Smartphones souverän nutzen

Wie man im Handy-Dschungel die kontrolle behält

Hintergründe, Fakten und Praxiswissen für Schüler, Eltern und Lehrer

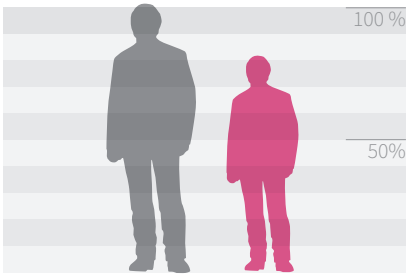
Mit Checklisten und praktischen Tipps für Übungen

MOBILSICHER

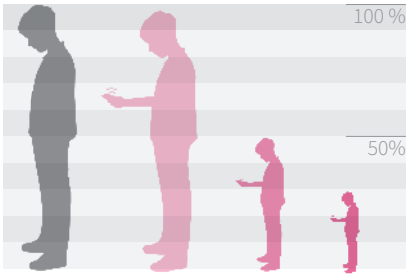
mit Unterstützung von: klicksafe Die EU-Initiative

Grußwort

81 % der Deutschen (ab 14 Jahren) nutzen ein Smartphone (Bitkom 2019).

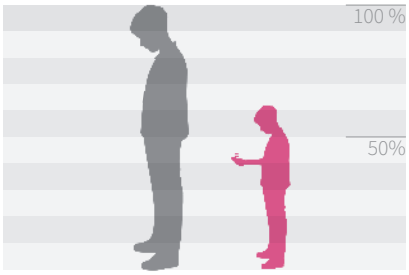


97 % der Jugendlichen zwischen 12 und 19 Jahren haben ein Smartphone (JIM Studie 2018). Bei den 6-bis-13-Jährigen haben **50 %** ein Handy (Smartphone und konventionelles Handy zusammengezählt), **39 %** haben ein Smartphone (KIM Studie 2018)



- alle Jugendlichen
- Jugendliche mit Smartphone (12-19 Jahre)
- Jugendliche mit Handy (6-13 Jahre)
- Jugendliche mit Smartphone (6-13 Jahre)

62 % der 12-bis-19-Jährigen nutzen täglich oder mehrmals pro Woche Video- oder Musikstreamingdienste (JIM-Studie 2018).



- alle Jugendlichen
- Jugendliche Nutzer von Video- oder Musikstreamingdiensten

Liebe Leserinnen, liebe Leser,

ob WhatsApp oder Snapchat, Instagram, YouTube oder Spotify: Smartphones sind aus dem Alltag von Jugendlichen – und zunehmend auch Kindern – nicht wegzudenken. Sie sorgen vor allem für Unterhaltung und Vernetzung mit anderen.

Wer den sinnvollen und verantwortungsvollen Umgang mit ihnen unterstützen möchte, muss aber auch die Risiken kennen: Kinder und Jugendliche kommen mit Hass und Gewalt in Kontakt, werden mit jugendgefährdenden Inhalten konfrontiert oder tappen in Kostenfallen. Auch sind Kinder und Jugendliche einer Unmenge von Werbung und Kaufanreizen ausgesetzt. Oder es geht einfach nur das Gerät verloren – aber der Schaden geht weit über den materiellen Wert hinaus, weil die Fotos und Kontakte verloren sind.

Über die Risiken der Smartphone-Nutzung und ihre Ursachen gibt es viele Missverständnisse. Was sind Anzeichen für eine Smartphonesucht? Wie groß ist die Gefahr, online gemobbt oder verfolgt zu werden? Werden durch irreführendes Design oder psychologische Tricks manipulierende Kauf- und Nutzungsanreize gesetzt? Wie steht es um den Datenschutz?

Umso wichtiger ist es, dass Lehrerinnen und Lehrer, aber vor allem Eltern diese Themen kennen und die Risiken realistisch einzuschätzen wissen. Denn sie sind die Vorbilder, die Kinder und Jugendliche darin stärken können, das Handy souverän zu nutzen.

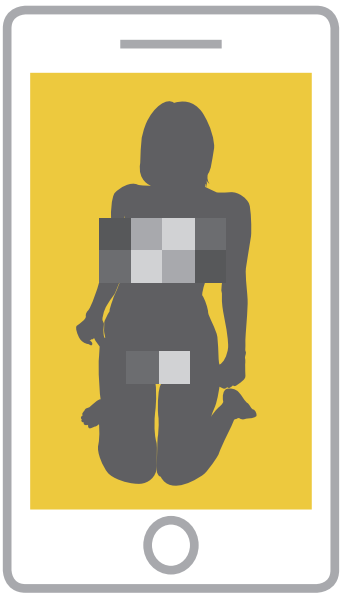
Das Bundesministerium der Justiz und für Verbraucherschutz fördert vor diesem Hintergrund das Projekt mobilsicher.de des Berliner Vereins iRights e.V. in Kooperation mit dem ITUJ e.V.. Das Projekt hat speziell für Lehrerinnen und Lehrer, Eltern und Jugendliche die vorliegende Handreichung erarbeitet.

Es freut mich, dass durch die Unterstützung von klicksafe, der EU-Initiative für mehr Sicherheit im Netz, die Reichweite der Broschüre gesteigert wird und sowohl Multiplikatoren als auch die Nutzerinnen und Nutzer selbst angesprochen werden.

Ich wünsche eine spannende und interessante Lektüre!

Gerd Billen
Staatssekretar im Bundesministerium der Justiz
und für Verbraucherschutz

Inhalt



Handystress und Handysucht

Pornografie und Sexting

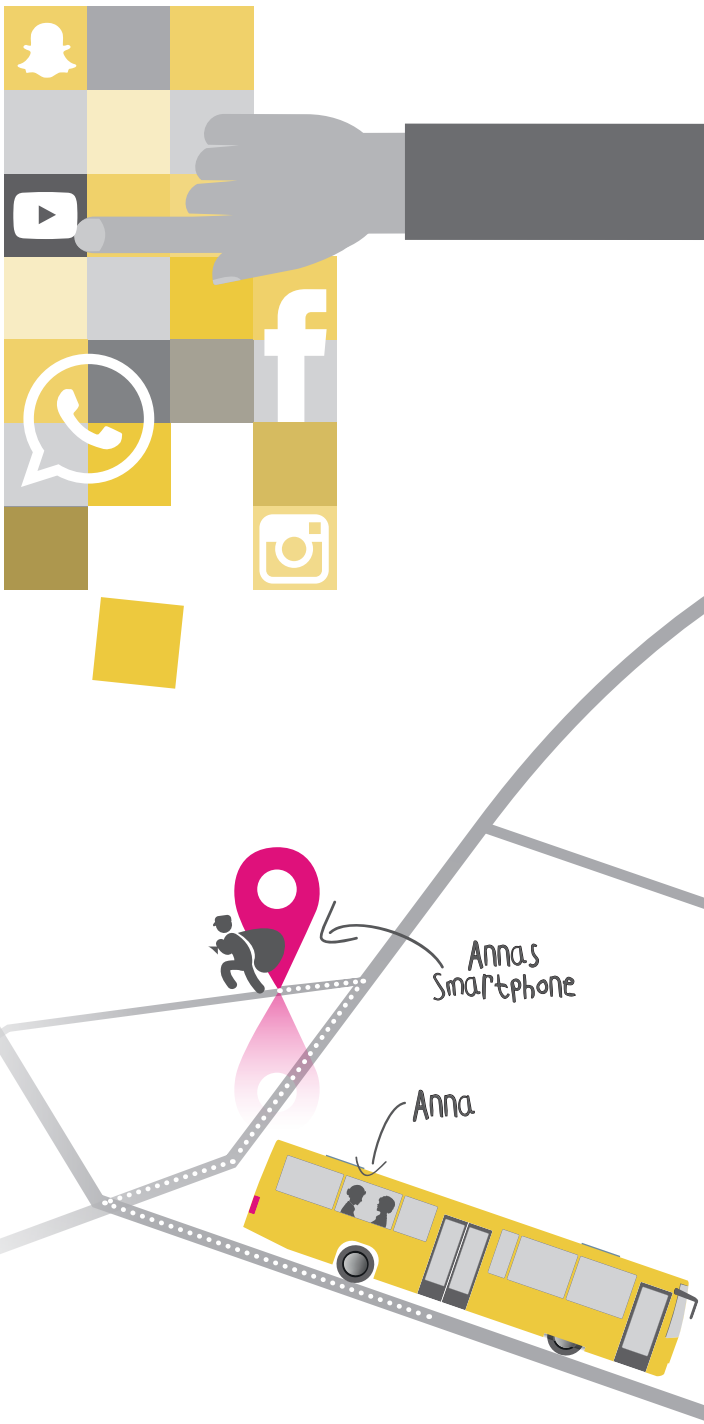
Hass, Gewalt, Volksverhetzung

Alles rund um Apps

Diebstahl und Datensicherheit

Kostenfallen

Zusatzmaterial



Handystress und Handysucht

Viele Jugendliche scheinen förmlich an ihren Handys zu kleben. Sie tragen sie immer bei sich, checken Nachrichten auf WhatsApp oder Instagram im Minutentakt – egal ob in der U-Bahn oder mitten im Gespräch.

Unterhaltung und Kommunikation mit Gleichaltrigen sind wichtige Bedürfnisse von Heranwachsenden. Das Smartphone bietet viele Möglichkeiten, sie zu befriedigen. Das kann jedoch schnell von Genuss in Zerstreutheit, Konzentrationsschwäche und sogar in Sucht umschlagen. Die ständige Sichtbarkeit in sozialen Netzwerken und Messengern kann zu Angst und sozialem Stress führen. So berichten viele Jugendliche von der Angst, etwas zu verpassen oder von den Altersgenoss*innen ausgeschlossen zu werden, wenn sie nicht immer online sind und auf Nachrichten nicht sofort antworten. Für Außenstehende ist es nicht einfach zu erkennen, ob sich das Nutzungsverhalten von Kindern und Jugendlichen noch im normalen Bereich befindet. Kinder und Jugendliche können die Situation selbst oft nicht einschätzen. Haben sie das Handy noch unter Kontrolle? Ab wann wird es zum Stressfaktor? Wie können Eltern und Lehrer*innen Anzeichen von Sucht erkennen?

Gibt es Handysucht überhaupt?

Eine Handysucht in dem Sinne gibt es nicht, da Betroffene nicht nach einem bestimmten Gerät süchtig werden, sondern nach einer Aktivität. Bei Smartphones handelt es sich dabei in der Regel um Aktivitäten, die zum Formenkreis der Internetsucht gehören. Das Wort Internetsucht ist keine klinische Diagnose, sondern ein Sammelbegriff für die suchtartige Nutzung verschiedener Anwendungen, die im Internet stattfinden. Im Groben zeichnen sich dabei die Kategorien ab:

- Spielen (Gaming)
- Soziale Netzwerke, vor allem Facebook
- Kommunikation (Messenger, SMS, Foren)
- Pornokonsum (Videos, Bilder, Cybersex)
- Online-Shopping

Weitere Kategorien könnten dazukommen oder schon vorhandene noch genauer definiert werden. Wenn im Folgenden von Internetsucht die Rede ist, sind alle Unterformen gemeint.

Das klinische Klassifikationssystem DSM wird vom US-amerikanischen Fachverband „American Psychiatric Association“ herausgegeben und gilt auch in Deutschland als Standardwerk für die Diagnose mentaler Erkrankungen. Aktuell ist die 5. Auflage, DSM-5. Darin gibt es erstmals Diagnosekriterien für die „internetbezogene Spielesucht“, also die Kategorie „Gaming“. Auch das klinische Klassifikationssystem ICD der Weltgesundheitsorganisation WHO listet in der 11. Auflage (verabschiedet im Mai 2019) erstmals diese Diagnose auf.

Für andere Internet-Aktivitäten, wie etwa Chatten oder Pornografiekonsum, gibt es noch keine Diagnosekriterien, da hierfür noch Daten fehlen. Fachleute gehen aber davon aus, dass dies noch kommen wird. Bislang werden Betroffene bei diesen Aktivitäten daher mit Hilfsdiagnosen wie „Abnorme Gewohnheiten“ oder „Störung der Impulskontrolle“ erfasst.

Erste Studien zu dem Thema geben Hinweise darauf, dass es einen deutlichen Unterschied zwischen spielebezogenem und nicht spielebezogenem Internetgebrauch

gibt. So sind von spielebezogener Internetsucht überwiegend Jungen und Männer betroffen (Wartberg et al. 2017). Bei den anderen Anwendungen sind Mädchen und Frauen etwas stärker betroffen. Die Betroffenen sind bei der spielebezogenen Internetsucht offenbar stärker in ihrem Alltag beeinträchtigt und landen eher in der Klinik. Die Sucht scheint insgesamt schwerer zu verlaufen.

Wann spricht man von Sucht?

Ab wann man von einer Sucht im medizinischen Sinne spricht, kommt ganz auf die Art des Suchtmittels an. Für die Sucht nach Substanzen, zum Beispiel Alkohol, gibt es schon lange konkrete Kriterien, die für die Diagnose erfüllt sein müssen. Die anerkannten Diagnosekriterien (nach DSM-5) für die internetbezogene Spielesucht sind denen der substanzbezogenen Sucht sehr ähnlich. Danach liegt eine Sucht dann vor, wenn mindestens fünf von diesen neun Kriterien über einen Zeitraum von zwölf Monaten erfüllt sind:

- Gedankliche Vereinnahmung: Betroffene beschäftigen sich in Gedanken ständig mit dem Spiel und haben ein starkes Verlangen danach weiterzuspielen.
- Entzugssymptome: Betroffene sind zum Beispiel nervös oder gereizt, wenn sie nicht spielen können.
- Toleranzentwicklung: Sie müssen immer mehr Zeit mit dem Spiel verbringen, um die gleiche Befriedigung zu erreichen.
- Kontrollverlust: Sie versuchen ohne Erfolg, mit dem Spielen aufzuhören.
- Verhaltensbezogene Einengung: Sie haben keine Lust an anderen Aktivitäten oder Hobbys mehr.
- Nachteile im Alltag: Obwohl sie wissen, dass sich das Spielen negativ auf ihren Job oder die Schule auswirkt, können Betroffene nicht aufhören.
- Täuschen über das wahre Ausmaß der Aktivität: Sie täuschen nahestehende Personen darüber, wie oft und wie lange sie spielen.
- Emotionsregulation: Sie benutzen das Spiel, um negative Gefühle abzubauen oder zu lindern.
- Vernachlässigung wichtiger Lebensbereiche: Sie gefährden oder verlieren wichtige Bekanntschaften, den Beruf, die schulische Karriere.

Wie lange jemand spielt – Stunden oder Tage –, spielt bei der Diagnose nicht die zentrale Rolle. Auf diesen neun Kriterien basieren zwei anerkannte und gut erforschte Messverfahren: CIUS (Compulsive Internet User Scale), ein Fragebogen zum Erfassen von suchtartigem Internetgebrauch insgesamt, und die SMD-Skala (Social Media Disorder Scale) zum Erfassen von suchtartigem Social-Media-Gebrauch.

Sucht: Wer ist gefährdet?

Es gibt verschiedene Merkmale, die bei Personen mit Internetsucht besonders häufig vorkommen. Sie gelten als Risikofaktoren für die Erkrankung:

- impulsive Persönlichkeit
- geringes Selbstwertgefühl
- weniger Gewissenhaftigkeit
- stärkere Empfindung von Einsamkeit und von geringer sozialer Unterstützung
- mehr Misstrauen gegenüber Mitmenschen
- hohe Stressempfindlichkeit
- ungünstige Bindungserfahrung in der frühen Kindheit

Wichtige Warnsignale

Es gibt drei Merkmale, die besonders stark mit einer ausgeprägten Internetsucht verbunden sind. Hierbei sollten Sie aufmerksam werden:

- kein Interesse an anderen Aktivitäten und Hobbys
- Nervosität oder Ängstlichkeit bei Nicht-Nutzung
- Nutzung nimmt in Dauer und Intensität zu

Aufklärung zum Thema Smartphone-Nutzung kann einen bewussten und stressfreien Umgang damit fördern. Als Prävention gegen Internetsucht ist reine Informationsvermittlung aber wirkungslos.

Typische Begleitsymptome

Neben den eigentlichen Diagnosekriterien gibt es auch einige typische Begleitsymptome. Diejenigen, bei denen sich die neun Kriterien erfüllt haben, haben meistens auch:

- mehr Fehltage in Schule oder Job
- schlechtere Schulnoten
- Schlafprobleme
- Weitere psychische Störungen, am häufigsten ADHS (Aufmerksamkeits-/ Hyperaktivitätsstörung), Depressionen, Angststörungen.
- Stärkeres Abhängigkeitsgefühl. Es ist, wenn man einen Verdacht hat, durchaus sinnvoll zu fragen: „Fühlst du dich abhängig?“

Zahlen und Fakten

Eine belastbare Trendabschätzung ermöglicht die Drogenaffinitätsstudie der Bundeszentrale für gesundheitliche Aufklärung BZgA, da hier zwei Messpunkte erhoben wurden, einmal 2011 und einmal 2015.

Darin wurden 5.000 und 7.000 Personen im Alter von 12-25 Jahren deutschlandweit nach ihrer Internet-Nutzung nach CIUS befragt.

Anteil der exzessiven Internetnutzer*innen (mehr als 30 Punkte nach CIUS) 2011

3,3 % der Jugendlichen zwischen 12 und 17 Jahren.

2,1 % der jungen Erwachsenen zwischen 18 und 25 Jahren.

Anteil der exzessiven Internetnutzer*innen (mehr als 30 Punkte nach CIUS) 2015

5,8 % der Jugendlichen zwischen 12 und 17 Jahren.

2,8 % der jungen Erwachsenen zwischen 18 und 25 Jahren.

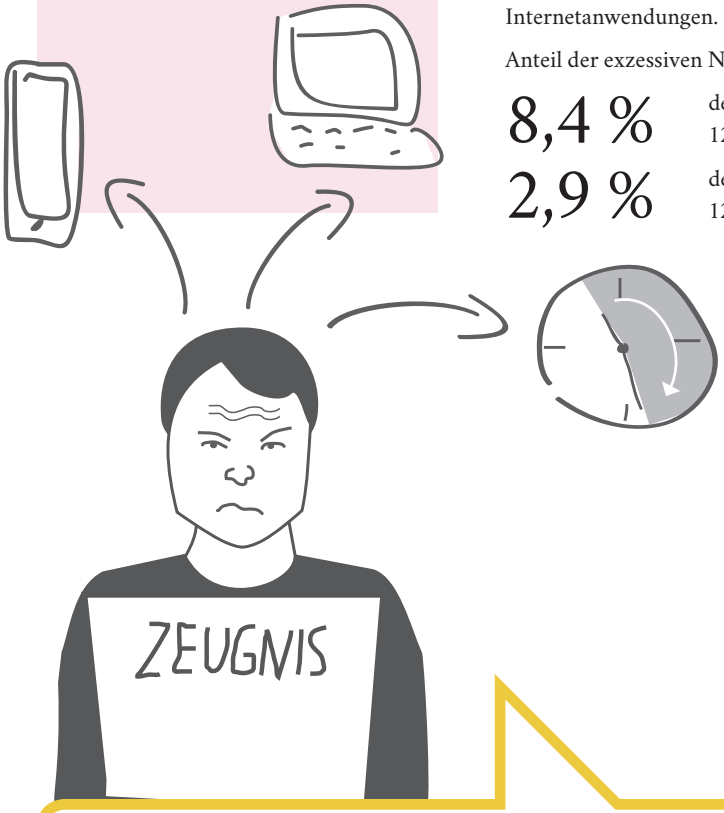
In dieser Studie wurde nicht unterschieden zwischen spielebezogenen Internetanwendungen und anderen Anwendungen. In der Gruppe der 12-17-Jährigen sind Mädchen stärker betroffen, ansonsten ist das Geschlechterverhältnis ausgeglichen.

Eine Studie des Deutschen Zentrums für Suchtfragen des Kindes- und Jugendalters (DZSKJ) von 2016 erfasste ausschließlich die exzessive Nutzung von spielebezogenen Internetanwendungen. Befragt wurden 1.531 Jugendliche von 12-25 Jahren.

Anteil der exzessiven Nutzer*innen von spielebezogenen Internetanwendungen 2016

8,4 % der Jungen/Männer zwischen 12 und 25 Jahren.

2,9 % der Mädchen/Frauen zwischen 12 und 25 Jahren.



Ob jemand internetsüchtig ist oder nicht, lässt sich nicht unbedingt an der Zahl der Stunden festmachen, die er oder sie im Internet verbringt.

