Code** gesichert sein. So verhinderst du, dass andere Menschen darauf zugreifen können, wenn du es zum Beispiel irgendwo liegen lässt.
- Achte darauf, dass das WLAN zuhause verschlüsselt ist. Besprich das mit deinen Eltern! Eine **verschlüsselte Internetverbindung** verhindert, dass Fremde auf eure Daten zugreifen können.
- Wenn du dich auf einer Internetseite anmeldest **(Login)**, dann melde dich auch wieder ab! Nur wenn du abgemeldet **(Logout)** bist, kann niemand Anderer deinen Zugang nutzen.

Hier kannst du dir Notizen machen

Ich möchte zu diesen Themen mehr erfahren. Auf Seite 53 unter „Internetquellen" finde ich weiterführende Links.

Einstellungen der App

Die Superpower!

Lilly: Vor den Sommerferien habe ich mir ein neues Spiel runtergeladen. Alle haben das in meiner Klasse gehabt! Ich bin nicht wirklich gut darin gewesen und habe besser als Mohammed sein wollen, daher habe ich mir die Superpower (= *zusätzlich erworbene Funktionen)* geholt! Mohammeds Gesichtsausdruck ist unbezahlbar gewesen, als ich ihn im Spiel besiegt habe! Er ist der Beste darin gewesen und hat es nicht fassen können, dass ich nun besser bin!

Zwei Wochen später hat meine Mama mich ins Wohnzimmer gerufen. Sie hat ausgesehen, als hätte ich schon wieder mein Fahrrad mitten in der Einfahrt liegen gelassen.

Lillys Mama: Lilly! Sieh dir mal deine Handyrechnung an! Was ist denn da los, bitte? Hast du mit jemandem aus Australien telefoniert oder warum ist diese so hoch?

Lilly: Wir haben uns die Rechnung gemeinsam angesehen und haben herausgefunden, dass meine Superpower und die Outfits für meine Spielfigur echtes Geld gekostet haben! Ich habe das nicht gewusst und gedacht, dass mir dafür einfach Punkte abgezogen werden. Ich habe einfach mit Mohammed mithalten wollen.

Max: Auweia, das hat sich nicht ausgezahlt. Und was habt ihr dann gemacht?

Lilly: Ich habe zu meiner Mama gesagt, dass ich es selber zahlen werde. Aber sie hat gemeint, dass es nicht meine Schuld gewesen ist, weil nicht sofort erkennbar gewesen ist, dass diese Superpower tatsächliches Geld kostet. Sie hat gesagt, dass auch sie mehr aufpassen hätte müssen und wir uns die Rechnung teilen können. Sie wird mir helfen, die Einstellungen durchzugehen und die Möglichkeit, so einfach etwas übers Handy zu kaufen, abstellen. Aber seitdem passe ich da sehr auf.

Ich habe mich wegen der Sache schlecht gefühlt und es ist mir peinlich gewesen, Mohammed nur durch die Superpower besiegt zu haben. Am nächsten Tag in der Schule habe ich Mohammed die ganze Geschichte erzählt.

Aber, weißt du was, Max?

Max: Was denn?

Lilly: Auch Mohammed hat sich unabsichtlich die Superpower gekauft und ist nur deshalb so gut im Spiel gewesen!

Beide lachen!

Fragen

Was machst du, wenn du so etwas erlebst?

Wen kannst du fragen, wenn du unsicher bist?

Weißt du, wie du am Handy Sachen kaufen kannst?

Kennst du Spiele, bei denen man etwas kaufen kann?

Du bestimmst, wer was von dir im Netz sehen darf! Dafür hast du mehrere Möglichkeiten in den Privatsphäre-Einstellungen der Apps und Plattformen. Denke daran, dass du dich vor Cyber-Kriminalität schützen kannst, wenn persönliche Daten wie Heimatort, Schule oder Urlaubspläne nicht öffentlich einsehbar sind. Überprüfe die Einstellungen immer wieder, da sie sich mit jedem Update ändern können. Eine weitere wichtige App-Einstellung ist das Deaktivieren von In-App-Käufen!

Deaktiviere In-App-Käufe!

Stichworte

- **In-App-Käufe**
  Sind zusätzliche Inhalte, die du in einer App kaufen kannst.

- Achtung **mögliche Kostenfalle**: Viele Apps und Spiele kann man gratis downloaden und nutzen. ABER: Um beim Spielen schneller weiter zu kommen oder um neue Funktionen freizuschalten, bieten viele Spiele In-App-Käufe an.
- Du kannst diese Käufe auf all deinen Geräten (Smartphone, Tablet etc.) **in den Einstellungen deaktivieren**. Lass dir gegebenenfalls von deinen Eltern dabei helfen!
- *Siehe auch "Achte auf versteckte Kosten!"*

Poste keinen Standort!