Vorbeugen und behandeln

Vorbeugen kann bei den verschiedenen Formen der Internetsucht sehr wirksam sein. Allerdings verwechseln viele Menschen Vorbeuge- und Aufklärungsmaßnahmen.

Wissenschaftlich erprobte Vorbeugemaßnamen setzen an den Risikofaktoren an (siehe Kasten „Sucht: Wer ist gefährdet?“). Bei der Internetsucht trainieren Psycholog*innen mit Betroffenen zum Beispiel, mit negativen Gefühlen besser umzugehen oder die Angst vor Mitmenschen abzubauen. Diese Faktoren kann man mit Methoden aus der kognitiven Verhaltenspsychologie positiv verändern. Die Erfahrung aus anderen Suchtstörungen zeigt, dass reine Aufklärungsmaßnahmen im Sinne von Informationsvermittlung zwar wichtig, aber zur Vorbeugung von Sucht wirkungslos sind.

Mit PROTECT (Professioneller Umgang mit technischen Medien) haben Wissenschaftler*innen der pädagogischen Hochschule erstmals ein Präventionsprogramm gegen Internetsucht für Jugendliche entwickelt, das auf wissenschaftlichen Erkenntnissen beruht. Die Wirksamkeit konnte in einer Studie (2015 bis 2018) nachgewiesen werden. Das Konzept richtet sich an Schulen. Dort sollen besonders gefährdete Jugendliche erkannt und im Vorfeld gestärkt werden. Derzeit bietet die Hopp Foundation kostenlose Fortbildungen für Pädagog*innen an, damit diese das Programm selber an ihren Schulen durchführen können.

Für Betroffene empfehlen Fachleute, professionelle Beratung in Anspruch zu nehmen. Geeignete Anlaufstellen sind zum Beispiel die Suchtberatungsstellen. Auch Erziehungsberatungsstellen und Psycholog*innen können Hilfe leisten.

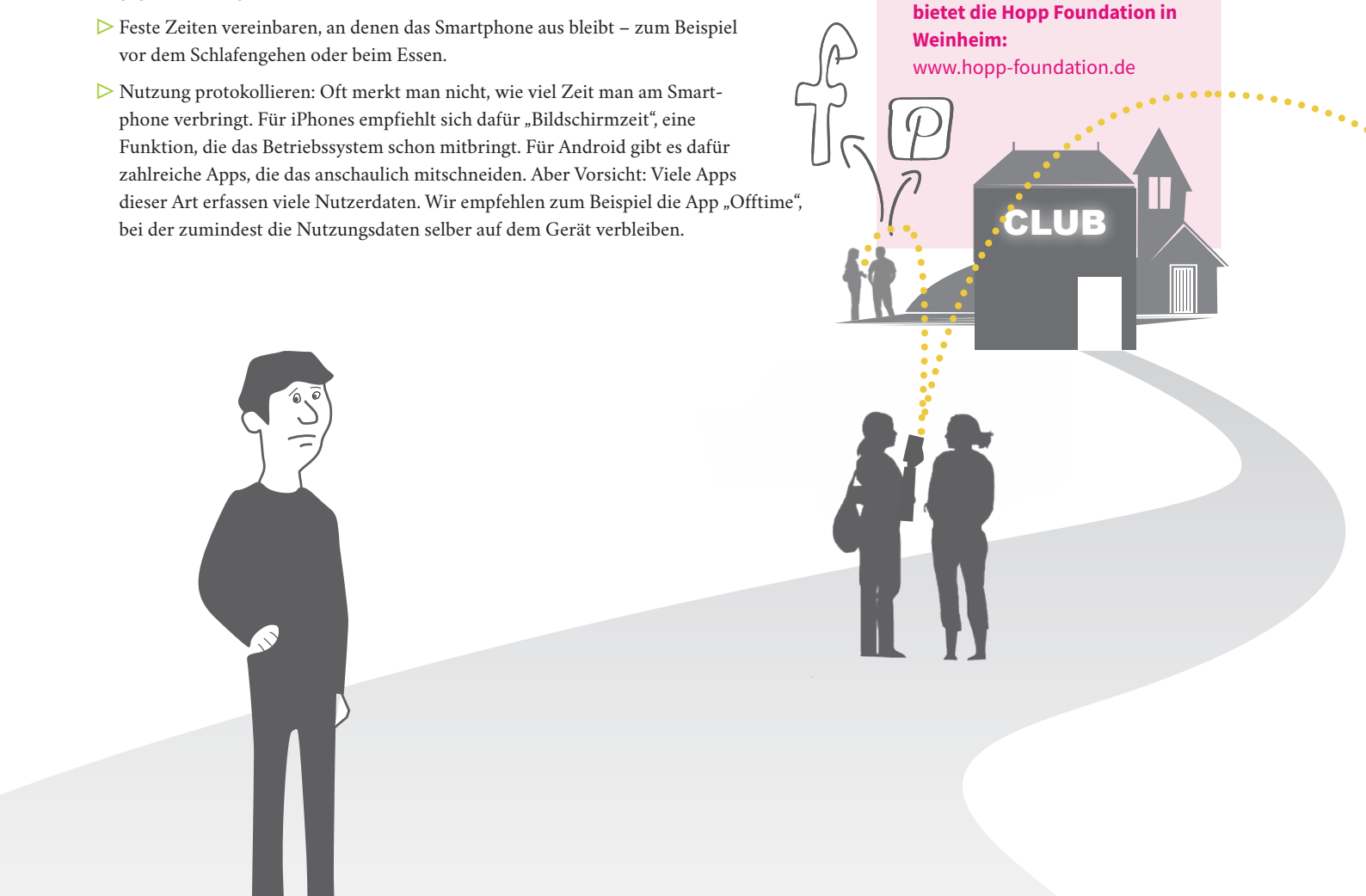
▷ Tipps und Übungen

Die meisten Nutzer*innen werden nicht internetsüchtig. Trotzdem kann es Stress verursachen, wenn man rund um die Uhr mit dem Handy online und erreichbar ist. Dagegen können ganz einfache Maßnahmen helfen:

- ▷ Feste Zeiten vereinbaren, an denen das Smartphone aus bleibt – zum Beispiel vor dem Schlafengehen oder beim Essen.
- ▷ Nutzung protokollieren: Oft merkt man nicht, wie viel Zeit man am Smartphone verbringt. Für iPhones empfiehlt sich dafür „Bildschirmzeit“, eine Funktion, die das Betriebssystem schon mitbringt. Für Android gibt es dafür zahlreiche Apps, die das anschaulich mitschneiden. Aber Vorsicht: Viele Apps dieser Art erfassen viele Nutzerdaten. Wir empfehlen zum Beispiel die App „Offtime“, bei der zumindest die Nutzungsdaten selber auf dem Gerät verbleiben.

Hilfe und Beratung

- **Fachverband Medienabhängigkeit e.V.:** Dort gibt es Informationsmaterial, Referent*innen und eine umfassende Adressliste mit Beratungsangeboten deutschlandweit.
- **OASIS Online Ambulanz-Service für Internetsüchtige:** Vom Bundesministerium für Gesundheit gefördertes Angebot. Bietet einen Online-Fragebogen für den Selbsttest, weiterführende Online-Sprechstunden für Betroffene und Informationen zu Anlaufstellen vor Ort.
- **Ins Netz gehen:** Online-Angebot der Bundeszentrale für gesundheitliche Aufklärung. Online-Selbsttest und -Beratung, Information zu Anlaufstellen vor Ort.
- **PROTECT:** Präventionsprogramm für Schulen.
- **Workshops für Lehrer*innen bietet die Hopp Foundation in Weinheim:** www.hopp-foundation.de



Wichtige Begriffe

Sexting: Eine Kombination aus den Wörtern „Sex“ und „Texting“. Damit ist das Versenden von erotischen Texten und Bildern gemeint – in der Regel an den Partner. Dazu gehören auch erotische Fotos oder Videos von sich selbst, zum Beispiel in Unterwäsche, Nacktbilder bestimmter Körperregionen oder Oben-ohne-Aufnahmen. Besonders beliebt sind dafür die Smartphone-Anwendungen Snapchat und WhatsApp.

Pornografie: Eine allgemeingültige gesetzliche Definition des Begriffes Pornografie gibt es nicht. Der Bundesgerichtshof hat in einer Entscheidung zumindest solche Darstellungen darunter verstanden, die „unter Hintansetzung sonstiger menschlicher Bezüge sexuelle Vorgänge in grob aufdringlicher, anreißerischer Weise in den Vordergrund rücken und ausschließlich oder überwiegend auf die Erregung sexueller Reize abzielen“. Das bedeutet, dass nicht jede Darstellung von nackten Körpern oder sexuellen Handlungen automatisch als Pornografie gilt.

Strafmündigkeit: Jugendliche sind grundsätzlich ab dem 14. Lebensjahr strafmündig. Das bedeutet: Begehen sie Straftaten, können sie für diese vor Gericht verantwortlich gemacht werden. Kinder unter 14 Jahren gelten im deutschen Strafrecht als „schuldunfähig“. Allerdings müssen auch Kinder unter 14 Jahren die Regelungen der Strafgesetze beachten, sie werden nur noch nicht gerichtlich verfolgt.

Jugendstrafrecht: Für Jugendliche (14 bis18 Jahre) gibt es ein spezielles Jugendstrafverfahren. Es ist im Jugendgerichtsgesetz (JGG) geregelt. Sein Kerngedanke ist „Erziehung vor Strafe“. So können Gerichte zum Beispiel für eine Straftat Erziehungsmaßregeln verordnen. Es gibt eigene Anstalten für den Vollzug. Auch Heranwachsende (18- bis unter 21-Jährige) können nach JGG beurteilt werden.

Pornografie und Sexting

Eine Frage, die Eltern und anderen Bezugspersonen oft Sorgen bereitet, ist: Was machen die jungen Nutzer*innen auf dem Smartphone? Welche Inhalte konsumieren sie?

Längst nicht alles, was mit einem internetfähigen Smartphone geteilt, gesehen und gelesen werden kann, ist harmlos. Viele Inhalte können verstören, Angst und Verunsicherung auslösen. Gerade Nutzer*innen im Kindesalter wissen noch nicht, was sie auf YouTube und anderen Plattformen alles erwartet. Auf der anderen Seite sind Jugendliche sehr interessiert an Sex und allem, was dazugehört. Einige Inhalte sind auch schlichtweg illegal. Was genau, das ist manchmal schwer zu beurteilen. Ab wann gilt die Darstellung sexueller Akte als Pornografie? Wann ist nur die Weitergabe strafbar, wann auch schon der Besitz?

Zahlen und Fakten

In Deutschland gibt es nach wie vor wenige Erhebungen zu dem Thema.

Die derzeit aktuellsten belastbaren Zahlen stammen aus einer Studie von 2017. Wissenschaftler*innen der Universitäten Münster und Hohenheim führten eine Onlinebefragung mit 1.048 Jugendlichen im Alter von 14 bis 20 Jahren durch. In der Studie wurden „Pornos“ definiert als Darstellung sexueller Handlungen, bei der entblößte Geschlechtsteile deutlich sichtbar sind. Dadurch sollte eine Abgrenzung von Softpornos erreicht werden.

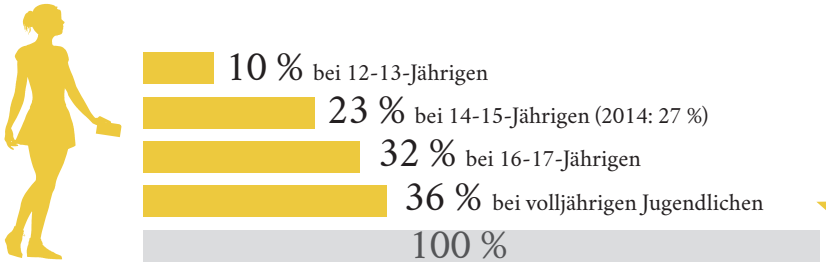
Im Ergebnis zeigen sich deutliche Unterschiede zwischen den Geschlechtern.

Jungen		Mädchen
57 %	geben an, schon mal pornografische Bilder oder Filme gesehen zu haben	37 %
24,5 %	geben an, einmal pro Woche oder häufiger Pornos zu konsumieren	25,5 %
40 %	waren beim ersten Kontakt mit Pornos nicht alleine	42 %
37 %	berichten, dass ihr erster Kontakt mit Pornos ungewollt war	59 %
25 %	haben nach dem ersten Pornokonsum mit einer Person darüber gesprochen	28 %

Das durchschnittliche Alter beim ersten Konsum beträgt 14 Jahre. 28 Prozent der Befragten geben an, Pornos auf dem Handy zu konsumieren, 21 Prozent auf dem Computer. Zeitschriften oder DVDs spielen praktisch keine Rolle mehr.

Die Ergebnisse decken sich mit anderen vergleichbaren Studien. Die wichtigsten Erkenntnisse daraus: Pornokonsum ist kein Randphänomen, sondern gehört zur Lebenswelt der meisten Jugendlichen. Das Bild vom „einsamen, männlichen Pornonutzer" lässt sich nicht halten – Jugendliche konsumieren Pornografie oft in der Gruppe. Erschreckend viele Jugendliche kommen ungewollt mit Pornos in Kontakt. Und: Noch immer wird das Thema tabuisiert – der Großteil der Jugendlichen spricht mit niemandem über das Gesehene.

Neben dem reinen Konsum verschicken Jugendliche sexuell explizite Nachrichten – mit und ohne Bilder (sogenanntes Sexting). Der Medienpädagogische Forschungsverbund Südwest (mpfs) erhebt jährlich in der sogenannten JIM-Studie die Mediennutzung in Deutschland bei Jugendlichen zwischen 12 und 19 Jahren. Dabei werden 1.200 Jugendliche telefonisch befragt. In der JIM-Studie 2015 wurde auch das Thema Sexting abgefragt. 26 Prozent der Befragten gaben an, Sexting im Bekanntenkreis schon einmal mitbekommen zu haben. Dabei gibt es starke Altersunterschiede. Gegenüber 2014 sind die Zahlen vor allem bei den 14-15-Jährigen rückläufig.



Jugendliche verhalten sich in Sachen Sex konservativer als noch vor zehn Jahren.

Rechtliches

Pornografie an Jugendliche zu verbreiten ist verboten

Das Strafgesetzbuch verbietet die „Verbreitung pornographischer Schriften" unter bestimmten Umständen (§ 184 StGB). Mit „Schriften" sind Texte, Bilder und Videos gemeint. Auch Inhalte auf Speicherkarten oder Handys können als „Schrift" gelten. Es ist unter anderem verboten, solche Inhalte Jugendlichen unter 18 Jahren zugänglich zu machen. Nach Ansicht von Jurist*innen fällt darunter zum Beispiel auch, wenn man solches Material auf dem Handybildschirm anderen zeigt. Der bloße Besitz von pornografischen Materialien ist nicht strafbar.

Kinder- und Jugendpornografie: Schon der Besitz ist verboten

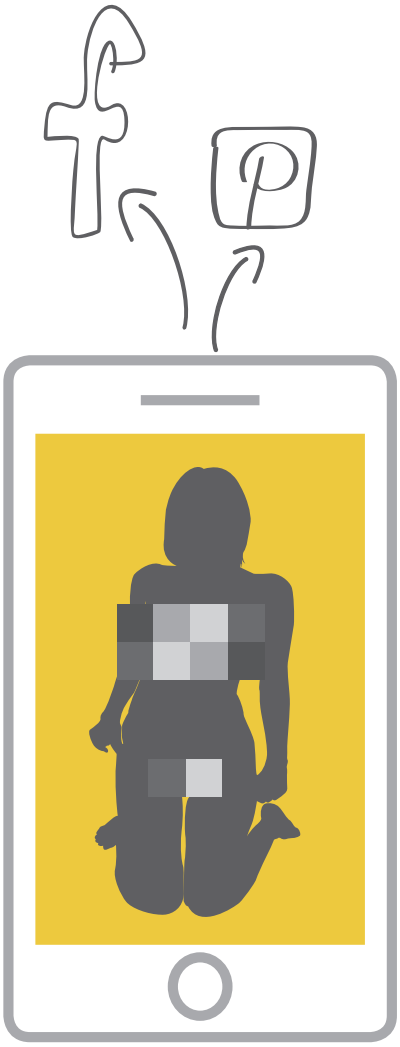
Bei kinderpornografischen Darstellungen ist das anders: In Deutschland sind gemäß Paragraf 184b Strafgesetzbuch Produktion, Verbreitung und auch der Besitz von Kinderpornografie verboten. Auch der Beschaffungsversuch von Kinderpornografie kann strafbar sein. Unter Kinderpornografie versteht man explizite Darstellungen sexueller Handlungen von, an und vor Personen unter 14 Jahren. Seit 2008 gilt dies gemäß Paragraf 184c Strafgesetzbuch auch für Jugendpornografie (pornografische Darstellungen sexueller Handlungen von, an und vor Personen zwischen 14 und 18 Jahren). Jugendliche können sich in extremen Fällen auch strafbar machen, wenn sie pornografische Bilder oder Videos von sich selbst anfertigen. Für sie gilt in diesem Fall das Jugendstrafrecht. Kinder unter 14 Jahren sind hingegen schuldunfähig und werden nicht gerichtlich verfolgt.

Ist Pornokonsum schädlich?

Jugendliche (und sogar Kinder) können über das Internet leicht an Pornos kommen und konsumieren sie auch stark. Zum Teil geschieht dies schon lange, bevor sie selbst sexuell aktiv werden. Viele Erwachsene machen sich Sorgen, dass dadurch realitätsferne Vorstellungen von Sexualität entstehen. Das kann dazu führen, dass Jugendliche verunsichert werden, weil sie weder aussehen wie die Darsteller, noch ihre sexuellen Erfahrungen dem Gesehenen entsprechen. Andere Befürchtungen sind, dass die Jugend

Weitere Informationen

- **Bundeszentrale für gesundheitliche Aufklärung:** Informationen zu Jugendsexualität und Sexualpädagogik
  www.sexualaufklaerung.de
  www.forschung.sexualaufklaerung.de
- Informationen und Materialien für die fächerübergreifende Sexualerziehung
  www.schule.loveline.de
- Selfies, Sexting, Selbstdarstellung, Unterrichtsmaterial der EU-Initiative klicksafe
  www.klicksafe.de



sexuell verrohen könnte oder Wertevorstellungen von Liebe und Bindung verliert. Außerdem transportieren die meisten Pornos ein problematisches Rollenbild, das Frauen als verfügbare Objekte darstellt. Obwohl die Gefahr nicht ganz von der Hand zu weisen ist, deuten Studien darauf hin, dass der Effekt von Pornos auf das Sexualverhalten von Jugendlichen nur schwach ist. Nur etwa fünf Prozent der Verhaltensunterschiede ließen sich bei Probanden durch Pornokonsum erklären (Mathias Weber, 2009).

Relativ eindeutig scheint aber der Zusammenhang von Konsum gewalttätiger Pornografie und aggressivem sexuellen Verhalten zu sein. Zu diesem Ergebnis kommen verschiedene Studien der vergangenen zehn Jahre.

Insgesamt tendieren Jugendliche keineswegs in Richtung sexueller Verwahrlosung. Die Zahlen der Bundeszentrale für gesundheitliche Aufklärung (BzgA) im Bericht „Jugendsexualität“ von 2015 zeigen das Gegenteil. So ist der Anteil der Jugendlichen zwischen 14 und 17 Jahren, die schon einmal Geschlechtsverkehr hatten, seit 2005 rückläufig. 2005 hatten 39 Prozent der Mädchen und 33 Prozent der Jungen in diesem Alter das erste Mal Sex; 2014 waren es 34 Prozent der Mädchen und 28 Prozent der Jungen. Dass Jugendliche früher Sex haben, weil sie Pornos gucken und sexuell „verwahrlosen“, lässt sich also nicht feststellen. Die Befragung zeigt auch, dass Liebe und Treue für Jungen und Mädchen seit 1970 immer wichtiger geworden ist. Sexuelle Erfahrungen finden vornehmlich in festen Beziehungen statt. Die Zahl der Jugendschwangerschaften, die häufig als Zeichen für den Verfall sexueller Werte gesehen wird, hat sich in den letzten Jahren nicht wesentlich verändert. Man kann daraus schließen, dass sich Jugendliche insgesamt also eher konservativer verhalten als noch vor zehn Jahren. Problematisch wird es allerdings, wenn Kinder und Jugendliche unfreiwillig auf Inhalte stoßen, die sie ekeln, erschrecken oder verstören, oder wenn sie in Chats von Pädophilen angesprochen werden. Aus pädagogischer Sicht ist es daher wichtig, Heranwachsende mit den Erfahrungen, die sie im Internet mit sexuellen Inhalten machen, nicht alleine zu lassen, sondern ihnen als kompetenter und unaufgeregter Ansprechpartner zur Seite zu stehen.