Stichworte

- **Standort**
  Ort, wo man sich gerade befindet, z.B. eine Stadt oder eine Adresse.
- **Ortungsdienst**
  Anwendungen, die den eigenen Standort oder den des jeweiligen Gerätes anzeigen.

- Fremde im Netz sollten nicht wissen, wo du dich befindest, wo du wohnst oder wo du zur Schule gehst etc. Du kannst **auf allen Geräten einstellen, dass dein Standort nicht einsehbar ist**! Lass dir dabei von den Erwachsenen helfen!
- *Siehe auch "Deine Daten gehören nur dir!"*

Kontrolliere deine Privatsphäre-Einstellungen!

Stichworte

- **Privatsphäre**
  Ist dein eigener, nichtöffentlicher Bereich, der nur dich etwas angeht und den andere Menschen nicht betreten/einsehen dürfen.
- **Privatsphäre-Einstellungen**
  Sind Sicherheitseinstellungen in einer App oder auf einer Social Media Plattform, wo du festlegen kannst, wer was von dir sehen darf.

- Gib keine Informationen über dich öffentlich preis! **Deaktiviere in deinen Apps und auf den Plattformen jede Form von öffentlicher Sichtbarkeit!** Beispiele Instagram oder TikTok: Wenn nur Freund:innen und Bekannte deine Posts sehen sollen, stellst du dein Profil auf „privat". Auf Facebook kannst du für jeden Post festlegen, wer die Zielgruppe sein soll. Dort kannst du auch einen Privatsphäre-Check machen, um zu sehen, ob du deine Informationen wirklich nur mit jenen Personen teilst, mit denen du sie teilen möchtest.

- Denke immer daran, dass Menschen, die du im Internet kennengelernt hast, keine realen Freund:innen sind! Bei **Online-Freund:innen** kannst du nie wissen, wer das in Wirklichkeit ist. Daher solltest du mit dem Weitergeben oder Zeigen von Informationen über dich vorsichtig sein. Zugang zu deinen privaten Inhalten sollten nur deine echten Freund:innen haben!
- **Lege auch fest, wer dich kontaktieren darf!** Fremde sollten keine Möglichkeit haben, dir Nachrichten zu schicken!
- Auf den meisten Plattformen kannst du einstellen, dass ein **Foto von dir oder mit dir erst nach deiner Einwilligung verlinkt** werden kann.
- Lass dir bei den Einstellungen von deinen Eltern oder anderen Vertrauenspersonen helfen!
- *Siehe auch "Gib nicht zu viel von dir preis!"*

Tipp

- **Extra-Tipp:** Schritt-für-Schritt-Anleitungen zu den wichtigsten Privatsphäre-Einstellungen auf den verschiedenen Plattformen findest du auf *saferinternet.at*.

Hier kannst du dir Notizen machen

Ich möchte zu diesen Themen mehr erfahren. Auf Seite 53

unter „Internetquellen" finde ich weiterführende Links.

Ich in der digitalen Welt

Papa muss noch viel lernen!

Lilly und Max sitzen im Park und beobachten die Enten im See. Lilly holt ihr Handy heraus und macht ein Foto von den kleinen Enten.

Max *(lacht)***:** Lilly! Hast du die Enten auch gefragt, ob es okay ist, dass du sie fotografierst?

Lilly *(muss auch lachen)***:** Das würde ich machen wenn sie sprechen könnten, Max! Denkst du, sie haben einen eigenen Facebook-Account?

Max *(kann sich vor Lachen nicht mehr halten)***:**
Ja klar haben sie einen und viele Follower! Sie sind Enten-Stars!

Lilly: Aber zumindest stelle ich es nicht auf Facebook und markiere sie.

Max: Was meinst du?

Lilly: Mein Papa hat ein Foto von mir und meinen Geschwistern auf Facebook gestellt, auf dem wir noch ganz klein waren. Und er hat mich markiert und so hat es meine ganze Klasse gesehen. Eine Mitschülerin hat mich am nächsten Tag darauf angesprochen und sich über mich lustig gemacht, wie ich als kleines Kind ausgesehen habe. Das ist echt fies gewesen und hat mich traurig gemacht.

Max: Wow, das ist echt gemein von ihr gewesen.
Und irgendwie auch blöd von deinem Papa, ohne dein Einverständnis ein Bild von dir und deinen Geschwistern zu posten!

Lilly: Ja, Papa muss noch viel lernen. Auf dem Foto war nämlich auch unser Haus im Hintergrund zu erkennen. Jetzt wissen alle, die das Bild gesehen haben, wo wir wohnen, weil die Straße und auch die Hausnummer zu erkennen sind. Nicht mal das hat ihn aufgehalten! Aber ich habe mit ihm geredet und er wird so etwas nicht mehr tun. Als Versöhnung hat er mir angeboten, dass ich ein doofes Foto von ihm posten darf. Das habe ich dann auch gemacht!

Max *(lacht)***:** Haha

Lilly: Und falls Papa doch wieder einmal darauf vergisst, habe ich meine Einstellungen geändert. Jedes Mal, wenn mich jemand markieren möchte, bekomme ich zuerst eine Nachricht. Ich muss also erst auf "bestätigen" klicken! Zumindest sehen es dann meine Freund:innen nicht!

Max: Du hast dich ja wirklich gut abgesichert!

Fragen

Haben deine Eltern schon einmal ein Foto veröffentlicht, mit dem du nicht einverstanden warst?

Wenn ja, hast du das angesprochen und gesagt, dass du das nicht möchtest?

Das Internet ist ein Ort, in dem wir uns selbst präsentieren, uns mitteilen und mit anderen austauschen können. Das hat viele Vorteile, birgt aber auch Gefahren. Das Internet vergisst nie!

Gib nicht zu viel von dir preis!

Stichworte

- **Selbstdarstellung**
  Die Art und Weise, wie sich eine Person anderen gegenüber darstellt z.B. welche Informationen sie über sich preisgibt und in welcher Form.
- **Sexting**
  Versenden und Austauschen von Nacktaufnahmen über Internet und Smartphone.

- Überlege gut, **welche Inhalte** du über dich postest oder jemandem schickst! Könnten dir Fotos, Videos oder Infos über dich später unangenehm oder peinlich sein? Könnte sie jemand so verwenden, dass es für dich unangenehm wird?
- Überprüfe immer wieder deine **Privatsphäre-Einstellungen** in deinen Sozialen Netzwerken *(siehe auch "Einstellungen der Apps").* Du bestimmst wer was von dir sehen darf!
- Sei vor allem vorsichtig beim Weitergeben von **freizügigem Bildmaterial (Sexting)**! Damit sind erotische Fotos, Videos und Nacktaufnahmen gemeint. Bevor du solche Inhalte von dir versendest, überlege gut, ob du der anderen Person wirklich vertrauen kannst. Bist du dir zu hundert Prozent sicher, dass deine privaten Aufnahmen nicht an Dritte weitergegeben werden? Wenn du solche dennoch verschicken möchtest, dann achte darauf, dass dein Gesicht nicht zu erkennen ist. Achtung: Das Weitergeben von Nacktaufnahmen von Personen unter 18 Jahren ist verboten. Mit der Weitergabe machst du dich strafbar! Auch Fotos in Bademode oder knappen Outfits können problematisch sein. Es gibt Menschen, die solche Aufnahmen im Internet unerlaubt sammeln und für illegale Zwecke missbrauchen!
- **Urlaubsfotos** sind schön und erzielen viele Likes, aber mögliche Einbrecher:innen könnten sich über die Information freuen, dass aktuell niemand zuhause ist. Teile Urlaubsfotos niemals öffentlich, zumindest nicht solange du noch auf Urlaub bist!

Das Internet vergisst nicht!

Stichworte

- **Inhalte ohne Reue, Datenspuren**
  Sind Spuren, die du bei Aktivitäten im Internet hinterlässt.

- **Cookies**
  Sind kleine Dateien, die auf deinem PC oder Handy gespeichert werden, wenn du eine Website besuchst.

- **Nutzer-Profil**
  Sind gespeicherte und zusammengefasste Informationen, die über Cookies gesammelt werden, und anzeigen, wer was wann und wo gesucht, angeklickt und gekauft hat und die somit Werbezwecken dienen.

- Ist eine Information erst einmal weiterverbreitet worden, lässt sie sich kaum noch löschen. Inhalte sind im Internet fast unmöglich zu entfernen! Postings können (zu einem späteren Zeitpunkt) unpassend und peinlich werden. Beispiele sind Partyfotos, auf denen man sichtlich betrunken posiert, private Blödelfotos oder Fotos von peinlichen Situationen, die man einmal witzig fand, aber später eben nur noch peinlich. **Daher veröffentliche keine Bilder, Videos oder Beiträge aller Art, die dir oder auch anderen irgendwann unangenehm sein könnten.** Auch wenn du sie zum Beispiel auf deinem Account löschst, weißt du nicht, wer sie vielleicht schon kopiert hat oder an welcher anderen Stelle der Inhalt wieder auftauchen könnte.

- Mit jedem Klick, jedem Chat, jedem Post und nahezu jeder Aktivität im Internet erzeugen wir **Datenspuren.** Wir hinterlassen Infos über unsere Interessen, unseren Standort, unsere Geräte, unser Kaufverhalten und vieles mehr. Neben unseren Freund:innen und Bekannten (vor allem auf Social Media) können dies auch Konzerne mitverfolgen. Dies tun sie mit Cookies, welche für Werbezwecke (Nutzer-Profile) eingesetzt werden. Suchst du im Internet zum Beispiel nach neuen Fußballschuhen und aktivierst im entsprechenden Online-Shop ein Cookie, bekommst du sehr wahrscheinlich auch auf anderen Internetseiten Werbung für Fußballschuhe zugespielt.

Deine Daten gehören nur dir!