Wie gefährlich ist Sexting?

Sexting, also das Verschicken freizügiger Bilder von sich selbst zum Beispiel an den Partner, hat ein sehr negatives Image. Das liegt daran, dass der Begriff selber erst durch die Berichterstattung über einige extreme Fälle in den USA größere Bekanntheit erlangte. Zu nennen wäre hier der Fall der 13-jährigen Hope Witsell, die 2009 Selbstmord beging. Sexting-Bilder von ihr waren in Umlauf geraten und über soziale Netzwerke verbreitet worden. Damit einher ging eine ungeheure Mobbing- und Verleumdungswelle, aus der sie vermutlich keinen Ausweg mehr sah. Auch wegen dieser Erfahrungen haben Medienpädagog*innen lange Zeit empfohlen, Jugendlichen ganz vom Versenden freizügiger oder sexueller Bilder abzuraten. In letzter Zeit gibt es jedoch vermehrt Stimmen, die meinen, dass dadurch dem Opfer fälschlicherweise die Schuld zugewiesen wird. Denn der Umkehrschluss dieser Empfehlung lautet ja: „Wer solche Bilder verschickt, ist selbst schuld.“ Das aber verkennt, dass der eigentlich unmoralische Akt das unerlaubte Verbreiten der Nacktbilder ist. Besonders perfide ist, dass viele Versender*innen sich dabei für moralisch überlegen halten. Anstelle von Sexting-Abstinenz empfiehlt es sich also eher, Jugendlichen den verantwortungsvollen Umgang mit den Bildern anderer Personen zu vermitteln. Einvernehmliches Sexting sollte wie einvernehmlicher Sex

Sexting, also das Verschicken freizügiger Bilder von sich selbst zum Beispiel an den Partner, hat ein sehr negatives Image.

toleriert werden. Dazu gehört, die Heranwachsenden vor sexuellen Übergriffen und Mobbing besser zu schützen und ihnen einvernehmliches Verhalten besser zu vermitteln und vorzuleben.

▷ Tipps und Übungen

Für Eltern: Let's talk about sex

Sexuelle Neugier ist normal. Es ist nicht sinnvoll, sie zu unterdrücken oder zu stigmatisieren. Entscheidend ist, dass Erwachsene den Jugendlichen die Möglichkeit geben, die gesehenen Bilder zu verarbeiten und einzusortieren.

- Wenn Sie annehmen, dass Ihr Kind Pornos anschaut, dann suchen Sie das Gespräch – auch wenn es schwierig ist.
- Sprechen Sie mit Ihrem Partner oder Ihrer Partnerin über das Thema, befragen Sie Freunde und befreundete Eltern.
- Machen Sie sich Ihre eigene Einstellung zu dem Thema bewusst. Ein Gespräch funktioniert besser, wenn Sie wissen, worüber Sie reden.
- Informieren Sie sich. Gehen Sie auf einschlägige Seiten wie redtube.com, youporn.com, xhamster.com – um das zu sehen, was auch die Jugendlichen sehen.
- Sprechen Sie mit Ihrem Sohn oder Ihrer Tochter über die gesetzlichen Regelungen zum Thema.

Für Eltern: Filter nutzen

Für Eltern von Kindern bis etwa 14 Jahre empfiehlt es sich, Filter und technische Einschränkungen zu nutzen. So können Sie zumindest verhindern, dass junge Nutzer*innen ungewollt auf erschreckende Inhalte stoßen.

- Bei der YouTube-App kann man im Menü eine Option wählen, die „Eingeschränkter Modus" heißt. Dadurch werden sexuelle und gewalthaltige Inhalte weitgehend gesperrt. Mit „YouTube Kids" gibt es auch eine Kinderversion der App mit weiteren Einschränkungsmöglichkeiten.
- Es gibt Suchmaschinen für Kinder, die nur für Kinder geeignete Webseiten als Ergebnisse anzeigen – zum Beispiel „FragFINN" oder „Blinde Kuh". Für Smartphones und Tablets gibt es sie als Apps. Bei jüngeren Kindern sollte eine solche App den Browser ersetzen.
- Sie können in der Google-Suche die Funktion „Safe Search" aktivieren. Damit werden anstößige Suchergebnisse herausgefiltert. Öffnen Sie dazu die Google-App, tippen Sie unten rechts auf „Mehr" und dann auf „Einstellungen > Allgemein".
- Speziell für iOS: Hier gibt es mit der Funktion „Bildschirmzeit" seit iOS 12 die Möglichkeit, genaue Zugriffsbeschränkungen für Webseiten einzurichten. Das Menü finden Sie unter „Einstellungen > Bildschirmzeit > (ggf. aktivieren) > Beschränkungen > Inhaltsbeschränkungen > Webinhalt". Sie können einen Jugendschutzfilter wählen oder bestimmte Webseiten manuell sperren oder freigeben.

Für Pädagog*innen: Arbeitsmaterial

Die EU-Initiative klicksafe hat in Kooperation mit Partnern Arbeitsmaterialien für Schule und die außerschulische Jugendarbeit unter dem Titel: "Let's talk about Porno" entwickelt. Bestellung und Download unter:

https://www.klicksafe.de/bestellung/

Filme für Jugendeinrichtungen oder Schule:

- „Geiler Scheiß", ein Film über Jugendliche und Pornografie. © Medienprojekt Wuppertal. (2008, 37 Min, plus 83 Min. Extras), freigegeben ab 12 Jahren.
- „Voll porno, oder was?" ein Film, der auf Informationsmaterial des EU-Projektes klicksafe.de aufbaut. Studio schriftBild, didactimedia (2011, 28 Min.), für Schüler*innen ab der achten Klasse.

Hilfe und Beratung

- Anonyme und kostenlose Beratung durch Mitarbeiter*innen von Pro Familia. Onlineforum zum anonymen Austausch. www.sextra.de
- Onlineangebot der Bundeszentrale für gesundheitliche Aufklärung. Chat rund um Sexualität und Partnerschaft. www.loveline.de
- Das Angebot der „Nummer gegen Kummer" bietet telefonische Beratung für Eltern, Kinder und Jugendliche sowie Online-Beratung für Kinder und Jugendliche. www.nummergegenkummer.de
- Hilfeportal Sexueller Missbrauch: Anlaufstelle für Betroffene von sexualisierten Übergriffen und sexueller Gewalt, Telefonhotline und Datenbank mit Beratungsangeboten und Therapeut*innen bundesweit sowie Informationen zu dem Thema. Vom Unabhängigen Beauftragten für Fragen des sexuellen Kindsmissbrauchs. www.hilfeportal-missbrauch.de.

Für Eltern von Kindern bis etwa 14 Jahre empfiehlt es sich, Filter und technische Einschränkungen zu nutzen.

Hass, Gewalt, Volksverhetzung

„Connecting people“ – dieser Slogan einer Mobilfunkfirma kann für alle Medien stehen. Mit den gleichen technischen Möglichkeiten können aber auch Angst, Hass und Gewalt verbreitet und geschürt werden.

Soziale Netzwerke und Messenger bieten neue Möglichkeiten, Menschen mit Worten oder Bildern bis in ihr Wohnzimmer hinein zu ärgern und zu drangsalieren, ja regelrecht fertigzumachen. Solche Hasskampagnen gegen Einzelne oder Gruppen sind nicht nur eine extreme psychische Belastung für die Betroffenen, sie sind meist auch strafbar.

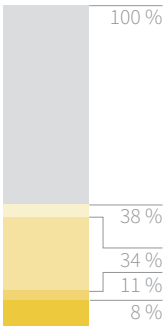
Auch das sogenannte Stalking – hartnäckige Versuche der Kontaktaufnahme oder Verfolgung durch andere (Fremde, aber oft auch ehemalige Partner) – wird einfacher, wenn Menschen jederzeit digital erreichbar sind.

Die Darstellung von Gewalt in Videos scheint für Jugendliche eine große Faszination auszuüben. Dabei reicht die Spannbreite von der Videodokumentation kleinerer Überraschungsangriffe mit einem gewissen Spaßfaktor über ernsthafte Prügel- und Misshandlungsszenen bis hin zu Folter und Hinrichtung von Menschen.

Solche Videos werden aus verschiedenen Gründen unter Jugendlichen weitergereicht: Sei es, um Tabus zu brechen, um cool zu sein, um andere zu schocken oder als Mutprobe. Strafbar ist dabei nicht nur die gefilmte Tat, sondern auch das Aufnehmen und das Verbreiten von solchem Material.

Zahlen und Fakten

Mobbing und unerlaubte Bildweitergabe



11 % der 12-19-Jährigen geben an, dass schon mal peinliche oder gemeine Videos und Bilder von ihnen verbreitet wurden.

34 % der 12-19-Jährigen haben schon einmal erlebt, dass jemand innerhalb des eigenen Bekanntenkreises per Handy oder Internet fertiggemacht wurde (Cybermobbing).

8 % berichten, dass sie schon selber von Cybermobbing betroffen waren.

38 % dder 12-19-Jährigen berichten, dass ihnen häufig oder gelegentlich Hassbotschaften im Internet begegnen.

Quelle: JIM-Studie 2018

Wichtige Begriffe

- **Snuff:** „To snuff out“ heißt im Englischen „jemanden auslöschen“. Mit Snuff werden Videos bezeichnet, die echte oder realitätsnahe Darstellungen von Tötungen enthalten. Sie stammen oft aus Kriegsgebieten und zeigen zum Beispiel Hinrichtungen. Es ist strafbar, solche Videos zu verbreiten.
- **Happy Slapping:** Bedeutet übersetzt in etwa „fröhliches Schlagen“. Gemeint sind damit Angriffe auf Personen, die mit dem Handy gefilmt werden. Wurden zunächst tatsächlich als Scherz erschrockene Gesichter, etwa nach dem Übergießen mit einem Glas Wasser gefilmt, so versucht man sich mittlerweile immer weiter mit abartigen oder brutalen Gewaltaufnahmen zu überbieten. Opfer sind sowohl Fremde als auch bekannte Personen.
- **Cybermobbing:** Das Wort „Mobbing“ kommt aus dem Englischen und bedeutet, „jemanden ärgern, drangsalieren, fertigmachen“. Die Erweiterung „Cyber-“ bedeutet Mobbing mit den Mitteln des Internets, zum Beispiel durch entsprechende Postings oder das Verbreiten demütigender Bilder oder Videos.
- **Cyberstalking:** Das Wort „Stalking“ stammt aus dem Englischen und bedeutet „jemandem nachstellen, verfolgen“. Stalker verfolgen ihre Opfer, betreiben Telefonterror, schicken Briefe, warten an der Wohnungstür oder vor dem Büro auf sie. Die Erweiterung „Cyberstalking“ beschreibt diese Art des Nachstellens im digitalen Raum, per Postings in sozialen Netzwerken, via Messenger, SMS oder Mail. Cyberstalking kommt meist nicht alleine daher, sondern in Verbindung mit herkömmlichem Stalking.

Gewalt und Volksverhetzung

In der Studie „Gewalt im Web 2.0“ von 2008 befragten Forscher*innen der Hochschule der Medien in Stuttgart 804 Jugendliche zwischen 12 und 19 Jahren zum Thema Gewalt im Internet. 25 % der Jugendlichen, die das Internet nutzen, gaben an, schon mal gewalthaltige Inhalte im Internet gesehen zu haben.

50 % davon sahen Prügelvideos mit unbekannten Personen.

42,3 % davon sahen Fotos oder Videos von Folter und Hinrichtungen.

11,9 % davon gaben an, Prügelvideos mit bekannten Personen oder mit sich selbst gesehen zu haben.

38,9 % davon gaben an, schon mal rechtsradikale Inhalte gesehen zu haben.

100 %

Im Jahr 2017 registrierte das Kompetenzzentrum für Jugendschutz im Internet, Jugendschutz.net, 7.513 Verstöße gegen das Jugendschutzgesetz im Internet.

20 % davon kamen aus dem Bereich politischer Extremismus. Gegenüber dem Vorjahr nahm diese Kategorie ab: 2016 waren es noch 38 %. Insgesamt 6 % der Verstöße kamen aus der Kategorie allgemeine Gewalt.

Rechtliches

Gewaltdarstellung

Unter die strafbaren Gewaltdarstellungen fällt laut Paragraf 131 Strafgesetzbuch (StGB) jeder Inhalt, der „grausame oder sonst unmenschliche Gewalttätigkeiten gegen Menschen oder menschenähnliche Wesen in einer Art schildert, die eine Verherrlichung oder Verharmlosung solcher Gewalttätigkeiten ausdrückt oder die das Grausame oder Unmenschliche des Vorgangs in einer die Menschenwürde verletzenden Weise darstellt.“

Verboten ist es unter anderem, solche Darstellungen Minderjährigen anzubieten oder zugänglich zu machen. Dazu gehört auch, dass man sie nicht ins Internet stellen darf. Der bloße Besitz von Gewaltvideos ist nicht strafbar. „Happy Slapping“-Videos etwa können leicht zu diesen verbotenen Gewaltdarstellungen zählen.

Wann genau eine grausame Darstellung im Gesetzessinn verharmlosend oder die Menschenwürde verletzend ist und wann sie unter den Schutz der Kunstfreiheit fällt, hängt vom Einzelfall ab.

Weitere Informationen

- **Hass-im-Netz.info:** Ein Angebot von Jugendschutz.net, mit Meldemöglichkeit und Informationen speziell zu Extremismus und Hass im Netz. www.hass-im-netz.info
- **EU-Initiative Klicksafe:** Das deutsche Awareness Centre der EU hat in Zusammenarbeit mit Jugendschutz.net die Broschüren „Rechtsextremismus hat viele Gesichter“ und „Salafismus online“ herausgegeben, mit vielen konkreten Vorschlägen für Praxisprojekte in Schule und Jugendarbeit. www.klicksafe.de/rechtsextremismus/ www.klicksafe.de/salafismus/
- **Klicksafe:** Mehr Informationen zum Thema Hatespeech. www.klicksafe.de/hate-speech

Hilfe und Beratung

www.nummergegenkummer.de

Das Angebot bietet telefonische Beratung für Eltern, Kinder und Jugendliche sowie Online-Beratung für Kinder und Jugendliche. Experten beraten dort nicht nur zu Problemen mit dem Internet, sondern zu allen Lebensbereichen – Schule, Stress mit den Eltern oder Sexualität.

Unter den Begriff Volksverhetzung fallen laut Paragraf 130 StGB Inhalte, die zum Hass gegen bestimmte Bevölkerungs-gruppen aufrufen.

Volksverhetzung

Unter den Begriff Volksverhetzung fallen laut Paragraf 130 StGB Inhalte, die zum Hass gegen bestimmte Bevölkerungsgruppen – etwa aufgrund ihrer religiösen oder nationalen Zugehörigkeit, ihrer ethnischen Herkunft – oder gegen einzelne Zugehörige dieser Gruppen aufrufen.

Es ist generell verboten, solche Inhalte zugänglich zu machen oder anzubieten.

Absatz 3 und 4 im Paragraf 130 StGB verbietet zudem das öffentliche Leugnen oder Verharmlosen des Völkermordes, der unter der Naziherrschaft begangen wurde, sowie die öffentliche Verherrlichung der nationalsozialistischen Gewalt- und Willkürherrschaft, sofern dadurch der öffentliche Frieden gestört wird.

Unter den Paragrafen fällt vor allem rechtsextremistische Hasspropaganda. Aber auch Hasskommentare auf Facebook und Twitter gegen verschiedenste Gruppen und Personen können darunterfallen. Volksverhetzende Inhalte sind ebenso wie Verleumdung und Beleidigung nicht von der Meinungsfreiheit gedeckt.

Weiterleiten von Bildern

Das Weiterleiten und Veröffentlichen privater Fotos ohne Einwilligung ist in Deutschland verboten. Generell gilt das Recht am eigenen Bild (Paragraf 22 Kunsturhebergesetz), zudem wird seit 2004 eine „Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen“ (Paragraf 201a Strafgesetzbuch) auf Antrag strafrechtlich verfolgt.

Bei einer Veröffentlichung im Internet haben Betroffene Unterlassungsanspruch gegenüber den Betreibern der Webseite (Paragraf 1004 Bürgerliches Gesetzbuch in Verbindung mit den Paragrafen 22 folgende des Kunsturhebergesetzes). Dazu können zivilrechtlich Schadenersatzansprüche geltend gemacht werden. Wird also das eigene Bild ungewollt weitergegeben, kann man sich durchaus erfolgreich wehren.

Bei minderjährigen Opfern muss der Strafantrag jedoch durch die Erziehungs-berechtigten gestellt werden. Dies setzt voraus, dass die betroffenen Jugendlichen sich ihren Eltern anvertrauen können.

▷ Tipps und Übungen

Für Eltern: Filter nutzen

Für Eltern von Kindern bis etwa 14 Jahre empfiehlt es sich, Filter und technische Einschränkungen zu nutzen. So können sie zumindest verhindern, dass junge Nutzer*innen ungewollt auf erschreckende Inhalte stoßen.

- Bei YouTube kann man im Menü eine Option wählen, die „Eingeschränkter Modus“ heißt. Dadurch werden die meisten sexuellen und gewalthaltigen Inhalte nicht angezeigt. Mit „YouTube Kids“ gibt es auch eine Kinderversion der App, mit weiteren Einschränkungsmöglichkeiten.
- Es gibt Suchmaschinen, die nur für Kinder geeignete Webseiten als Ergebnisse anzeigen – zum Beispiel „FragFINN“ oder „Blinde Kuh“. Bei jüngeren Kindern sollte eine solche App den Browser ersetzen. Sie können in der Google-Suche die Funktion „Safe Search“ aktivieren. Das geht in Ihrem Browser oder in der Google-App. Damit werden anstößige Suchergebnisse herausgefiltert.
- Speziell für iOS: Hier gibt es mit der Funktion „Bildschirmzeit“ seit iOS 12 die Möglichkeit, genaue Zugriffsbeschränkungen für Webseiten einzurichten. Das Menü finden Sie unter „Einstellungen > Bildschirmzeit > (ggf. aktivieren) > Beschränkungen > Inhaltsbeschränkungen > Webinhalt“. Sie können einen Jugendschutzfilter wählen oder bestimmte Webseiten manuell sperren oder freigeben.

Sozialkompetenz stärken

Um Mobbing und Cybermobbing zu verhindern, muss vor allem der sozialverträgliche Umgang miteinander gestärkt und geschult werden. Informationen und Materialien für Eltern und Pädagogen gibt es bei der EU-Initiative klicksafe.

- Handbuch „Was tun bei (Cyber)mobbing?“ Systemische Intervention und Prävention in der Schule
- Cyber-Mobbing Erste Hilfe App

Alle Materialien unter:
www.klicksafe.de/themen/kommunizieren/cyber-mobbing/

Rechtslage besprechen

Viele Jugendliche wissen nicht, wann sie sich strafbar machen. Besprechen Sie die Rechtslage in typischen Situationen mit Ihrem Kind oder mit Ihren Schülern.

Bitte petzen!

Bei Suchmaschinen, Videoplattformen und den Betreibern sozialer Netzwerke können Sie rechtsextreme Beiträge, Hassaufrufe, Mobbing oder gewalthaltige Inhalte melden. Die gemeldeten Inhalte werden dann überprüft und gegebenenfalls entfernt. Auch gegen Cybermobbing ist die wirksamste Strategie, einen Erwachsenen einzuschalten.

Wichtig: Sichern Sie Beweismaterial, zum Beispiel mit Screenshots, damit der Vorgang nachvollzogen werden kann.

YouTube: Um ein Video bei YouTube als unangemessen zu melden, müssen Sie ein Nutzerkonto dort haben und angemeldet sein. Um ein Video zu melden, klicken Sie auf die drei Punkte unter oder über dem Video und dann auf das Fähnchen-Symbol.

Facebook: Um eine Gruppe oder ein Einzelprofil bei Facebook als unangemessen zu melden, müssen Sie über ein Nutzerkonto verfügen und eingeloggt sein.

Bei einzelnen Postings: Oben rechts über jedem Post finden Sie drei Punkte. Wenn Sie darauf klicken, öffnet sich ein Menü, in dem Sie „Beitrag melden“ auswählen können. Bevor Sie die Meldung absenden, müssen Sie den Grund angeben, weshalb Sie den Beitrag melden. Sie können auch Gruppen, Profile und Seiten melden.