Stichworte

- **Persönliche Daten, Anonymität/anonym bleiben**
  Bedeutet im Netz unerkannt, also nicht identifizierbar zu sein.
  Zum Beispiel spielen oder chatten, ohne deinen Namen anzugeben.

- Deine Adresse, deine Handynummer oder deine E-Mail-Adresse etc. **sind deine persönlichen Daten**! Diese müssen geheim bleiben und dürfen nicht an fremde Personen weitergegeben werden. Gib sie niemals unbedacht an – nicht im Internet, nicht in einer App!

- Meist ist es sicherer, anstatt deines richtigen Namens einen **Spitznamen** oder nur deinen Vornamen anzugeben. Dies gilt vor allem in digitalen Chaträumen oder Foren. *Siehe "Verwende einen Nickname!"*

- Überlege gut, welche **Infos auf Fotos** du postest oder auf anderem Wege weitergibst! Sieht man darauf etwa ein Straßenschild deiner Wohnstraße oder sogar deine Hausnummer? Mache diese Infos unkenntlich oder schneide sie weg, bevor du das Bild veröffentlichst!

Regelmäßige Kontrolle

Woher weißt du wo ich bin?

Lilly und Max holen sich im Supermarkt ein Eis und wollen dann in den Park gehen. Max nimmt ein Erdbeerwassereis und Lilly entscheidet sich diesmal für das große Schokoeis. Die beiden bezahlen an der Kasse.

Max: Hey Lilly, ist das nicht deine kleine Schwester da hinten?

Lilly: Was wo? Ich sehe niemanden. Außerdem hat sie Hausarrest, hängt zu viel am Handy rum und hat daher schon Schimpfer von der Lehrerin bekommen.

Max: Naja, aber sollte sie dann nicht eher rausgehen und was unternehmen? Beim Zuhause-Rumsitzen wird einem ja eher langweilig. Da will man lieber am Handy rumspielen.

Lilly *(lacht)***:** Ja, da hast du wohl recht. So, genug gequatscht. Komm, jetzt gehen wir in den Park!

Lilly läuft los und startet ein Rennen mit Max.

Lilly: Wer zuerst unterm großen Baum sitzt, hat gewonnen!

Lilly: Gewonnen! Wuhuu!

Max: Du bist aber auch früher gestartet. Naja, gratuliere trotzdem!

Die beiden setzen sich hin und beobachten die Enten im See. Lilly holt ihr Handy heraus und macht ein Bild mit Snapchat und versendet es an ihre Freundin Mia.

Lilly: Das gibt es nicht, meine Schwester hat mir einen Snap *(= ein Bild)* geschickt, also ist sie wohl wieder an ihrem Handy. Da hat die Strafe meiner Eltern ja viel gebracht *(Lilly lacht)*.

Max: Da! Schau! Das ist doch deine Schwester!

Lilly: Hä? Ich sehe nichts. Lass mich mal das Foto ansehen, das sie geschickt hat! *(Lilly sucht nach dem Bild)*

Nora *(Lillys Schwester springt plötzlich aus dem Nichts hinter dem großen Baum hervor)***:** Buh! *(Lilly und Max springen beide auf)*

Lilly: Nora? Was tust du hier? Du hast uns zu Tode erschreckt. Woher weißt du überhaupt, wo wir sind?

Nora *(lacht)***:** Schau dir zuerst das Bild an.

Lilly öffnet das Bild. Es ist vom Supermarkt, wo sie vorhin das Eis gekauft haben.

Lilly: Verfolgst du uns etwa? Und woher weißt du überhaupt, wo wir sind?

Nora: Du machst es mir ja nicht allzu schwer. *(Sie öffnet Snapchat und zeigt ihr die Karte. Lillys Figur ist auf der Karte zu erkennen.)*

Lilly: Ich habe nicht einmal gewusst, dass es so etwas gibt. Das stelle ich sofort aus! Warte, wie geht das eigentlich? *(Nora hilft ihrer großen Schwester, ihren Standort zu deaktivieren. Max schaut den beiden zu und deaktiviert auch gleich seinen Standort.)*

Max *(lacht)***:** Du wirst sicher einmal Agentin oder Spionin, Nora! *(Nora lacht.)*

Fragen

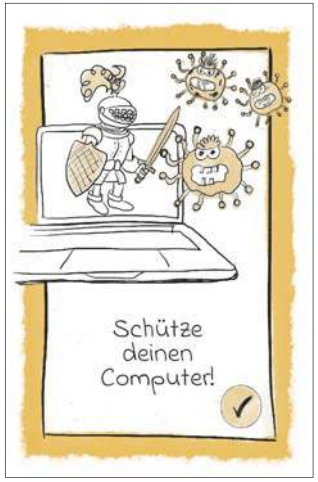
Wie geht es dir, wenn du diese Geschichte hörst?

Welche Erfahrungen hast du damit gemacht?

Hast du so etwas auch schon erlebt?

Was würdest du deinem:r Freund:in raten?

Beim sicheren Nutzen von Handy, Computer und Co. spielt auch der technische Aspekt eine wichtige Rolle. Regelmäßige Updates und Virenschutzprogramme gehören unbedingt dazu.



Schütze deinen Computer!

Stichworte

- **Schadsoftware (Malware)**
  Sind Programme, die sich unbemerkt Zugang zu einem Computer/ Tablet/Handy verschaffen und unerwünschte und/oder schädliche Funktionen ausführen.
- **Computervirus**
  Ist ein sich selbst verbreitendes Computerprogramm, das schadhafte Veränderungen an der Hard- und/oder Software vornehmen kann und zur Malware gehört.

- Werden auf Klick beispielsweise tolle kostenlose Dienste oder Gewinnspiele angeboten, kann es passieren, dass du unabsichtlich und unerkannt **schädliche Software** auf deinem Gerät installierst. Malware dient zum Beispiel dazu, deine Daten auszuspionieren oder dich mit Werbung zuzuspammen. Spammen bedeutet, dass du unaufgefordert Infos (zum Beispiel Werbung) bekommst, die du gar nicht bekommen willst. Manchmal wird die schädliche Software auch zur

Erpressung eingesetzt. So kann es passieren, dass dein PC, Tablet oder Handy über die Malware gesperrt werden und nur gegen Lösegeld wieder entsperrt werden können.

- Gegen Schadsoftware können **Anti-Malware- bzw. Virenschutzprogramme** helfen. Rede darüber mit deinen Eltern!

- Sei bei deinen **E-Mails im Posteingang** vorsichtig! Stammt eine Nachricht von einer unbekannten Person mit eigenartiger Adresse? **Achtung**: Sie könnte einerseits einen gefährlichen Anhang haben wie beispielsweise eine ".exe"-Datei, die auf Klick eine schädliche Software auf deinem Endgerät (PC, Notebook, Tablet, Handy) installiert. Auch andere Anhänge können beim Anklicken Computerviren aktivieren. Oder womöglich wirst du aufgefordert, eine gefährliche Internetseite aufzurufen.

Mache regelmäßig Updates!

Stichworte

- **Update**
  Ist eine Aktualisierung, das heißt Programme oder Inhalte werden auf den neuesten und sichersten Stand gebracht.

- Die Entwickler:innen von Programmen z.B. am Handy oder PC verbessern immer wieder ihre Produkte. Das heißt, sie bringen immer wieder **neue, verbesserte Versionen der Produkte** heraus. Du solltest immer die letzte Version verwenden, da du so auch besser gegen Viren oder Datenklau geschützt bist.

- Besonders wichtig sind die regelmäßigen **Updates bei den Virenschutz-programmen**!

Kontrolliere regelmäßig deine Inhalte!

- Überprüfe immer wieder deine eigenen Kanäle! Sind die **Fotos, Videos und Beiträge passend** oder fühlst du dich beim einen oder anderen nicht ganz sicher? Dann lieber löschen als sich unwohl fühlen!

- Auf manchen Plattformen gibt es die Funktion **„Meine Seite für Andere“ oder Ähnliches** (wie z.B. Facebook: “Anzeigen aus Sicht von”), mit der man sein Profil aus der Perspektive anderer Nutzer:innen überprüfen kann.

- Schau auch **regelmäßig** in den Fotoalben von Freund:innen nach, ob alle Fotos von dir ok sind bzw. ob du überall die Erlaubnis zur Verwendung gegeben hast! Sonst bitte darum, dass das jeweilige Foto gelöscht wird!

- *Siehe auch "Das Recht am eigenen Bild!"*

Hier kannst du dir Notizen machen

Ich möchte zu diesen Themen mehr erfahren. Auf Seite 53 unter „Internetquellen“ finde ich weiterführende Links.

Hacker:innenkarten

Es ist nicht alles, wie es scheint

Lilly: Hätte ich nur selber so schöne Sommersprossen! Und ihre Augen, so blau! Schau Max! Kennst du das Mädchen?

Max: Wow! Das sind aber viele Sommersprossen. Nein, die kenne ich nicht, wie kommst du da drauf?

Lilly: Du hast doch von deiner neuen Nachbarin erzählt, mit der du öfter Fußball spielst. Das ist sie doch, oder? Die heißt genau gleich und hat auch viele Fußball-Stories auf ihrem Account!

Max: Ich bin doch nicht blöd! Ich werde wohl jemanden erkennen, mit dem/der ich fast täglich Fußball spiele! Hmm, sie sieht da total anders aus, das kann ich dir sagen! Und diese Sommersprossen, die sind sicher nicht echt!

Max große Schwester Clara kommt zur Tür herein.

Clara: Hey, ihr hängt in letzter Zeit aber auch immer nur am Handy. Geht doch mal raus, es ist tolles Wetter heute!