Man kann anstößige Inhalte auch außerhalb der Plattformen melden. Anlaufstellen sind:

- Die Polizei: Hier kann man Anzeige erstatten, wenn es sich um eine Straftat handelt.
- Jugendschutz.net: Die Institution recherchiert im Internet nach jugendgefährdenden Inhalten und setzt sich gegebenenfalls mit dem Anbieter in Verbindung, um dafür zu sorgen, dass das Angebot aus dem Netz genommen wird. Jugendschutz.net ist organisatorisch an die Kommission für Jugendmedienschutz der Landesmedienanstalten (KJM) angegliedert. Inhalte können per E-Mail an hotline@jugendschutz.net oder per Online-Formular auf www.jugendschutz.net/hotline/ gemeldet werden.
- Internet-Beschwerdestelle: Sie wird vom Industrieverband eco und der Freiwilligen Selbstkontrolle Multimedia-Diensteanbieter e.V. (FSM) betrieben. Beschwerden werden dort juristisch geprüft und Anbieter ggf. zur Löschung aufgefordert. www.internet-beschwerdestelle.de

Viele Jugendliche haben keine Ahnung, wann sie sich strafbar machen.

Wichtige Begriffe

- **Android:** Betriebssystem für mobile Geräte; von Google. In Deutschland läuft auf 79 Prozent aller verkauften Smartphones das Betriebssystem Android (StatCounter, Q2 2019).
- **iOS:** Betriebssystem für mobile Geräte der Firma Apple. Läuft ausschließlich auf iPhones und iPads von Apple. In Deutschland läuft iOS auf etwa 20 Prozent aller verkauften Smartphones. (StatCounter, Q2 2019).
- **IP-Adresse:** Jedes Gerät, das mit dem Internet verbunden ist, hat eine IP-Adresse. Die IP-Adresse gibt ungefähre Auskunft über den Standort – also in welchem Land, ggf. sogar in welcher Stadt man sich befindet. Der Internet-Provider kann der IP-Adresse auch den Inhaber des Internet-Anschlusses zuordnen.

Handy und Apps im Unterricht

- **Unterrichtsreihe „Mobile Medien – Neue Herausforderungen“:** Kurze Unterrichtseinheiten zu den Themen Handynutzung und Herausforderungen bei der Nutzung mobiler Medien, von Klicksafe und Handysektor. www.klicksafe.de/mobilemedien
- **Unterrichtseinheiten „Smartphone & Apps“:** https://www.klicksafe.de/paedagogen-bereich/smartphones-apps-im-unterricht/
- **klicksafe-Infoflyer zu beliebten Apps:** Download & Bestellung unter https://www.klicksafe.de/bestellung/

Alles rund um Apps

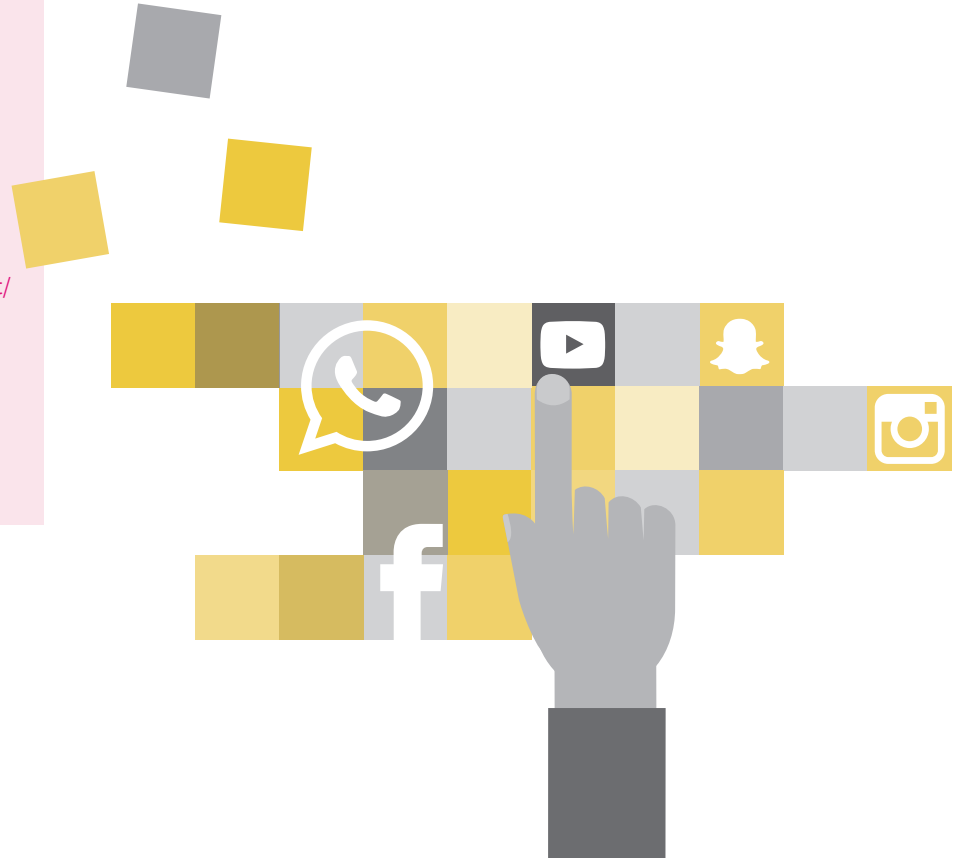
Was für den Desktop- oder Laptop-Computer das Programm ist, mit dem man Musik hören, Texte schreiben oder Fotos bearbeiten kann, das ist für das Smartphone die App. Erst durch Apps werden Mobilgeräte zu den Alleskönnern, die sie heute sind. App steht dabei für das englische Wort „application“, auf Deutsch Anwendung.

Apps gibt es zuhauf, meist kostenlos, in den jeweiligen App-Stores (Play-Store für Android, App-Store für iOS). Das Problem: Fast alle Apps können eine Verbindung ins Internet aufbauen und darüber Daten versenden. Ob sie das tun oder nicht, wann sie sich verbinden und welche Informationen sie verschicken, ist für Nutzer*innen nicht erkennbar.

Die meisten Nutzer*innen wissen in der Regel wenig über die Hersteller ihrer Apps und welches Geschäftsmodell dahintersteht. Nicht selten besteht es leider darin, Nutzerdaten zu sammeln und zu verkaufen.

In der Befragung des Medienpädagogischen Forschungsverbundes Südwest von 2018 (JIM-Studie) sollten die Jugendlichen angeben, welche drei Apps für sie am wichtigsten sind. Dabei landeten fünf Namen mit zweistelligen Prozentzahlen auf den ersten Plätzen. Alle anderen Apps folgten mit Abstand. Diese fünf Apps sind WhatsApp, Instagram, YouTube, Snapchat und Spotify. Die Facebook-App hingegen in dieser Altersgruppe in der Bedeutungslosigkeit verschwunden.

Diese fünf Apps wollen wir hier im Detail vorstellen und erklären, wie sie mit Nutzerdaten umgehen. Wir geben Tipps, wie man die Datenerfassung einschränken kann und nennen Alternativen. Außerdem stellen wir Ihnen zwei Apps vor, die erst seit kurzem die deutschen Kinderzimmer erobern: Die Musikvideo-App TikTok und das Spiel Fortnite sind mit besonderer Vorsicht zu genießen.



Kommunizieren

Die unangefochtene Nummer eins bei Jugendlichen sind Messenger, also Anwendungen, mit denen man Nachrichten und Bilder kostenlos über das Internet verschicken und empfangen kann.

In der JIM-Umfrage von 2018 nannten 87 Prozent der befragten Jugendlichen WhatsApp als eine der drei wichtigsten Apps auf ihrem Smartphone.

Eckdaten WhatsApp

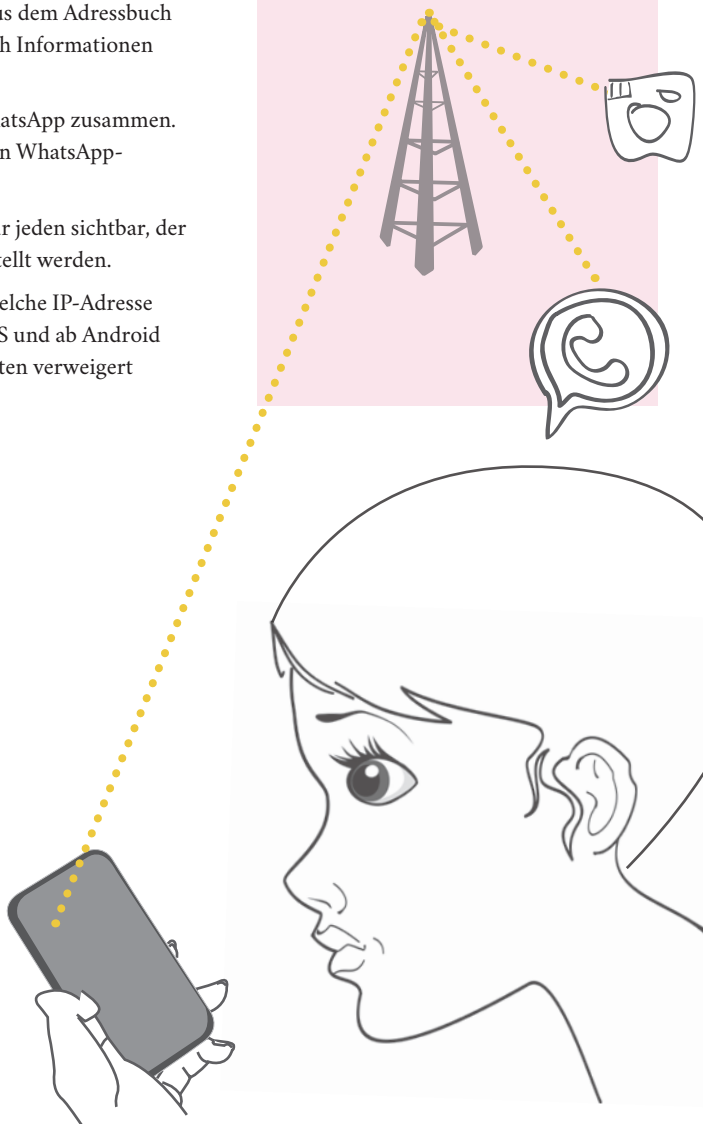
- Der Betreiber und Hersteller WhatsApp Inc. wurde 2014 von Facebook gekauft und gehört seitdem zur Facebook-Gruppe. Firmensitz ist in Kalifornien, USA.
- WhatsApp hatte nach Firmenangaben 2018 weltweit 1,5 Milliarden monatliche Nutzer*innen.
- Seit April 2016 werden alle Nachrichten Ende-zu-Ende verschlüsselt versendet. WhatsApp, beziehungsweise Facebook, kann die Nachrichten selbst nicht entschlüsseln.
- Um mit jemandem zu kommunizieren, muss man dessen Handynummer kennen.
- Die Nutzung ist laut allgemeinen Geschäftsbedingungen erst ab 16 Jahren erlaubt.
- Ab 2020 wird WhatsApp Werbeanzeigen einblenden.

Privatsphäre WhatsApp

- Um den Dienst zu nutzen, muss man sich mit seiner Telefonnummer registrieren.
- Der Betreiber erfasst und speichert Verbindungsdaten: Wer hat wann mit wem kommuniziert.
- Um WhatsApp sinnvoll zu nutzen, müssen alle Telefonnummern aus dem Adressbuch auf WhatsApp-Server geladen werden. Damit erhält WhatsApp auch Informationen über Personen, die den Dienst gar nicht nutzen.
- Seit Mai 2018 führt WhatsApp Nutzerdaten von Facebook und WhatsApp zusammen. Damit erhält Facebook unter anderem auch die Telefonnummer von WhatsApp-Nutzer*innen und verknüpft sie mit dem Facebook-Konto.
- Standardmäßig ist die Information, ob man online ist oder nicht, für jeden sichtbar, der die eigene Telefonnummer kennt. Damit können Nutzerprofile erstellt werden.
- WhatsApp speichert, welches Gerät, welches Betriebssystem und welche IP-Adresse man nutzt und wo man sich befindet. Letzteres kann man unter iOS und ab Android 6.0 verhindern, indem man der App den Zugriff auf die Standortdaten verweigert (siehe Abschnitt: Zugriffsrechte anzeigen und einschränken).

Im Internet surfen: Auch Browser sind Apps

- Viele Nutzer*innen nehmen den Browser, mit dem sie auf dem Smartphone ins Internet gehen, nicht als App wahr. Tatsächlich ist es aber eine, die für Privatsphäre und Sicherheit sehr wichtig ist. Und: Man kann den Browser genauso wie auf dem PC aussuchen und austauschen.
- Der Browser Firefox von Mozilla (für Android) schützt Ihre Privatsphäre besser als die Standard-App Chrome. iOS-Nutzer*innen können den Tracking-Schutz von Firefox Klar in den Safari-Browser einbinden. Wie man Firefox richtig konfiguriert, lesen Sie auf mobilsicher.de unter „Firefox konfigurieren“. Wie Sie den Klar-Browser einbinden, erklären wir im Beitrag „Klar-Browser (iOS)".



WhatsApp verlangt Zugriff auf Kamera, Kontakte, Standort, Mikrofon, Telefon, SMS, Internet.

Tipps für Apps: So kriegen Sie Ihre Apps in den Griff.

- **F-Droid (nur Android):** Apps mit übergriffigen Berechtigungswünschen kann man einfach auch nicht installieren. Fast immer gibt es eine bessere Alternative. Apps, die Ihre Privatsphäre in der Regel respektieren, finden sich zum Beispiel im alternativen App-Store F-Droid. Für iOS-Geräte ist es ohne weitreichende Eingriffe (Jailbreak) nicht möglich, Apps aus alternativen Quellen zu beziehen.
- **AppGuard:** Mit AppGuard der Firma SRT kann man auch auf älteren Android-Versionen die Zugriffsrechte von übergriffigen Apps einschränken.
- **Obscuracam:** App zum Entfernen von Metadaten aus Bildern.
- **Messenger:** Es gibt einige sichere Messenger, die kaum Daten sammeln, zum Beispiel „Wire“, „Signal“ oder „Threema“.
- **Firewall (nur Android):** Fast alle Apps erhalten die Berechtigung, ins Internet zu gehen. Diese kann man ihnen nicht entziehen. Wer einzelnen Apps das Surfen verbieten möchte, ohne die Verbindung gleich ganz zu kappen, kann dies mit einer Firewall tun. Wir empfehlen die Apps „NoRoot Firewall“ oder „NetGuard“.

Details zu den genannten Apps finden Sie bei mobilsicher.de

Bilder teilen

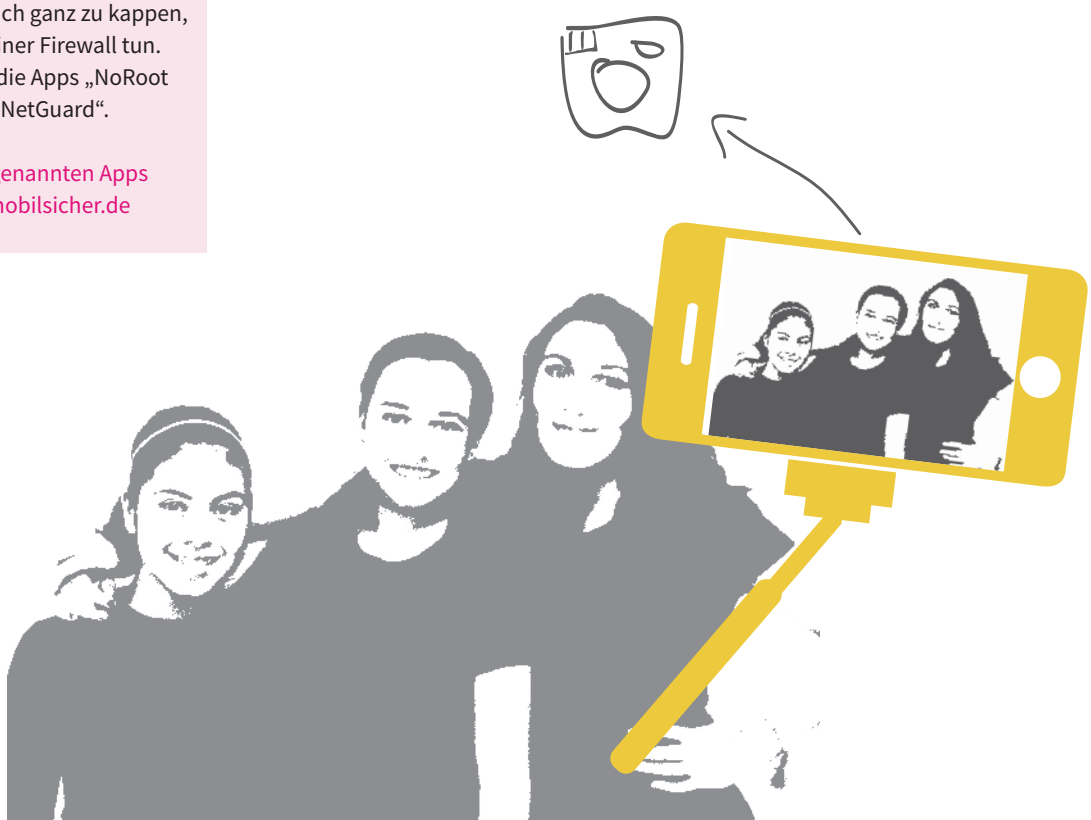
In der JIM-Studie 2018 nannten 48 Prozent der befragten Jugendlichen „Instagram“ als eine der drei wichtigsten Apps auf ihrem Smartphone. Instagram ist ein Dienst, mit dem man Bilder und Videos erstellen, mit Filtern bearbeiten, in seinem eigenen Nutzerkonto veröffentlichen oder mit anderen Nutzer*innen teilen kann. 31 Prozent nannten „Snapchat“, einen Dienst zum Versenden von Bildern.

Eckdaten Instagram

- Betreiber ist die „Instagram LLC“, die seit 2012 im Besitz von Facebook ist. Der Firmensitz befindet sich in Kalifornien, USA.
- Laut Firmenangaben hatte Instagram 2019 weltweit eine Milliarde monatliche Nutzer*innen.
- Nutzer*innen können sich mit E-Mail-Adresse, Facebook-Konto oder Telefonnummer anmelden.
- Laut Geschäftsbedingungen darf Instagram ab 13 Jahren genutzt werden.
- Der Dienst blendet Werbeanzeigen und bezahlte Beiträge ein.

Instagram Privatsphäre

- In der App kann man sein Adressbuch hochladen, um Bekannte zu finden. Instagram nutzt diese Kontaktdaten aber auch für Werbezwecke.
- Verbindungsdaten, IP-Adresse, Geräte-ID, Browser und Gerätetyp sowie Standortdaten werden gespeichert. Letzteres kann man unter iOS und ab Android 6.0 verhindern, indem man der App den Zugriff auf die Standortdaten verweigert (siehe Abschnitt: Zugriffsrechte anzeigen und einschränken).
- Die App teilt Nutzerinformationen mit Unternehmen der Facebook-Gruppe, wo sie mit Daten aus den anderen Facebook-Diensten verknüpft werden.
- Personen auf Bildern können von anderen Nutzer*innen mit Namen versehen werden und sind dadurch leichter auffindbar.



Tipps zur sicheren Nutzung

- Man kann das eigene Instagram-Konto auf „privat“ stellen, die Kommentarmöglichkeiten einschränken und seinen Online-Status verbergen. Dadurch können nur Nutzer*innen Ihre Bilder sehen und kommentieren, die Sie vorher ausgewählt haben und niemand sieht, wann Sie Instagram verwenden.
- Unangemessene Inhalte melden kann man unter „Optionen“ im Hilfebereich der App oder direkt unter dem betreffenden Foto oder Kommentar. Auch anderer Missbrauch, zum Beispiel gefälschte Profile, können dort gemeldet werden.