Max: Hey Clara! Komm mal her, kennst du das Mädchen? Lilly behauptet, das ist unsere neue Nachbarin, du weißt schon, die mit den guten Fußballtricks!

Clara: Zeig her! Ja, das kommt schon hin, das ist doch ihr Garten da hinten. Aber sie hat definitiv ein paar Filter verwendet. Daher sieht sie aus wie eine völlig andere Person! *(lacht)* Die Sommersprossen stehen ihr aber! Schon arg, wie sehr man sich da verändern kann. Einerseits ist es lustig, sich so anders sehen zu können, aber manchmal ist es echt schon unheimlich, wie sehr du dich mit einem Filter verändern kannst. Viele Mädchen aus meiner Klasse denken, sie sehen dadurch hübscher aus und gefallen den Jungs besser. Blödsinn! Viele machen sich ständig fertig, weil sie in echt nicht so aussehen wie mit den Filtern. Damit sehen alle irgendwie gleich aus – das finde ich ein bisschen gruselig. Dabei sind die Mädchen super, so wie sie in echt sind!

Jetzt kommt sich Lilly irgendwie total blöd vor! Sie ist da voll drauf reingefallen. Aber jetzt versteht sie, dass es auf unterschiedlichen Apps diese Filter gibt, und nicht alles so ist, wie es scheint.

Fragen

Verwenden Personen, denen du folgst, solche Filter?

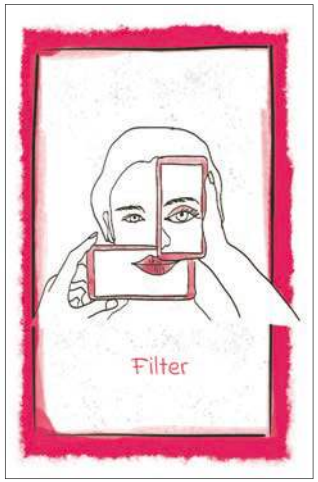
Wenn ja, warum tun die das deiner Meinung nach?

Verwendest du selbst solche Filter?

Wie geht es dir, wenn du diese Geschichte hörst?

Was würdest du deinem:r Freund:in in so einem Fall raten?

Der digitale Raum bietet viele tolle Möglichkeiten, aber es kann auch viel Unerwünschtes passieren! Von technischen Dingen wie Privatsphäre-Einstellungen und Software-Updates bis hin zu Cyber-Mobbing und Inhalten, die du nicht mehr löschen kannst: Um möglichst sicher zu sein, musst du auf viele unterschiedliche Dinge aufpassen.



Filter

Mit Filtern lassen sich Fotos oder auch Videos verändern. Eine spezielle Form ist der Face-Filter (Gesichts-Filter), mit dem sich beispielsweise die Poren verfeinern, das Gesicht aufhellen oder Hautunreinheiten kaschieren lassen. Sprich, man kann sich auf Fotos mit solchen und anderen Schönheitsfiltern vermeintlich “schöner und attraktiver” machen. ABER: Die Realität sieht anders aus! Mit Filtern bearbeitete Fotos vermitteln ein falsches Bild. Denk daran, dass Fotos immer bearbeitet sein können und die Menschen darauf nicht immer so gut ausschauen. Aber das muss ja auch gar nicht sein: Jeder Mensch ist einzigartig und auf seine Weise schön! Auch ohne Filter!

Öffentliches Netzwerk

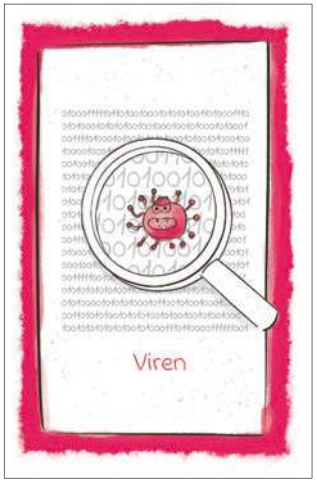
Für Kinder und Jugendliche ist es üblich, sich überall nach einer Internetverbindung /WLAN umzusehen. Die Verbindung zum kostenlosen Internet ist rasch hergestellt, doch damit können sehr einfach unverschlüsselte Daten von unerwünschten Benutzer:innen gelesen werden.

Siehe auch "Pass auf dein Passwort auf!"

Unseriöses Gewinnspiel

Möchtest du an einem Gewinnspiel teilnehmen, ist meist das Ausfüllen von Pflichtfeldern notwendig. Damit gibst du persönliche Daten bekannt! Diese werden für Werbezwecke verwendet und können an Dritte verkauft werden.

Siehe auch "Achte auf versteckte Kosten!"



Viren

Wenn du im Internet surfst, E-Mails empfängst, Online-Spiele spielst oder Dateien tauschst, muss der Computer oder auch jedes andere Gerät vor Viren geschützt werden. Rede mit deinen Eltern darüber! Sie sollten alle deine Geräte mit Virenschutzprogrammen versehen. Wenn du ein solches Programm hast, achte auf regelmäßige Updates! Öffne keine verdächtigen E-Mails!