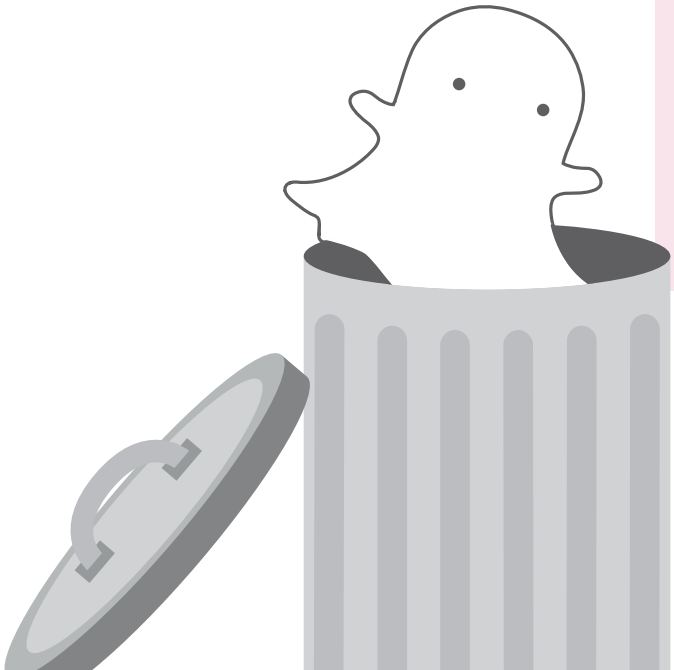
Eckdaten Snapchat

- Betreiber ist Snap Inc., Firmensitz ist in Kalifornien, USA.
- Snapchat hat laut Firmenangaben weltweit 203 Millionen tägliche Nutzer*innen (Stand Q2 2019).
- Snapchat ist ein Dienst, mit dem Bilder und kurze Videos vom Smartphone oder Tablet an andere Nutzer*innen des Dienstes über das Internet verschickt werden können. Es ist keine SIM-Karte nötig. Die Bilder können mit Filtern verfremdet und kommentiert werden. Das Besondere an Snapchat: Die versendeten Bilder werden nach kurzer Zeit wieder gelöscht.

Snapchat Privatsphäre

- Nutzer*innen müssen sich mit Namen und Geburtsdatum registrieren.
- Die App erfasst Gerätetyp, Betriebssystem, Browser, die eigene Telefonnummer, Mobilfunkprovider und Standort. Letzteres kann man unter iOS und ab Android 6.0 verhindern, indem man der App den Zugriff auf die Standortdaten verweigert (siehe Abschnitt: Zugriffsrechte anzeigen und einschränken).
- Sämtliche Nutzungsdaten, also was man wann an wen gepostet hat, welche Bilder man angesehen hat, mit wem man Kontakt hat, werden erfasst und für personalisierte Werbung ausgewertet.
- Speichert alle versendeten Bilder und anderen Inhalte auf seinen Servern, auch wenn sie für Nutzer*innen gleich wieder verschwinden.

Hinweis: Auch wenn die Bilder schon nach Sekunden wieder aus dem Nutzerkonto des Empfängers verschwinden, können sie trotzdem in Umlauf geraten. Denn der Empfänger kann die Bilder durch einen Screenshot speichern, bevor Snapchat sie löscht. Dies kommt auch häufig vor. Man sollte daher auch auf Snapchat nie etwas versenden, von dem man nicht möchte, dass es verbreitet wird.

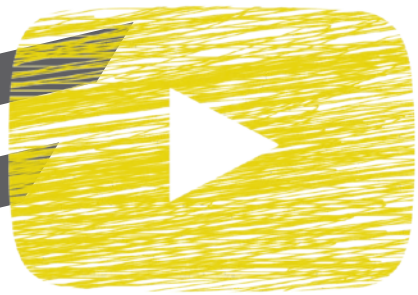


Fehleinschätzung Zugriffsrechte

Selbst wenn man die Berechtigungen einer App vor dem Installieren prüft, bleibt noch die Frage: Was bedeuten diese Rechte eigentlich? Die drei größten Fehleinschätzungen sind:

- **Telefon:** Diese Berechtigung erlaubt einer App nicht nur zu telefonieren. Sie kann damit auch die IMEI, die eigene Telefonnummer, die SIM-Kartennummer und den Mobilfunkprovider auslesen.
- **Daten aus dem Internet empfangen:** Hat nichts damit zu tun, ob die App ins Internet gehen darf oder nicht. Mit dieser Berechtigung können Apps lediglich sogenannte Push-Nachrichten über einen Google-Dienst auf das Gerät senden. Das kann zum Beispiel die Benachrichtigung der Twitter-App sein, dass ein Tweet geteilt wurde, oder von der E-Mail-App, dass eine Mail empfangen wurde.
- **Zugriff auf alle Netzwerke:** Mit dieser Berechtigung können Apps bestehende Internetverbindungen nutzen, um Daten zu versenden und zu empfangen. Ab Android 6.0 wird sie automatisch gewährt und standardmäßig nicht angezeigt. Apps können damit aber auch die sogenannte MAC-Adresse auslesen. Das ist die Identifikationsnummer des eingebauten Netzwerkadapters. Sie ist weltweit eindeutig. Auch damit lässt sich ein Gerät identifizieren.

Wie man Zugriffsrechte anzeigen und verwalten kann, wird bei mobilsicher.de im Detail erklärt.



Videos schauen

Die App des Videoportals YouTube gehört laut JIM-Studie 2018 für 37 Prozent der Befragten zu den drei wichtigsten Apps. YouTube ist ein Video-Portal im Internet. Nutzer*innen können sich dort ein Nutzerkonto anlegen und dann eigene Videos hochladen. Besucher können eingestellte Videos durchsuchen, ansehen und kommentieren. Die YouTube-App ermöglicht einen für Smartphones optimierten Zugriff auf das Portal.

Eckdaten YouTube

- Betreiber ist die YouTube LLC. Geschäftssitz ist in Kalifornien, USA. YouTube wurde 2006 von Google Inc. gekauft. Google ist seit 2015 ein Tochterunternehmen des neu gegründeten Konzerns Alphabet Inc.
- Laut Firmenangaben hat YouTube 1,9 Milliarden registrierte Nutzer*innen pro Monat (Stand Q1 2019).

YouTube Privatsphäre

- Wer die App nutzt, stimmt der Datenschutzerklärung von Google zu, die sehr weitreichende Rechte verlangt: Eingetippte Suchanfragen, angesehene Videos, IP-Adresse und Hardware-Informationen werden an Google gesendet und dort mit Daten aus anderen Google-Diensten verknüpft.
- Android: In der Standard-Einstellung wird der Such- und Wiedergabeverlauf von YouTube im Google-Konto gespeichert und mit anderen Informationen aus dem Konto verknüpft.
- Hinweis: YouTube kann man auch mit dem Browser auf dem Smartphone aufrufen. In diesem Fall speichert der Browser, welche Videos man angesehen hat.

Tipps zur sicheren Nutzung

- Im Google-Konto kann man deaktivieren, dass Google den Suchverlauf und den Wiedergabeverlauf speichert.
- Nutzt man YouTube mit dem Browser, empfiehlt es sich, den Browserverlauf regelmäßig zu löschen.
- Kinder sollten niemals alleine auf YouTube surfen – per Vorschlagsfunktion können sie leicht ungewollt auf unangemessene Inhalte stoßen. Auch der Inhaltefilter der App ist nicht ganz zuverlässig.

Zahlreiche Daten werden gespeichert. Zusätzlich ermitteln eingebaute Sensoren ständig weitere Daten wie Umgebungstemperatur, Höhe oder den Neigungswinkel des Gerätes.

Musik hören

Spotify ist ein Musikstreaming-Dienst, der neben Musik auch Hörbücher, Podcasts und Videos anbietet. Immerhin 10 Prozent der Befragten nannten die App als eine der drei wichtigsten auf dem Smartphone. Spotify kann man mit Werbeunterbrechungen kostenlos nutzen. Premium-Kund*innen erhalten erweiterte Funktionen, wie die Möglichkeit zum Offline-Hören und bessere Musikqualität.

Eckdaten Spotify

- Spotify wird betrieben vom schwedischen Unternehmen Spotify AB. Firmensitz ist Stockholm.
- Laut eigenen Angaben hat Spotify 232 Millionen aktive Nutzer, von denen 108 Millionen zahlende Abonnenten sind (Stand Juli 2019). Das Repertoire umfasst etwa 40 Millionen Songs.

Spotify Privatsphäre

- Spotify fragt bei der Anmeldung nach einer E-Mail-Adresse, Geburtsdatum und Geschlecht.
- Die App erfasst die Geräteversion, die Betriebssystemversion, die Sprache und eine Benutzer-ID.
- Spotify sammelt sämtliche Nutzungsdaten, also welche Lieder man hört, wie lange man sie hört, wonach man sucht, welche Playlists man anlegt usw. Damit werden einerseits die Algorithmen gefüttert, mit denen Spotify passende Musik vorschlägt – andererseits wird passende Werbung geschaltet.

Tipps zur sicheren Nutzung

- Wer seinen Account zunächst mit Facebook anlegt, sich das aber dann anders überlegt, kann diese Verknüpfung im Nachhinein nicht mehr kappen. Wir empfehlen daher, sich mit einer E-Mail-Adresse und Passwort anzumelden. Sie können im Nachhinein Ihren Facebook-Account hinzufügen, wenn Sie Musik mit Freunden teilen wollen. Dann lässt sich die Verbindung auch wieder trennen.
- Standardmäßig ist das Profil und die eigene Höraktivität öffentlich, das heißt, jede*r Spotify-Nutzer*in kann sie sehen. Ändern Sie die Einstellung, wenn Ihre Playlist privat bleiben soll.

10 Prozent der Befragten nannten Spotify als eine der drei wichtigsten Apps auf dem Smartphone.

Neue Apps im Kinderzimmer

TikTok

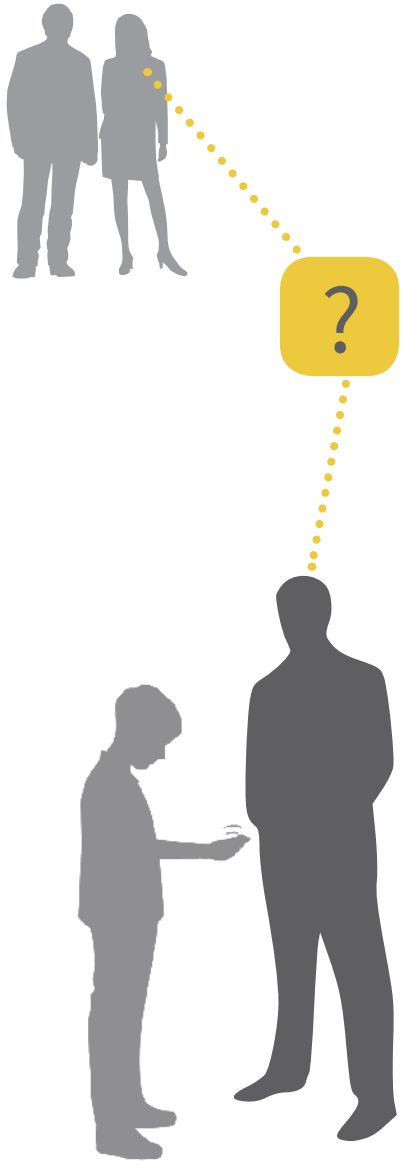
TikTok ist eine Musikvideo-App mit Social-Media-Funktionen. Nutzer*innen können dort Playback- und Karaoke-Videos aufnehmen, die maximal 15 Sekunden lang sind. Es haben sich inzwischen zahlreiche Stars mit mehreren Millionen Anhängern entwickelt.

2018 fusionierte TikTok mit der App Musical.ly, die ähnliche Funktionen bot. Musical.ly – und auch der Nachfolger TikTok – sind in die Kritik geraten, da die App nicht ausreichend gegen pädophilen Missbrauch vorging.

So konnte mobilsicher.de 2018 bei Musical.ly zahlreiche Videos dokumentieren, in denen sich sehr junge Mädchen verstörend aufreizend darstellten. Erwachsene Nutzer spornten diese Mädchen dabei an, noch freizügigere Videos von sich zu posten. Gruppen solcher Nutzer stellten regelrechte Sammlungen dieser Videos zusammen und tauschten sie untereinander.

Oft sind Annäherungsversuche verpackt in überschwängliche Komplimente wie „Du bist so schön, so sexy“ oder mit dem Versprechen, berühmt zu werden, wie „I want to feature you“. Sie werden von jungen Nutzer*innen oft nicht als gefährlich erkannt.

Tun Sie sich mit anderen Eltern oder Freunden zusammen, um der Erfahrung der Jugendlichen möglichst nahe-zukommen.



TikTok (beziehungsweise der Vorläufer Musical.ly) ist schon bei Grundschüler*innen sehr beliebt: Laut Jim-Studie 2018 nutzten bei den 12-13-Jährigen 15 Prozent der Befragten die App mehrmals pro Woche. Bei den 18-19-Jährigen waren es nur 6 Prozent. Offiziell darf man TikTok allerdings erst ab 13 nutzen.

Eckdaten TikTok

- Betreiberin von TikTok ist die chinesische Firma Beijing Bytedance Technology.
- Laut eigenen Angaben hat die App weltweit 130 Millionen Nutzer*innen, die durchschnittlich 39 Minuten am Tag dort verbringen. In Deutschland nutzen 4,1 Millionen die App aktiv (Stand November 2018).
- Nutzer*innen können mit echtem Geld digitale „Geschenke" kaufen und ihren Idolen schicken. Die Beschenkten können diese in echtes Geld eintauschen. Ein Teil des Kaufpreises bleibt dabei bei TikTok.
- TikTok hat derzeit noch kein tragendes Geschäftsmodell – die Einnahmen aus den Geschenken decken nicht die Kosten. In der App wird momentan keine Werbung geschaltet.

TikTok Privatsphäre

- Die App liest laut Nutzungsbedingungen die Telefonnummer, SIM-Karten-Nummer und Geräteinformationen aus. Sie speichert Nutzungsdaten und setzt Tracking-Cookies.
- Diese Daten kann TikTok laut Datenschutzerklärung auch an andere weitergeben, etwa an Geschäftspartner.

Tipps zur sicheren Nutzung

- In der Standardeinstellung sind alle Inhalte, die man hochlädt, öffentlich für alle sichtbar. Das sollte man ändern, sodass nur bestätigte Freunde die Inhalte sehen und kommentieren können.
- In TikTok sind In-App-Käufe möglich – Nutzer*innen können Spezialeffekte für ihre Videos kaufen oder virtuelle Geschenke an ihre Stars schicken. Eltern sollten die Einstellungen für Käufe überprüfen und ihre Kinder auf Kostenfallen aufmerksam machen.
- Erklären Sie Ihrem Kind typische Annäherungsstrategien: Überbordendes Lob, Aufforderungen, noch mehr Haut zu zeigen und Versprechen von Ruhm und Geld sollten Alarmsignale sein.
- Videos, die Sie per Direktnachricht (DM) schicken, können leicht auf anderen Plattformen weiterverbreitet werden und können nicht mehr zurückgeholt werden. Aufforderungen, freizügige Videos per DM zu schicken, sollten ein Alarmsignal sein.
- Dasselbe gilt für die Aufforderung, die Kommunikation auf eine andere App zu verlegen.
- Vereinbaren Sie feste Regeln, welche Videos gepostet werden dürfen. Kinder haben auf TikTok nichts zu suchen. Auch Jugendliche sollten dort nicht unbeaufsichtigt sein.

Fortnite

Fortnite ist ein sogenanntes Koop-Survival-Game für PC, PlayStation 4, Xbox One, Nintendo Switch, Android, iOS und Mac OS. Dabei treten Spieler*innen im Team oder alleine gegeneinander an und müssen Aufgaben erfüllen. Bei der kostenlosen Variante „Fortnite Battle Royal" wird man mit 100 anderen Spieler*innen über einer Insel abgeworfen. Wer am Ende übrigbleibt, hat gewonnen. Im Spiel gibt es einen Sprach- und Text-Chat, in dem sich die Spieler*innen miteinander unterhalten können.

Fortnite ist von der USK (Unterhaltungssoftware Selbstkontrolle) ab 12 Jahren freigegeben. Laut JIM-Studie 2018 ist Fortnite bei 12- bis 17-Jährigen das beliebteste Spiel.

Etliche Experten haben dem Spiel ein besonders hohes Suchtpotential attestiert, darunter die britische Verhaltensforscherin Lorrine Maren. Auch Suchtberatungsstellen vermerken seit 2018 einen spürbaren Anstieg der Patientenzahl im Zusammenhang mit dem Spiel.

Seit April 2018 gibt es „Fortnite Battle Royal" als App für iOS und seit Oktober 2018 für Android.

Eckdaten Fortnite

- Fortnite wurde von Epic Games aus den USA zusammen mit der polnischen Entwicklerfirma People Can Fly entwickelt. Vertrieben wird es von Epic Games gemeinsam mit Gearbox Publishing aus den USA.
- Laut Hersteller waren im März 2019 insgesamt 250 Millionen Spieler registriert, im Monat spielen 78,3 Millionen Menschen das Spiel.

Fortnite Privatsphäre

- Die App fragt nach dem Zugriff auf das Mikrofon für den Gamechat. Viele Gamer benutzen aber dafür ein gesondertes Programm namens Teamspeak, das es auch als mobile App gibt.
- In der Datenschutzerklärung beschreibt Epic Games, welche Daten es erhebt. Bei den mobilen Apps sind dies unter anderem die Geräte-ID, Hardware, Betriebssystem, IP-Adresse und vieles mehr. Daneben sammelt die Firma Nutzungsdaten, die bei der Verwendung des Spiels entstehen und gibt diese gegebenenfalls auch an Dritte weiter.

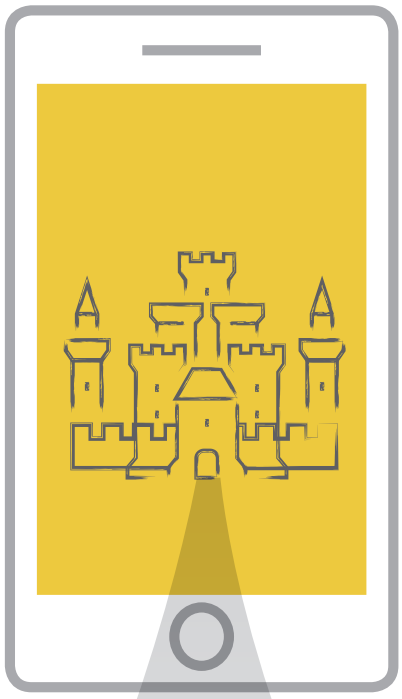
Tipps zur sicheren Nutzung

- Fortnite für Android gibt es nicht im Play-Store. Man kann sich die App beim Hersteller selbst als APK-Datei herunterladen. Dafür muss man vorher in den Einstellungen des Android-Geräts erlauben, dass Apps aus „unbekannten Quellen" installiert werden dürfen. Wichtig ist, danach die Option wieder auszuschalten.
- Bei Fortnite gibt es die Möglichkeit durch In-App-Käufe zusätzliche Ausrüstungsgegenstände oder Kostüme für die eigene Spielfigur zu kaufen. Eltern sollten ihre Kinder darüber aufklären, welche Kosten auf sie zukommen, und Käufe gegebenenfalls mit einem Passwort schützen.
- Daneben kann man in der Fortnite-App selbst die Kindersicherung aktivieren, die es zum Beispiel erlaubt, anstößige Sprache im Chat zu filtern, Freundschaftsanfragen zu blockieren oder die Namen von Nicht-Teammitgliedern herauszufiltern. Außerdem kann man dort auch den Text- und Sprach-Chat steuern.
- Eine Empfehlung vieler Pädagogen ist, dass Eltern Spiele ihrer Kinder selbst spielen sollten, damit sie verstehen, worum es überhaupt geht und wo Stolperfallen liegen. Dadurch können sie besser mit ihren Kindern reden und vermeiden Panikreaktionen.

Hilfe und Beratung

Bei Klicksafe gibt es ausführliche Informationen zu Fortnite für Eltern.
https://www.klicksafe.de/service/aktuelles/news/detail/fortnite-battle-royale-tipps-und-informationen-fuer-eltern/

klicksafe Video: Jugendliche erklären Faszination Fortnite.
https://www.klicksafe.de/service/aktuelles/videoreihe/



Tipps für Apps:

So kriegen Sie Ihre Apps in den Griff.

- F-Droid (nur Android): Apps mit übergriffigen Berechtigungswünschen kann man einfach auch nicht installieren. Fast immer gibt es eine bessere Alternative. Apps, die Ihre Privatsphäre in der Regel respektieren, finden sich zum Beispiel im alternativen App-Store F-Droid. Für iOS-Geräte ist es ohne weitreichende Eingriffe (Jailbreak) nicht möglich, Apps aus alternativen Quellen zu beziehen.
- Exif eraser: App zum Entfernen von Metadaten aus Bildern.
- Messenger: Es gibt einige sichere Messenger, die kaum Daten sammeln, zum Beispiel „Wire“, „Signal“ oder „Threema“.
- Firewall (nur Android): Fast alle Apps erhalten die Berechtigung, ins Internet zu gehen. Diese kann man ihnen nicht entziehen. Wer einzelnen Apps das Surfen verbieten möchte, ohne die Verbindung gleich ganz zu kappen, kann dies mit einer Firewall tun. Wir empfehlen die Apps „NoRoot Firewall“ oder „Blockada“. Details zu den genannten Apps finden Sie bei mobilsicher.de

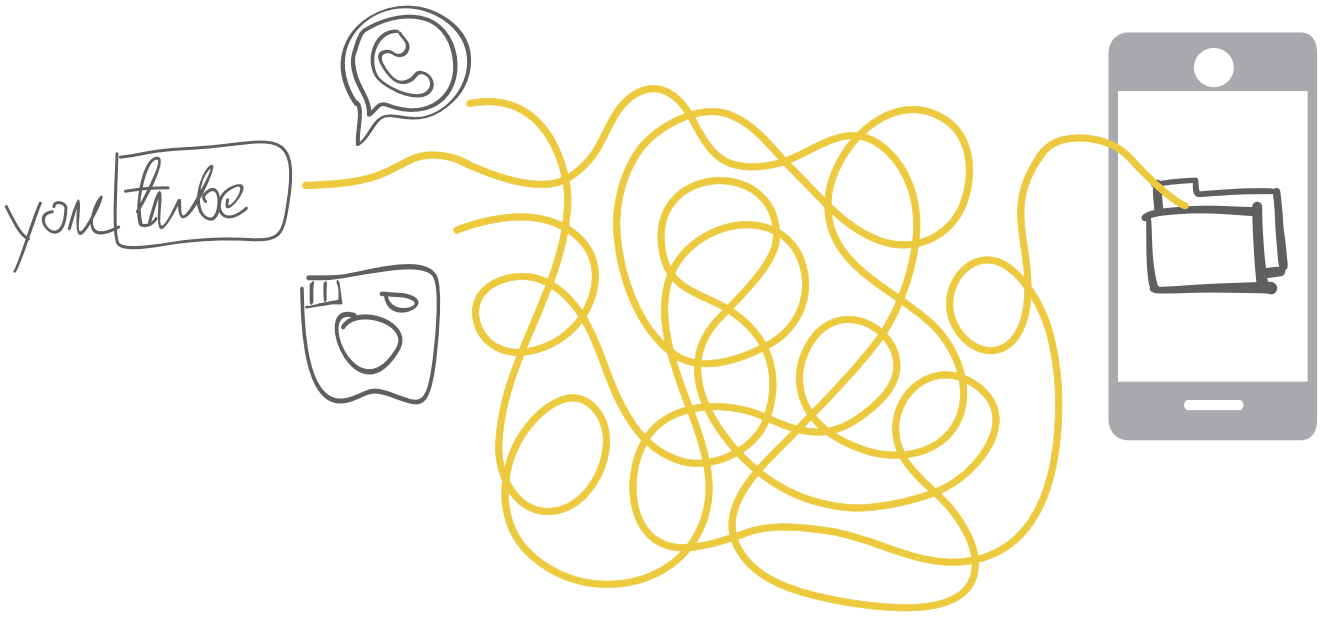
Fehleinschätzung Zugriffsrechte

Selbst wenn man die Berechtigungen einer App, vor dem Installieren prüft, bleibt noch die Frage: Was bedeuten diese Rechte eigentlich? Die drei größten Fehleinschätzungen sind:

- Telefon: Diese Berechtigung erlaubt einer App nicht nur zu telefonieren. Sie kann damit auch die IMEI, die eigene Telefonnummer, die SIM-Kartennummer und den Mobilfunkprovider auslesen.
- Daten aus dem Internet empfangen: Hat nichts damit zu tun, ob die App ins Internet gehen darf oder nicht. Mit dieser Berechtigung können Apps lediglich sogenannte Push-Nachrichten über einen Google-Dienst auf das Gerät senden. Das kann zum Beispiel die Benachrichtigung der Twitter-App sein, dass ein Tweet geteilt wurde, oder der E-Mail-App, dass eine Mail empfangen wurde.
- Zugriff auf alle Netzwerke: Mit dieser Berechtigung können Apps bestehende Internetverbindungen nutzen, um Daten zu versenden und zu empfangen. Ab Android 6.0 wird sie automatisch gewährt und standardmäßig nicht angezeigt. Apps können damit aber auch die sogenannte MAC-Adresse auslesen. Das ist die Identifikationsnummer des eingebauten Netzwerkadapters. Sie ist weltweit eindeutig. Damit lässt sich ein Gerät identifizieren.

Wie man Zugriffsrechte anzeigen und verwalten kann, wird bei mobilsicher.de im Detail erklärt.

Wie man Zugriffs-rechte anzeigen und verwalten kann, wird bei mobilsicher.de im Detail erklärt.



▷ Tipps und Übungen

Eltern und Lehrer: Einfach mal ausprobieren

Um mit Jugendlichen über ihren Umgang mit Apps zu sprechen, müssen Sie wissen, worum es geht. Um ein Gefühl für Dienste wie Snapchat oder Twitter zu bekommen, reicht es nicht, die Funktionsweise und das Logo zu kennen. Installieren Sie die Apps und versuchen Sie sich mit ein paar Posts. Tun Sie sich mit anderen Eltern oder Freunden zusammen.

Für den Unterricht: Kleine Werkstatt Zugriffsrechte

Lassen Sie sich anzeigen, wie viele Apps auf dem Handy Zugriff haben auf

- ▷ Adressbuch
- ▷ Ortsdaten
- ▷ Kalender
- ▷ Telefon
- ▷ SMS

Bei Android befindet sich die Einstellung unter:
Einstellungen → Apps → Tippen auf Zahnrad-Symbol oben rechts → App-Berechtigungen

Bei iOS befindet sich die Einstellung zu Zugriffsrechten unter:
Einstellungen → Datenschutz

Diskutieren Sie:

- ▷ Ist es bei jeder App einleuchtend, warum sie diese Rechte braucht?
- ▷ Welche Informationen erhält eine App mit den jeweiligen Berechtigungen?
- ▷ Legen Sie Hand an: Entziehen Sie den Apps Zugriffsrechte, die sie nicht brauchen.

Um mit Jugendlichen über ihren Umgang mit Apps zu sprechen, müssen Sie wissen, worum es geht.

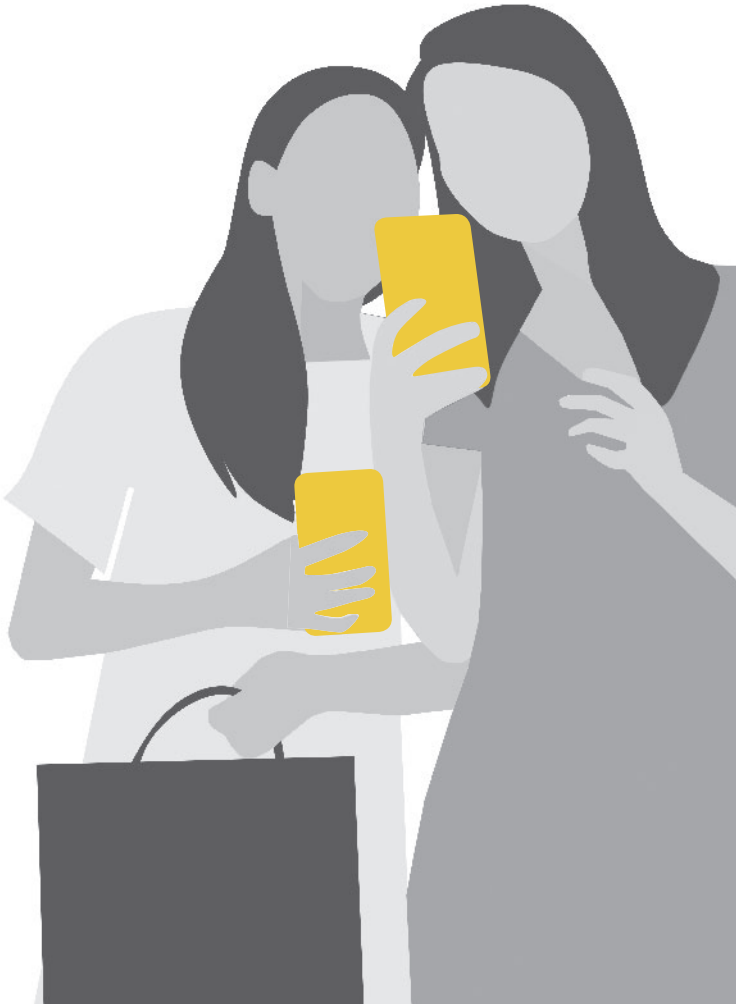
Kleine App-Werkstatt

Ziel ist es, die Apps auf dem eigenen Gerät kennenzulernen, sie einzuschätzen und gegebenenfalls durch bessere Apps zu ersetzen.

- ▷ Alle Teilnehmer*innen lassen sich anzeigen, wie viele Apps auf ihrem Gerät installiert sind.
- ▷ Bei wie vielen Apps ist die Funktion und der Anbieter bekannt?
- ▷ Bei wie vielen Apps ist die Funktion bekannt?
- ▷ Welche Merkmale sollte eine „gute“ App haben? (Im Sinne von Datenschutz, Transparenz, Sicherheit, Vertrauenswürdigkeit)

Welche Apps nutzen die Teilnehmer*innen für

- ▷ das Surfen im Internet
- ▷ die Suche im Internet
- ▷ Nachrichten senden (Messenger)
- ▷ E-Mail
- ▷ Erfüllen die verwendeten Apps die Forderungen an eine „gute“ App? Wenn nein, warum? Gibt es bessere Alternativen?



Lösungsvorschläge:

In unserem Merkblatt „Checkliste Apps“ am Ende dieses Heftes geben wir Hinweise, wie man eine App beurteilen kann.

Alternativen für die oben genannten Funktionen wären

- ▷ Surfen: Firefox-Browser
- ▷ Suchen: StartPage, DuckDuckGo
- ▷ Nachrichten senden: Wire, Threema, Signal
- ▷ Mail: K9, FairEmail (nur Android)

Details zu diesen Apps finden Sie online bei mobilsicher.de.

Wichtige Begriffe

- **IMEI:** Sie identifiziert jedes Mobilfunk-Gerät weltweit eindeutig. Sie wird beim Kontakt zum Mobilfunknetz an den Netzbetreiber übertragen. Viele Netzbetreiber im Ausland sperren Geräte anhand der IMEI, wenn diese als gestohlen gemeldet werden. In Deutschland erprobt die Telekom derzeit ein solches Verfahren. Die Polizei kann sichergestellte Geräte anhand der IMEI eindeutig identifizieren – aber nicht orten. Daher sollte man der Polizei und gegebenenfalls dem Mobilfunkprovider die IMEI mitteilen, wenn man einen Diebstahl meldet.
- **SIM-Karte:** Die SIM-Karte erhält man vom Mobilfunkprovider, zum Beispiel der Telekom. Sie ist nötig, damit das Smartphone sich im Mobilfunknetz einbuchen kann. Ohne SIM-Karte kann man nicht telefonieren. Über die SIM-Karte werden auch die Kosten für die Mobilfunknutzung abgerechnet.
- **Kill-Switch:** Auch Aktivierungssperre genannt. Ein Smartphone lässt sich damit nur in Betrieb nehmen, wenn der Nutzer oder die Nutzerin einen entsprechenden Code eingibt. Beim iPhone ist das die Apple-ID und das zugehörige Passwort, bei Android die Zugangsdaten zum Google-Konto. Bei Apple-Geräten ist sie standardmäßig aktiv. Bei Geräten mit Android 6.0 und höher (ab Werk) wird sie aktiv, sobald ein Google-Konto verknüpft und eine Bildschirmsperre mit PIN oder Muster eingerichtet ist. Theoretisch sind solche Geräte für Diebe wertlos, da sie nach dem Zurücksetzen auf Werkseinstellungen nicht ohne die Zugangsdaten in Betrieb genommen werden können. Für iOS-Geräte sank die Diebstahlquote nach der Einführung spürbar. Bei Android-Geräten kann die Funktion bei manchen Geräten mit technischen Tricks umgangen werden und ist bei günstigeren Modellen nicht immer implementiert.

Diebstahl und Datensicherheit

Smartphones sind zu unseren ständigen Begleitern geworden. Entsprechend leicht kann es passieren, dass die Geräte in falsche Hände geraten. Handys sind aber nicht nur eine beliebte Beute für Diebe. Sie werden auch ständig verloren oder irgendwo vergessen.

Wenn das Smartphone wegkommt, ist nicht nur ein kostspieliges Stück Technik weg, sondern auch alle Daten, die darauf gespeichert waren. Wenn es keine Datensicherung gibt, kann das für den Besitzer oder die Besitzerin schmerzhaft sein.

Aber es befinden sich oft auch Informationen auf dem Handy, mit denen bösartige Zeitgenoss*innen ernsthaften Schaden anrichten können. Das kann von gekaperten Online-Konten über teure Handyrechnungen bis hin zu Erpressung führen.

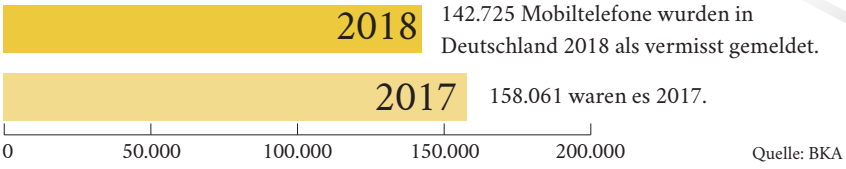
Sein Smartphone gegen unerwünschte Zugriffe zu sichern, ist nicht nur im Fall von Diebstahl oder Verlust wichtig. Schließlich ist es unser täglicher Begleiter und beinhaltet oft persönliche oder sogar intime Informationen.

Chat-Verläufe mit der besten Freundin oder die Facebook-Postings mit der Clique können als persönliches Tagebuch fungieren. Wer sein Smartphone unversperrt auf dem Küchentisch, der Schulbank oder im Büro liegen lässt, macht sich gegenüber neugierigen Klassenkamerad*innen, Kolleg*innen oder Geschwistern angreifbar. Eben mal die neueste SMS lesen oder den jüngsten Chat auf WhatsApp, das ist schnell getan und kann sehr aufschlussreich sein.

Wie schützt man Daten auf dem Smartphone vor Verlust und vor fremden Augen? Mit welchen Informationen können Kriminelle Schaden anrichten? Das Wichtigste zu diesen Fragen haben wir in diesem Kapitel zusammengestellt.

Zahlen und Fakten

Die gute Nachricht: Die Zahl der jedes Jahr als vermisst gemeldeten Handys scheint langsam zu sinken – vielleicht auch dank verbesserter Sicherheitsmaßnahmen. Sie ist aber mit über 100.000 pro Jahr noch immer sehr hoch. Da längst nicht jeder sein gestohlenes Gerät meldet, dürfte die Dunkelziffer noch deutlich höher sein.



Quelle: BKA

Was passiert mit gestohlenen Handys?

In der Regel landen gestohlene Geräte auf dem Gebrauchtwarenmarkt, nachdem sie auf Werkseinstellungen zurückgesetzt wurden. In einigen Fällen kommt es aber zu Folgeschäden, zum Beispiel, indem mit der SIM-Karte kostenpflichtige Nummern gewählt werden. 2012 wurde ein extremer Fall bekannt: Mit einem gestohlenen Handy wurden innerhalb von 24 Stunden durch Premium-Nummern Kosten in Höhe von 7.600 Euro verursacht.

Ebenfalls dokumentiert sind einige Fälle von Erpressungsversuchen mit gestohlenen Smartphones vor allem im Geschäftsbereich. Dabei drohten die Täter*innen mit der Veröffentlichung von Geschäftsgeheimnissen aus dem gestohlenen Gerät und forderten Geld für die Rückgabe.

Kettenreaktion: Das E-Mail-Konto als Schlüssel zur Online-Präsenz

Die E-Mail-Adresse ist nicht nur zum Austausch von Nachrichten wichtig, sondern auch für die Anmeldung bei Online-Diensten. Wer ein Facebook-, Twitter- oder Snapchat-Konto eröffnet, muss dabei eine E-Mail-Adresse angeben. An diese Adresse wird bei der Registrierung eine E-Mail mit einem Link geschickt, über den man das Konto bestätigt.

Wenn man sein Passwort vergisst, wird der Link für das neue Passwort auch an die registrierte E-Mail-Adresse geschickt. Fast alle Online-Dienste nutzen diese Funktion.

Wenn diese E-Mail-Adresse aber in der Mail-App auf dem Handy eingerichtet ist, kann es problematisch werden. Denn um auf dem Handy E-Mails zu checken, muss man nach der ersten Anmeldung kein Passwort mehr eingeben.

Wenn ein Dieb ein Smartphone ohne aktive Bildschirmsperre in seinen Besitz bringt, kann er neue Passwörter für das Facebook-, Amazon- oder Twitter-Konto anfordern.

Die einfachste Lösung für das Problem – neben einer guten Bildschirmsperre – ist, eine gesonderte E-Mail-Adresse speziell für Anmeldungen bei Online-Diensten anzulegen. Diese Adresse sollte nicht auf dem Smartphone eingerichtet sein, sondern nur auf einem Gerät abgerufen werden, das die eigenen vier Wände möglichst nicht verlässt.

Passwort oder Fingerabdruck?

Der beste Schutz gegen unberechtigte Zugriffe auf das Handy ist eine Bildschirmsperre. Um das Handy zu nutzen, muss man dann aber erst ein Passwort oder einen Code eingeben. Doch Passwörter und Codes, insbesondere lange und komplizierte, sind und bleiben unbeliebt.

Wenn große Dienste, wie zum Beispiel Yahoo oder Dropbox, angegriffen werden, kommen die gestohlenen Nutzerpasswörter oft an die Öffentlichkeit. Das Hasso-Plattner-Institut in Potsdam ermittelt jedes Jahr aus solchen Daten die am häufigsten verwendeten Passwörter. Seit Jahren landet die Kombination „123456“ auf dem ersten Platz, auch „passwort“ oder „hallo“ sind stets unter den Top Ten.

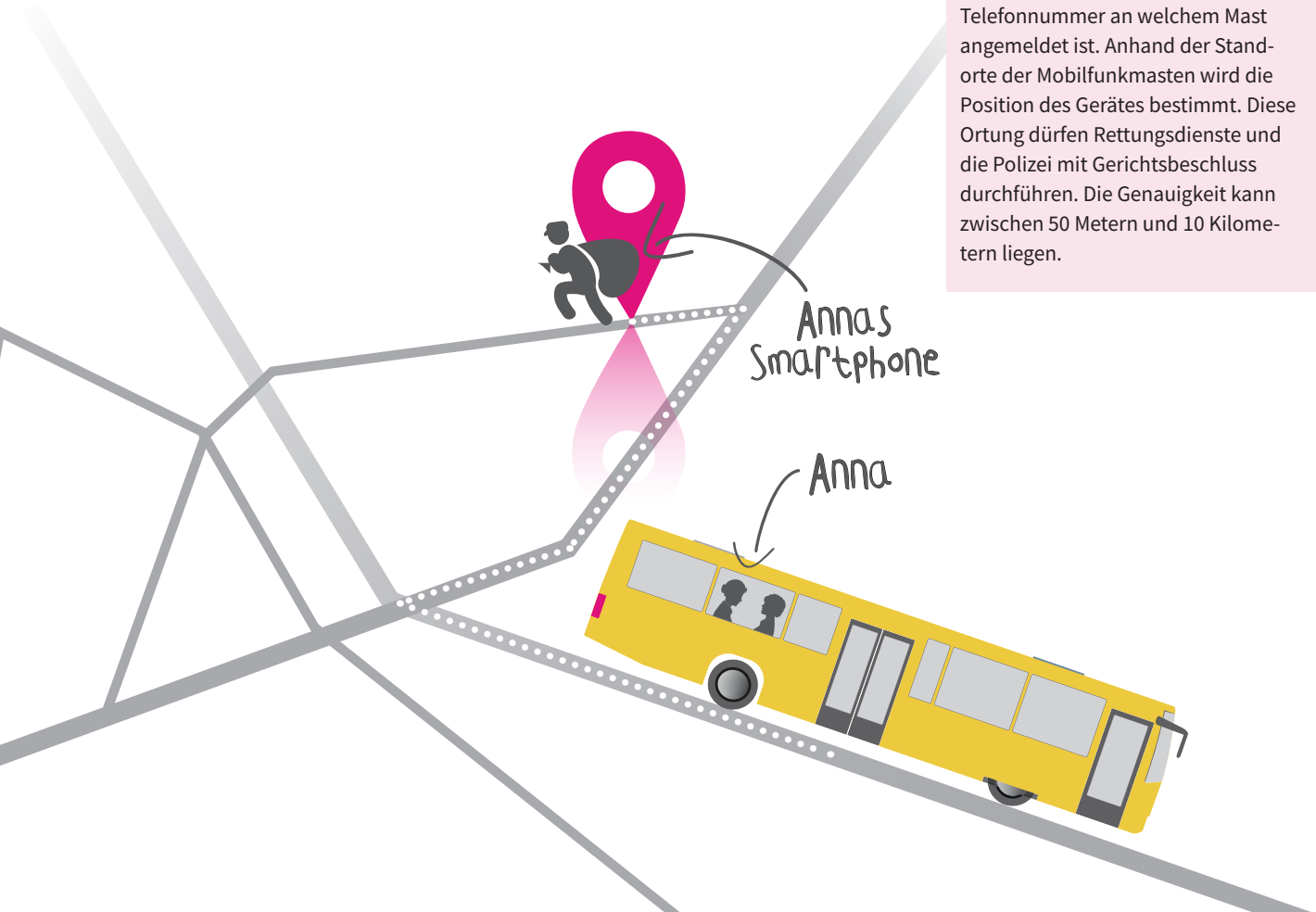
Woher weiß ein Smartphone, wo es ist?