Siehe auch "Bevor du klickst, denk nach!" und "Schütze deinen Computer!"

Influencer:innen

Schon die Bezeichnung sagt viel aus: „To influence“ bedeutet auf deutsch “beeinflussen”. Influencer:innen erreichen in sozialen Netzwerken sehr viele Menschen und haben ein großes Publikum, die sogenannten Follower:innen. Influencer:innen verdienen ihr Geld oft damit, dass sie bei ihren Fans Werbung für verschiedene Produkte machen. Denke daran, dass es zu deren Job gehört, dich zum Kaufen zu verführen!

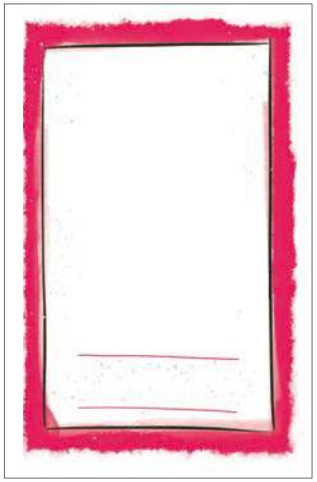
Grooming

Achtung: Wenn Fremde im Internet Kontakt mit Kindern und Jugendlichen aufnehmen, kann es sich um Cyber-Grooming handeln! Das bedeutet, dass sie sehr aufmerksam sind, hilfsbereit tun, Komplimente oder gar Geschenke machen, um sich einzuschmeicheln und Vertrauen aufzubauen. Es kann sich aber um Erwachsene handeln, die böse Absichten haben! Zuerst scheinen sie nett zu sein, aber dann wollen sie beispielsweise Nacktfotos von den Kindern und Jugendlichen! Das ist verboten! Wenn dich jemand anschreibt, den du nicht kennst, rede mit einer erwachsenen Vertrauensperson darüber! In den Privatsphäre-Einstellungen auf Social Media-Plattformen kannst du von vornherein festlegen, wer dich kontaktieren darf.

Siehe auch "Kontrolliere deine Privatsphäre-Einstellungen!"

Mobbing

Cybermobbing hat viele Gesichter: Wenn peinliche Fotos, Videos oder Fotomontagen von anderen Kindern oder Jugendlichen veröffentlicht oder versendet werden, bei Bloßstellungen, Beschimpfungen und Lästereien zum Beispiel in Chatgruppen, wenn Lügen verbreitet werden oder beleidigende Kommentare abgegeben oder böse Nachrichten verschickt werden, dann ist das sehr verletzend für die betroffenen Personen. Sie können dadurch sogar krank werden! Mach nicht mit, auch wenn dich andere zu Mobbing-Aktivitäten anstiften! Egal, ob es dich selbst betrifft oder ob du es bei anderen Kindern und Jugendlichen mitbekommst, behalte es nicht für dich! Sprich mit deinen Eltern, einer:m Lehrer:in oder einer sonstigen Vertrauensperson darüber!



Gestalte deine eigenen Hacker:innenkarten

Worauf möchtest du noch aufpassen?
Im Internet gibt es viele unterschiedliche Möglichkeiten, wie du zu Schaden kommen kannst oder (unbeabsichtigt) anderen Schaden zufügst. Zeichne, was dir besonders wichtig ist, wenn du Online-Angebote nutzt, und gestalte so dein Spiel selbst mit!

Weitere Informationen

Scanne einfach mit deinem Handy den QR-Code und erfahre mehr über die Nutzung digitaler Medien!

Internetquellen

www.saferinternet.at

www.mediamanual.at

www.internet-abc.de

www.klicksafe.de

www.youngdata.de

parents.thorn.org

www.kinderbuero.at

SheepliveCartoons (Oben ohne Pelz):

youtube.com/watch?v=tVY5X1-cbVo

youtube.com/watch?v=NE_iZnLpvps

youtube.com/watch?v=LYj9FpkFXTI

youtube.com/watch?v=wz0TOpMK3UI

youtube.com/watch?v=CMxMAqFxWFo&feature=youtu.be

youtube.com/watch?v=LSVlAZld0Ew&feature=youtu.be

youtube.com/watch?v=tyHQUGym0Cc&feature=youtu.be

youtube.com/watch?v=bo0BpOnPP_0&feature=youtu.be

youtube.com/watch?v=frq3nj81GAM&feature=youtu.be

Literaturverzeichnis

- **Lukas Wagner:** Die Generation digital: Heranwachsen in einer vernetzten Welt. Leykam: Wien 2019
- **Alexander Geyrhofer:** Kindersicher im Internet. Die digitalen Gefahren für unsere Kinder und wie wir sie davor schützen. Edition a: Wien 2019