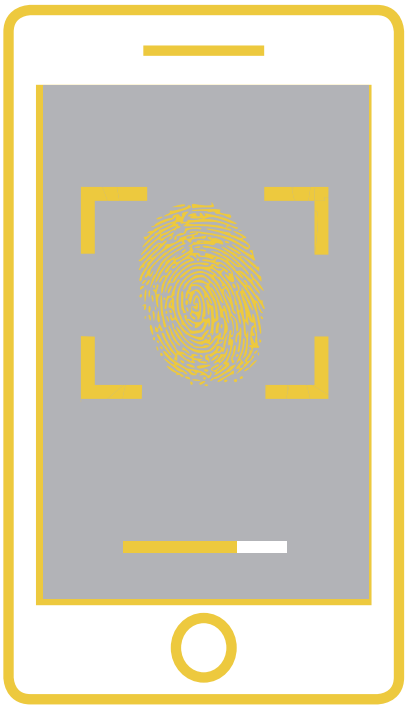
Der Standort eines Smartphones oder Tablets kann auf verschiedene Arten ermittelt werden. Die wichtigsten sind GPS- (Global Positioning System) und WLAN-Ortung.

- **GPS:** Das Gerät ermittelt seine Position durch Kommunikation mit Satelliten. Diese Position kann es dann per Internet oder Mobilfunk versenden.
- **WLAN:** Das Smartphone schickt eine Liste der WLAN-Netze, die es an seinem Aufenthaltsort empfängt, über das Internet an eine Datenbank, wo sie abgeglichen wird. Dort sind die Positionen vieler WLAN-Netze gespeichert. Das Gerät muss dazu nicht bei den WLAN-Netzen angemeldet sein.

Orten per Mobilfunknetz (GSM-Ortung oder Funkzellenortung)

Jedes Mobiltelefon meldet sich automatisch beim nächstgelegenen Mobilfunkmast an. Der Mobilfunkanbieter kann daher sehen, welche Telefonnummer an welchem Mast angemeldet ist. Anhand der Standorte der Mobilfunkmasten wird die Position des Gerätes bestimmt. Diese Ortung dürfen Rettungsdienste und die Polizei mit Gerichtsbeschluss durchführen. Die Genauigkeit kann zwischen 50 Metern und 10 Kilometern liegen.





Bei allen biometrischen Verfahren ist es bereits gelungen, sie mit Fälschungen auszutricksen. Große Hoffnung setzt man auf Algorithmen, die das typische Bewegungsmuster von Nutzer*innen erkennen sollen.

Viele Internetfirmen arbeiten daher an Verfahren, das ungeliebte Passwort abzuschaffen und mit biometrischen Daten zu ersetzen. Diese, so hoffen die Unternehmen, wären praktischer zu nutzen und würden damit besser akzeptiert.

Inzwischen gibt es zahlreiche Laptops und Smartphones mit Fingerabdruckscanner auf dem Markt. Sie bieten eine einfache Alternative, damit nur berechtigte Nutzer*innen auf ein Gerät zugreifen können. Auch die Entsperrung durch Bilderkennung ist inzwischen auf einigen Geräten verfügbar.

Allerdings ist es bei allen biometrischen Verfahren bereits gelungen, sie mit Fälschungen auszutricksen. Ob sie jemals so sicher sein werden wie ein gutes Passwort, ist daher fraglich. Besser als ein schlechtes Passwort sind sie aber allemal.

Diebstahlschutz

Bei fast allen modernen Smartphones gibt es eine Funktion, mit der man den Aufenthaltsort des Gerätes über das Internet bestimmen und das Gerät von der Ferne aus sperren oder sogar löschen kann.

So ist auf allen Android-Geräten die Funktion „Mein Gerät finden“ verfügbar. Die App von Google übermittelt den Aufenthaltsort des Handys dabei nur an Google, wenn Sie die Funktion zum Orten nutzen. Wir empfehlen daher dringend, sie zu aktivieren.

Wenn Sie sich in Ihr Google-Konto einloggen, bekommen Sie den Aufenthaltsort des Handys angezeigt, sofern es mit dem selben Konto verknüpft ist. Dort können Sie auch nachträglich eine Bildschirmsperre für ein Gerät installieren, falls es noch keine hat. Voraussetzung dafür ist, dass das Handy eine Internetverbindung über WLAN oder Mobilfunk aufbauen kann.

Auf iPhones der Firma Apple gibt es mit „Mein iPhone suchen“ eine vergleichbare Funktion. Hier muss man sich in die iCloud einloggen, um den Standort des Gerätes angezeigt zu bekommen oder eine Sperre einzurichten.

Viele Hersteller von Anti-Viren-Software haben inzwischen auch Apps zur Diebstahlsicherung herausgebracht. Diese haben aber nur dann einen Vorteil gegenüber den Lösungen von Apple und Google, wenn sie den Standort auch per SMS mitteilen können. Dann kann das Handy auch geortet werden, wenn es keine Internetverbindung, sondern nur Mobilfunknetz hat.

Bei all diesen Lösungen muss man beachten, dass der Hersteller der entsprechenden Sicherheitssoftware den Aufenthaltsort des Handys mehr oder weniger regelmäßig erfährt.

Alle genannten Lösungen zur Fernortung müssen VOR dem Verlust auf dem Gerät installiert und/oder aktiviert werden. Sie nutzen die geräteeigenen Ortungsdienste über GPS oder WLAN-Abfrage. Sie funktionieren nur, wenn das GPS/die Standortbestimmung an ist und das Handy eine Internetverbindung hat.

Weder Polizei noch Provider suchen ein gestohlenes Smartphone über Funkzellenortung (GSM, siehe Kasten S. 29). Dieses Verfahren wird nur bei schweren Straftaten eingesetzt.

▷ Tipps und Übungen

Es gibt ein paar einfache, aber effektive Maßnahmen, um im Falle eines Diebstahls das Schlimmste zu verhindern.

Übung eins: Kleiner Sicherheitsworkshop

▷ Überlegen Sie, was passieren könnte, wenn ein Gerät gestohlen wird, und was zu tun wäre.

Welchen Unterschied gibt es für den Fall, dass …

a: das Gerät unversperrt war?

b: das Gerät mit einer Bildschirmsperre gesichert war?

Lösungsvorschlag: In unserem Merkblatt „Handy weg? Den Schaden begrenzen“ am Ende dieses Heftes geben wir Tipps zum Ausschneiden.

▷ Fragen Sie die Teilnehmer*innen, welche Sicherheitsmaßnahmen sie auf ihrem Gerät aktiviert haben

Lösungsvorschlag: In unserem Merkblatt „Vorbeugen – Diebstahl und Kostenfallen“ am Ende dieses Heftes haben wir die wichtigsten Maßnahmen aufgelistet. Einige Punkte können Sie sofort erledigen.

Übung zwei: Passwort-Werkstatt

▷ Fragen Sie die Teilnehmer*innen, welches Sperrverfahren sie nutzen: keins, Muster, PIN, Passwort?

▷ Vermutlich wird es einige geben, die die Muster-Eingabe nutzen. Machen Sie eine Partnerübung. Zuerst stellt jeder ein „Test-Muster“ auf seinem Smartphone ein. Dann gibt einer das Testmuster zum Entsperren ein. Der andere schaut ihm dabei über die Schulter. Schafft es der „Schulterschauer“ auf Anhieb, sich das Muster so zu merken, dass er das Smartphone ebenfalls entsperren kann? Sprechen Sie darüber, welche Methoden sicher sind.

▷ Entwickeln Sie gemeinsam einen „Passwort-Algorithmus“. Denken Sie sich Regeln aus, nach denen Sie ein sicheres Passwort im Kopf generieren können.

Lösungsvorschlag:

▷ Merksatz bilden, am besten etwas Selbstausgedachtes wie „Jeden Donnerstagabend gehe ich mit meinem roten Gummipferd ins Schwimmbad kraulen.“

▷ Jeder zweite Buchstabe in jedem Wort kommt ins Passwort. Dabei wechseln wir groß und Kleinschrift ab. Das ergibt dann: eObEcIeOuNcR

▷ Buchstaben durch Zahlen und Sonderzeichen ersetzen: Alle Os werden durch @ ersetzt. Alle Is durch !. g kann durch 9 ersetzt werden, b durch 6. Das ergibt dann: e@6Ec!e@uNcR. Das ist ein sehr sicheres Passwort.

Hilfe und Beratung

Polizei: Bei gestohlenen Smartphones wenden Sie sich an die nächste Polizeidienststelle. Gegenüber Versicherungen und Provider steht man besser da, wenn es eine Polizeimeldung gibt.

Zentraler Kartensperrdienst: Wenn das Handy weg ist, sollten Sie auf jeden Fall die SIM-Karte sperren. Sonst können Unbefugte mit Ihrem Gerät unter Umständen hohe Summen vertelefonieren.

Das geht überall in Deutschland mit der **116 116.**

In unserem Merkblatt „Handy weg? Den Schaden begrenzen“ am Ende dieses Heftes geben wir Tipps zum Ausschneiden.

Kostenfallen

Das Thema ist viel älter als Smartphones, aber noch immer aktuell: Unerwartete Kosten auf der Mobilfunkrechnung, Abzock-Abos, die man gar nicht will, SMS-Käufe, die man nie getätigt hat.

Dazu kommt mit den Smartphones noch die Möglichkeit, Guthaben in Googles Play-Store oder in Apples App-Store zu hinterlegen und damit zum Beispiel Apps zu kaufen oder sogenannte In-App-Käufe zu tätigen.

Dabei kann man leicht den Überblick über die Kosten verlieren. Wo verbergen sich Kostenfallen und wie kann man sich dagegen schützen?

Direct Carrier Billing (veraltet: WAP-Billing)

Manche Dinge kann man direkt mit der Telefonnummer bezahlen, zum Beispiel die Testberichte der Stiftung Warentest. Die Kosten erscheinen dann auf der Mobilfunkrechnung – daher der Begriff „Direct Carrier Billing", direkte Abrechnung über den Mobilfunkanbieter.

Die Unternehmen oder Händler, die solche Dinge zum Kauf anbieten und über die Mobilfunknummer abrechnen, nennt man „Drittanbieter". Der Name kommt daher, dass es sich um eine Leistung handelt, die nicht vom Mobilfunkanbieter selbst kommt (das wäre der Erstanbieter) und auch nicht von einem Unternehmen, das vom Erstanbieter beauftragt wurde (das wäre der Zweitanbieter). Damit ein Drittanbieter über die Telefonnummer abrechnen kann, muss er sich erst beim Mobilfunkanbieter anmelden und dort freigeschaltet werden.

Das Bezahlen per Mobilfunkrechnung kann praktisch sein. Manchmal tauchen dort aber Beträge für Dinge auf, die man nie bewusst gekauft hat. In der Vergangenheit sind solche Fälle oft aufgetreten, weil manche Drittanbieter auf ihren Webseiten nur unzureichend gekennzeichnet haben, dass durch Antippen ein Kauf abgeschlossen wird – teils bewusst, teils aus Unkenntnis.

Inzwischen gibt es zwar bessere Sicherheitsmaßnahmen seitens der Telekommunikationsanbieter, das Problem besteht aber nach Aussage der Verbraucherzentralen fort – noch immer beschweren sich viele Nutzer*innen über ungewollte Käufe und Abos.

Wichtig: Wenn Sie mit Ihrem Handy im WLAN surfen, kann ein solcher Kauf nur stattfinden, wenn Sie Ihre Mobilfunknummer selbst irgendwo eingeben. Bösartige Anbieter versuchen Sie eventuell unter falschen Angaben dazu zu bringen. Wenn Sie über das Mobilfunknetz surfen, kann eine bösartige Webseite den Kauf auch abwickeln, ohne dass Sie die Nummer eintippen. Hier kann ein Kauf tatsächlich durch einen einzigen falschen Tipp auf ein Banner ausgelöst werden.

Vorsicht, falsche Freunde

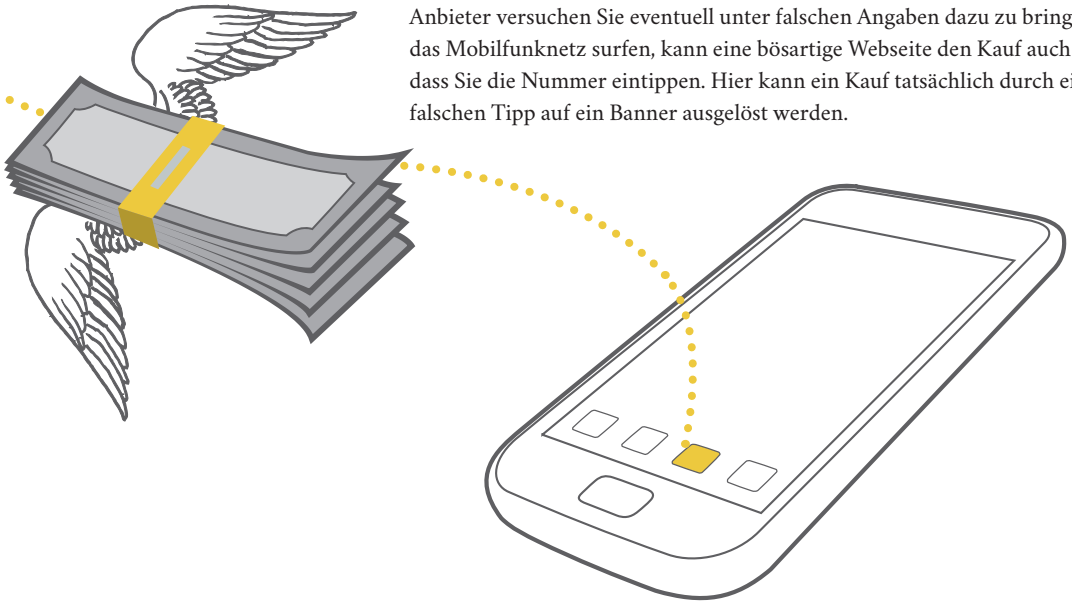
Wie das TAN-SMS-Verfahren ausgehebelt wird.
Surft man mit dem Handy im WLAN und landet auf einer Direct-Carrier-Billing-Seite, so setzen die Mobilfunkprovider das sogenannte SMS-TAN verfahren ein, um den Nutzer oder die Nutzerin zu authentifizieren.

Dabei müssen Nutzer*innen ihre Telefonnummer eingeben und bekommen daraufhin eine SMS mit einem Code. Diesen Code müssen sie wiederum für den Kauf eingeben.

Es gibt seit einigen Jahren einen Trick, um Nutzer*innen zu veranlassen, ihre Mobilfunknummer und den zugesendeten Code einer TAN-SMS einem Angreifer zu verraten.

Dabei wird man auf Facebook von einem vermeintlichen Freund angesprochen: „Hey, ich habe deine Handynummer verloren, kannst du sie mir eben schicken?" Wer darauf einsteigt, bekommt kurz darauf eine SMS mit einem Code zugesendet. Der Betrüger oder die Betrügerin schreibt dann etwas wie „Kannst du mir den Code schicken? Ich erklär es dir später."

Geht man darauf auch ein, kann auf der nächsten Mobilfunkrechnung eine böse Überraschung warten.



Sonderrufnummern

Alle Mobilfunkanbieter stellen sogenannte Sonderrufnummern zur Verfügung, um damit besondere Dienste abzurechnen. Zum Beispiel kann man mit einer SMS an eine bestimmte Nummer einen Beitrag zur Berliner Kältehilfe spenden. Diese Kosten tauchen ebenfalls in der Mobilfunkrechnung auf. Typische Sonderrufnummern beginnen mit:

- **0900** (Premiumdienste, Preisansage vorgeschrieben)
- **118** (Auskunftsdienste, Preisansage vorgeschrieben ab 2 Euro/Minute)
- **0137** (Massenverkehrsdienste, Preisansage vorgeschrieben)
- **0180** (Servicedienste, maximal 3 Euro/Minute oder 30 Euro gesamt)
- **012** (Neuartige Dienste, Preisansage ab 2 Euro/Minute vorgeschrieben)
- **SMS an fünf und sechsstellige Nummer** (Kurzwahldienste, Preisangabe vorgeschrieben ab 2 Euro pro Inanspruchnahme)

Zeiten in der Warteschleife dürfen nicht abgerechnet werden.

Während viele Sonderrufnummern legitimen Zwecken dienen, können sie auch missbraucht werden: Sonderrufnummern werden manchmal von Schadprogrammen missbraucht, die heimlich Anrufe tätigen oder SMS versenden.

Es gibt auch die Masche mit dem „Lockanruf". Dabei werden ganze Nummernblöcke automatisch von einer teuren Sonderrufnummer aus angerufen und nach einem Klingeln wieder aufgelegt. Wer zurückruft, muss zahlen.

In-App-Käufe

Bei In-App-Käufen können Nutzer*innen, wie der Name schon sagt, innerhalb der App gegen Geld Zusatzleistungen erwerben. Vor allem Spiele-Apps nutzen das. So lassen sich im Spiel Ausrüstungsgegenstände, Leben oder mehr Spielzeit dazukaufen. Das Spiel „Clash of Clans" steht regelmäßig an der Spitze der Apps mit den höchsten Umsätzen durch solche In-App-Käufe. Clash of Clans ist ein Online-Strategie-Spiel für Android und iOS, bei dem Nutzer*innen „Juwelen" kaufen können, um den Spielfortschritt zu beschleunigen.

Die Betreiber der App-Stores kennzeichnen Apps eindeutig, bei denen solche Käufe möglich sind. Bei In-App-Käufen ist Betrug weniger ein Problem als die fehlende Kostenübersicht. Gerade im Spielrausch können sich solche Käufe zu relevanten Summen zusammenläppern.

Kindern ist zudem nicht immer bewusst, dass es sich um echtes Geld handelt, wenn sie zum Beispiel Spielgeld kaufen. Besonders problematisch sind Apps, bei denen man Käufe mit Spielwährungen tätigt, die man wiederum mit echtem Geld einkauft. Diese Umrechnungen sollen die wahren Kosten verschleiern.

Vor allem bei Apps für iPhone und iPad ein Problem, aber auch bei Android bekannt: In-App-Abos. Oft sind diese nicht klar gekennzeichnet, sodass Nutzer*innen denken, sie tätigen eine Einmalzahlung. In Wirklichkeit wird der Betrag regelmäßig abgebucht.