Stichwortverzeichnis

Seite	
14	Abo (Abonnement)
43	Computervirus
39	Cookies
14	Datenklau
39	Datenspuren
12	Download
9	Falschmeldung (Fake News)
14	Gewinnspiel
51	Grooming
9	Hoax
14	In-Game-Kauf
31	In-App-Kauf
52	Mobbing
39	Nutzer-Profil
32	Ortungsdienst
40	Persönliche Daten, Anonymität
25	Phishing
33	Privatsphäre
33	Privatsphäre-Einstellungen
20	Das Recht am eigenen Bild
21	Respektvoll sein
43	Schadsoftware (Malware)
37	Selbstdarstellung
9	Seriöse Quelle
37	Sexting
32	Standort
43	Update
19	Urheber:in
19	Urheberrecht
14	Versteckte Kosten (In-App-Kauf)
25	WLAN (Hotspot)

Fragen ?

Du hast Anregungen, Fragen oder weitere Spielideen, dann melde dich bei uns:

Verein Kinderbüro® – Die Lobby für Menschen bis 14
Karmeliterplatz 2/3, 8010 Graz
+43 316 90370-180
office@kinderbuero.at
www.kinderbuero.at

Konzept | Grafik | Layout:

Sonja Zechner B.A.
Brunnengasse 9
A-8063 Eggersdorf bei Graz
www.sonjazechner.com

Sonja Zechner
Werbegrafik–Designerin

Herausgeber:

Verein Kinderbüro® – Die Lobby für Menschen bis 14
Karmeliterplatz 2/3
8010 Graz
www.kinderbuero.at

Vertrieb:

Karli Printi GmbH
Kärntner Straße 565
A-8054 Graz
www.karlisshop.at

karlis shop
schreiben zeichnen basteln
www.karlisshop.at

Druck:

Karli Printi GmbH®
Kärntner Straße 565
A-8054 Graz
www.karliprinti.at

Karli Printi
Schule • Business • Shop • Druck

Spielanleitung

Du willst gleich mit dem Spielen loslegen?

Mischt die Medienkompetenzkarten, Hacker:innenkarten und Aktionskarten zusammen und legt sie als einen verdeckten Stapel in eurer Mitte auf den Tisch. Die Karten werden einzeln gezogen. Wer von euch an der Reihe ist, darf sich nach Belieben so viele Karten vom verdeckten Stapel nehmen, wie er:sie möchte. Sie kommen aufgedeckt vor euch. Habt ihr auch eine Hackerkarte gezogen, ist der Spielzug zu Ende und ihr verliert alle Karten, die ihr in diesem Spielzug zu/auf einen offenen Ablagestapel gelegt habt. Danach ist der:die nächste Spieler:in an der Reihe.

Um das Spiel zu gewinnen, hast du viele verschiedene Möglichkeiten. Du kannst die Karten sogar verwenden, um Memory oder Schwarzer Peter zu spielen!

Die genaue Beschreibung der unterschiedlichen Spielvarianten und wie du sie spielst, findest du entweder in der beigelegten Spielanleitung oder digital unter:

Hier findest du den **Link zum Begleitheft** und **zur Spielanleitung**:

www.kinderbuero.at

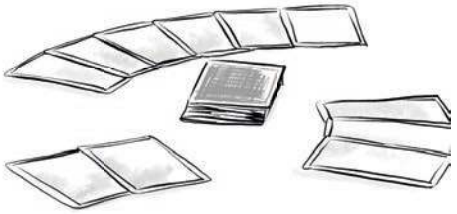
oder
www.karliprinti.at

DigiFit©

Mach dich fit fürs Netz

Spieler:innenanzahl, Alter und Dauer
2 - 6 Internetspezialist:innen
ab 8 Jahren
ca. 20 Minuten

Spielausstattung
60 Medienkompetenzkarten
24 Hacker:innenkarten
16 Aktionskarten
4 Blankokarten
1 Begleitheft
1 Spielanleitung



Spielziel
Sammle Medienkompetenzkarten. Wer als erstes die notwendige Kartenanzahl *(hängt von der Spielvariante ab)* gesammelt hat, gewinnt das Spiel. Doch hüte dich vor den Hacker:innenkarten!

Fazit
Digifit ist ein einfaches und schnelles Kartenspiel für die ganze Familie.
Wie im digitalen Netz musst du bei jeder Aktion überlegen, ob du den nächsten Schritt wagen möchtest und damit das Risiko eingehst, persönliche Daten zu verlieren. Mit jeder abgehobenen Karte steigt die Gefahr, die in der aktuellen Spielrunde gezogenen Medienkompetenzkarten wieder zu verlieren. Im Begleitheft erfährst du (gemeinsam mit Erwachsenen) mehr über die einzelnen Karten und die jeweiligen Gefahren im Netz.

Das Spiel und das Begleitheft sind für dich ein guter Einstieg, um gemeinsam mit deinen Eltern, Pädagog:innen oder Betreuer:innen mehr über Medien und ihre Tücken zu erfahren.