Rechtliches

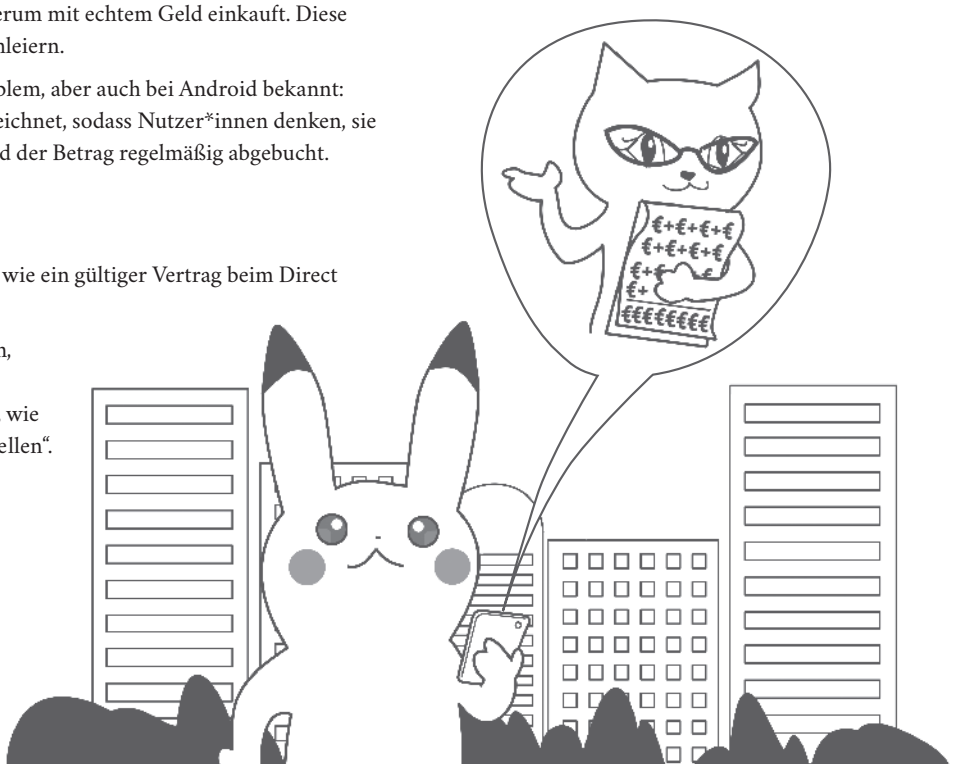
Es gibt eindeutige gesetzliche Regelungen dazu, wie ein gültiger Vertrag beim Direct Carrier Billing zustande kommt:

- Anbieter müssen explizit auf Käufe hinweisen, zum Beispiel durch eine Schaltfläche, auf der unmissverständliche Formulierungen stehen, wie „Jetzt kaufen" oder „Jetzt kostenpflichtig bestellen". Nur „Bestellen" gilt zum Beispiel nicht als eindeutig genug.

Was tun bei unbekannten Kosten?

Erster Ansprechpartner: Der eigene Mobilfunkanbieter. Widersprechen Sie der Rechnung und verlangen Sie dort Ihr Geld zurück.

- Mobilfunkrechnung kürzen – das empfehlen manche Verbraucherschützer*innen und Rechtsanwält*innen. Dabei geht man allerdings das Risiko ein, dass der Mobilfunkbetreiber den Anschluss sperrt. Die Anbieter dürfen das zwar nicht, es geschieht in der Praxis aber trotzdem.
- Abo oder Dienstleistung beim Drittanbieter kündigen: Es ist gesetzlich vorgeschrieben, dass auf der Rechnung der Name und die Adresse der Firma steht. Welche Leistung geliefert wurde, muss dagegen nicht angegeben werden. Am einfachsten ist es deshalb, schriftlich per Einschreiben der Forderung zu widersprechen und hilfsweise die Leistung zu kündigen. Hilfsweise deshalb, damit man nicht im Nachhinein anerkennt, dass ein Vertrag bestand.



Hilfe und Beratung

- **Verbraucherzentrale Nordrhein-Westfalen:** Hier gibt es Informationen und Musterbriefe für Kündigung und Widerspruch. www.verbraucherzentrale.nrw/node/12613
- **Europäisches Verbraucherzentrum Deutschland:** Bei Anbietern aus dem europäischen Ausland kann man sich dorthin wenden.
- **Verbraucherzentralen:** Bieten im Schadensfall Einzelberatung an. Die Kosten betragen rund 20 Euro (je nach Bundesland).

▷ Der Hinweis muss eindeutig, gut sichtbar sein und es darf nichts Anderes dabeistehen.

▷ Die Information, wie das Abo gekündigt werden kann, muss leicht zugänglich sein.

Sind diese Bedingungen nicht erfüllt, ist der Vertrag nicht gültig. Das Problem: Das nachzuweisen, ist meistens sehr schwierig.

Wer ist zuständig?

Beim Direct Carrier Billing kaufen die Mobilfunkanbieter die Forderungen vom Inhalteanbieter auf. Rechtlich gesehen sind sie auch der Ansprechpartner, wenn es Streitigkeiten gibt. Dazu gibt es ein einschlägiges Gerichtsurteil. In der Vergangenheit haben die Mobilfunkanbieter Nutzer*innen aber immer wieder an die Inhalteanbieter verwiesen. Lassen Sie sich nicht abwimmeln – wenden Sie sich im Zweifel an eine Verbraucherzentrale.

▷ Tipps gegen Kostenexplosionen

▷ **Informieren:** Kindern ist nicht immer klar, dass es bei In-App-Käufen um reales Geld geht. Eltern und Kinder sollten fest vereinbaren, wie viel Geld dort ausgegeben werden darf.

▷ **Drittanbietersperre einrichten:** Damit Drittanbieter nicht direkt über die Mobilfunkrechnung Dienstleistungen abrechnen können, kann man bei seinem Mobilfunkanbieter eine sogenannte Drittanbietersperre aktivieren. Dies ist kostenlos und geht meist online, per Anruf oder per Mail an den Kundenservice des Anbieters.

▷ **Regelmäßig die Rechnung überprüfen:** Klingt banal, aber viele tun es nicht: Regelmäßig überprüfen, ob die Posten auf der Handyrechnung stimmen. Je länger man wartet, desto höher wird der Schaden.

▷ **Bestätigungs-SMS und sonstige Meldungen beachten:** Hinweise auf dem Smartphone nicht einfach wegklicken, sondern lesen! Vor allem Kinder und Jugendliche darauf hinweisen, welche finanziellen Folgen eine Abofalle hat.

▷ **Achtung bei Anrufen von unbekannten Nummern:** Schauen Sie lieber einmal mehr hin, ob es sich nicht um eine Sonderrufnummer handelt.

▷ **Keine Zahlungsdaten hinterlegen.** Statt Kreditkarten- oder Lastschriftverfahren kann man auch Gutscheinkarten für Einkäufe mit dem Smartphone verwenden. Das bringt Kostenkontrolle und Schadensbegrenzung im Verlustfall.

▷ **In-App-Käufe mit Passwort schützen.** Für die großen App-Märkte kann man ein Passwort einrichten, das jedes Mal eingegeben werden muss, wenn man etwas kauft. Das geht im Play-Store unter
Menü (drei horizontale Striche oben links) → Einstellungen→ Authentifizierung für Käufe erforderlich.
Für den App-Store bei iOS finden Sie die Funktion unter
Einstellungen→ Allgemein→ Einschränkungen.

▷ **Abos regelmäßig überprüfen.** Android: Öffnen Sie die Play-Store-App, tippen Sie auf die drei waagerechten Striche oben links und dann auf Abos.
Für iPhones und iPads: Tippen Sie auf Geräteeinstellungen > Ihr Name > iTunes & App Store > Apple-ID > Apple-ID anzeigen > geben Sie Ihr Passwort ein > Scrollen Sie zu „Abos“.

▷ **Für iOS: Familienfreigabe nutzen.** Apple bietet ein umfangreiches Konzept für Familien an. Werden Apple-IDs zu einer Familie zusammengefasst, können beispielsweise Eltern die Einkäufe ihrer Kinder genehmigen.

▷ **Prepaid- oder Flatrate-Verträge nutzen.** Natürlich können auch durch die ganz normale Nutzung – Surfen, Telefonieren und Texten – Kosten entstehen. Wählen Sie für Ihr Kind ein Vertragsmodell, bei dem diese Kosten nicht ins Uferlose wachsen können.

Merkzettel Diebstahl und Kostenfallen: Vorbeugen

Geht ein Mobilgerät verloren, ist nicht nur der Kaufwert weg, sondern auch viele wichtige Daten. Mit diesen Tipps sind zumindest Ihre Daten bei Verlust oder Diebstahl geschützt. In manchen Fällen können Sie das Gerät damit auch leichter wiederfinden.

Bildschirmsperre einrichten	Sie finden die Funktion bei Android bei den Geräteeinstellungen unter dem Punkt Sicherheit, bei iOS unter „Touch ID & Code“.
Nur Android: Telefonspeicher verschlüsseln	Die Funktion befindet sich in der Regel bei den Geräteeinstellungen unter dem Punkt Sicherheit. Hinweis: Der Vorgang kann nicht rückgängig gemacht werden. iPhones und Geräte mit Android 7.0 und höher sind standardmäßig verschlüsselt, Nutzer*innen müssen nichts weiter unternehmen.
Sicherungskopie anlegen	Sichern Sie Ihre Daten regelmäßig, am besten lokal auf dem Rechner.
SIM-Karten-PIN nicht deaktivieren	Sonst könnten Diebe die SIM-Karte in ein anderes Telefon stecken und dann auf Ihre Kosten telefonieren.
iCloud-/Google-Konto: Starkes Passwort verwenden	Wer die Zugangsdaten zu Google-Konto oder iCloud kennt, kann damit an Daten aus Ihrem Gerät gelangen. Verwenden Sie ein starkes Passwort oder Zwei-Faktor-Authentifizierung.
Mail-Adresse zur Wiederherstellung	Richten Sie für Google-Konto oder iCloud eine Mail-Adresse zur Wiederherstellung ein, die nicht mit dem Mobilgerät verbunden ist. Auch für andere wichtige Konten wie Facebook oder WhatsApp sollte eine eigene Mail-Adresse existieren.
Fernzugriff einrichten	Sie können damit Ihr Gerät im Verlustfall orten und sperren. Android: Die Funktion „Mein Gerät finden“ ist in den Geräteeinstellungen unter dem Punkt „Sicherheit“. iOS: Die Funktion „Mein iPhone suchen“ finden Sie in den Einstellungen unter „Apple-ID > iCloud > Mein iPhone suchen“.
Wichtige Informationen notieren	IMEI-Nummer (eindeutige Identifikationsnummer des Gerätes): Wird angezeigt, wenn Sie *#06# wählen. Zentraler Kartensperrdienst: 116 116, oder aus dem Ausland: +49 30 4050 4050.
Drittanbietersperre einrichten	In der Regel genügt dafür ein formloses Schreiben per Mail an den Provider. Damit sind Sie vor Kosten durch Sonderrufnummern oder Direct Carrier Billing effektiv geschützt.
Guthabenkarte hinterlegen	Hinterlegen Sie für Käufe in App-Store oder Play-Store Guthabenkarten, das bringt Kostenkontrolle. Es gibt diese Karten in Drogerien und Supermärkten.
Passwort für Käufe einrichten	Wenn Kinder im Spiel sind: Richten Sie die Play-Store- oder App-Store-App so ein, dass sie vor jedem Kauf ein Passwort abfragt.

Merkzettel Handydiebstahl: Schaden begrenzen

Passieren kann es jedem – schneller als man denkt, kann das Smartphone weg sein. Egal ob verloren oder gestohlen, man kann einige Maßnahmen ergreifen, um den Schaden zu begrenzen.

Fernzugriff nutzen (falls aktiviert)	Falls Sie eine Funktion für den Fernzugriff installiert haben, nutzen Sie diese. Reagieren Sie sofort. Diebe werden versuchen, alle Fernzugriffsmöglichkeiten abzuschalten. Versuchen Sie, das Gerät zu sperren (falls es nicht schon gesperrt ist) und dann zu orten. Falls Sie dafür Googles „Mein Gerät finden“ nutzen, loggen Sie sich unter: www.google.de in Ihr Google-Konto ein und wählen den Punkt „Smartphone suchen“. Falls Sie „Mein iPhone/iPad suchen“ nutzen, loggen Sie sich unter www.icloud.com in Ihr iCloud-Konto ein.
Smartphone anrufen	Vielleicht haben Sie das Gerät nur verloren und ein Finder meldet sich. Falls sich niemand meldet, sperren Sie erst danach die SIM-Karte.
Falls das Gerät unauffindbar bleibt: SIM-Karte sperren	Unter der Telefonnummer 116 116 oder im Ausland +49 30 4050 4050. Sie können das Gerät dann nicht mehr anrufen. Für das Entsperren fallen Gebühren an.
Google-Konto/iCloud und Mailkonten sichern	Loggen Sie sich in Ihr Google-Konto / iCloud-Konto ein und ändern Sie das Passwort. Falls Sie E-Mail-Konten auf Ihrem Smartphone eingerichtet haben, ändern Sie auch die Passwörter dieser Konten.
Google Pay und Apple Pay	Falls Sie Google Pay nutzen: Beträge bis 25 Euro kann ein Dieb bezahlen, auch wenn Ihr Gerät gesperrt ist. Loggen Sie sich sofort in Ihr Google-Konto ein und sperren Sie die hinterlegten Bankkarten unter dem Punkt „Zahlungen und Abos -> Zahlungsmethoden verwalten“. Falls Sie Apple Pay nutzen: Der Dieb kann nur bezahlen, wenn er Ihr Gerät entsperren kann. Sie können die hinterlegten Bankkarten über Ihr iCloud-Konto sicherheitshalber sperren.
Internet-Konten sichern	Ihr Gerät bleibt verschwunden: Ändern Sie die Passwörter aller wichtigen Internet-Konten, mit denen Ihr Gerät verbunden ist, wie etwa Facebook, Twitter, WhatsApp.
Verlust melden	Melden Sie den Verlust der Polizei, Ihrem Provider und gegebenenfalls Ihrem Geräteversicherer.
Im Fundamt fragen	Fragen Sie im Fundamt oder in den Fundstellen von Bahn, Taxizentrale und so weiter. Manchmal trudeln Fundsachen dort auch erst nach einigen Tagen ein.

Checkliste: Apps richtig beurteilen

Was eine App wirklich auf dem Smartphone tut, kann man als Nutzer*in kaum kontrollieren. Es gibt aber einige Merkmale, die Hinweise darauf geben, ob eine App vertrauenswürdig ist:

Woher kommt die App:	Apps aus den Stores von Google oder Apple haben auf jeden Fall schon eine Überprüfung hinter sich. Bei Apps aus anderen Quellen sollte man besonders aufmerksam sein.
Wer ist der Hersteller:	Wem gehört der Dienst oder die App, die Sie gerade installieren? Gibt es eine Firmen-Webseite? Tippen Sie im Play-Store auf den Namen des Anbieters, sehen Sie, welche anderen Apps er betreibt. Auch das kann aufschlussreich sein.
Geschäftsmodell:	Womit verdient der Hersteller Geld? Wie werden die Kosten für das Bereitstellen der App oder des Dienstes gedeckt? Ist das Modell Werbung oder Datenhandel? Steht eine Stiftung dahinter oder eine freiwillige Community? Gerade wenn Sie für eine App nichts bezahlen, sollte diese Frage klar beantwortet sein.
Geschäftssitz des Herstellers:	Liegt der Firmensitz des Herstellers in einem Rechtsstaat, in dem Sie Ihre Interessen gegebenenfalls auch vor Gericht durchsetzen könnten? Gibt es eine Kontaktadresse?
Datenschutzerklärung:	Ist eine Datenschutzerklärung vorhanden? Wenn ja, ist dies ein gutes Zeichen. Der Hersteller hat sich zumindest formal mit Datenschutzanforderungen auseinandergesetzt. Ist die Datenschutzerklärung auf Deutsch? Wenn nein, ist sie eventuell nicht rechtskräftig.
Bewertungen:	Apps in den App-Stores können von Nutzer*innen bewertet werden. Oft lohnt sich ein Blick in die Kommentare, um von verbreiteten Problemen mit der App zu erfahren. Achtung: Positive Kommentare können auch gekauft sein.
Open Source:	Es ist immer von Vorteil, wenn der Programmcode einer App für jedermann zugänglich ist. Der Fachbegriff dafür ist Open Source (quelloffen). So können unabhängige Fachleute den Code auf Schwachstellen und versteckte Funktionen überprüfen. Der F-Droid-Store für Android enthält zum Beispiel ausschließlich Open-Source-Apps.
Berechtigungen:	Werfen Sie einen Blick in die Zugriffsberechtigungen der App. Sind sie plausibel? Allerdings ist nicht jede App mit vielen Zugriffsrechten gleich unseriös. Oft ist dies eine Kostensache: Es ist einfacher, eine App mit vielen Zugriffsrechten zu programmieren als eine mit wenigen.
Hinweis:	Die genannten Punkte sind allesamt „weiche" Kriterien. Es gibt seriöse Apps, die nur wenige davon erfüllen und unseriöse Apps, die fast alle erfüllen. In der Summe ergeben sie aber meistens ein korrektes Bild.

MOBILSICHER

Das Smartphone ist für viele die Schaltzentrale des täglichen Lebens: Ob Terminkalender, Kreditkarte, Stadtplan, Zeitung, Kamera, Musik-Player oder Ticket – im Handy ist alles digital an einem Platz.

Doch haben wir die Geräte wirklich im Griff? Wissen wir, mit welchen Unternehmen sie wann Kontakt aufnehmen und Informationen über uns versenden? Verstehen wir, wie zielgerichtete Werbung in Wahlkämpfen eingesetzt wird und was das mit unserer Facebook-App zu tun hat? Haben wir eine Ahnung, wer alles Zugriff auf unser Handy hat – Beziehungspartner*in, Chef*in oder Polizei? Erkennen wir die Maschen von Betrüger*innen, die längst auch in der Welt der Smartphones unterwegs sind?

Wir finden, zu einem selbstbestimmten Leben gehört, über die Schaltzentrale des eigenen Alltags selbst zu bestimmen. Das ist nicht nur möglich, es bringt auch Spaß und neue Perspektiven – denn die digitale Welt bietet viel mehr als nur den kommerziellen Mainstream. Deshalb sagen wir: „Holen wir uns die Macht zurück!“ – und fangen mit dem eigenen Handy an.

mobilsicher.de richtet sich an jede Person, die im Alltag ein Smartphone nutzt – ausdrücklich auch an Neulinge und Nicht-Expert*innen.

Egal, ob Sie zum ersten Mal ein Handy in Betrieb nehmen oder sich zu fortgeschrittenen Themen wie E-Mail-Verschlüsselung informieren wollen – bei uns ist für jede und jeden etwas dabei.

mobilsicher.de ist ein Kooperationsprojekt der gemeinnützigen Vereine iRights e.V. und ITUJ e.V. Finanziert wird es durch eine Förderung des Bundesministeriums der Justiz und für Verbraucherschutz und betrieben vom gemeinnützigen iRights e.V.

Weitere Informationen zu den Themen aus dieser Broschüre finden Sie auf unserer Webseite www.mobilsicher.de. Dort können Sie auch unseren Newsletter abonnieren und sich Anleitungen und Tipps ganz einfach per YouTube-Video ansehen.

mobilsicher.de

---

klicksafe
Die EU-Initiative

Die EU-Initiative klicksafe ist seit dem Jahr 2004 das nationale deutsche Awareness Centre im Verbund und in Zusammenarbeit mit weiteren 27 europäischen Partnern. Diese werden co-finanziert durch das CEF Telecom Programm der Europäischen Union. klicksafe wird gemeinsam von der LMK – medienanstalt rlp (Koordination) und der Landesanstalt für Medien NRW (LFM-NRW) umgesetzt. Außerdem koordiniert klicksafe den nationalen Safer Internet DE Verbund (www.saferinternet.de). Diesem gehören neben dem Awareness Centre klicksafe die Internet-Hotlines Internet-beschwerdestelle.de (durchgeführt von eco und FSM) und Jugendschutz.net sowie die Nummer gegen Kummer (Helpline) an. Ziel der europäischen Awareness Centres ist es, die Online-Kompetenz der Nutzer zu fördern und sie beim kompetenten und kritischen Umgang mit dem Internet und den neuen Medien zu unterstützen. Auf der Webseite www.klicksafe.de finden Nutzer eine Vielzahl von Informationen und Materialien zu digitalen Diensten und Themen.
Die Zielgruppen sind Lehrkräfte, Pädagogen, Eltern und Multiplikatoren.

www.klicksafe.de

Impressum

Konzeption und Texte:
Miriam Ruhenstroth
Gestaltung: Beate Autering, beworx.de

Verantwortlicher i. S. d. P.:
Matthias Spielkamp
mobilsicher.de
getragen vom iRights e.V.
Almstadtstr. 9/11, 10119 Berlin

redaktion@mobilsicher.de
www.mobilsicher.de

Eine Broschüre von

MOBILSICHER.DE

Das Infoportal für mehr Sicherheit auf Smartphone und Tablet.

Verständlich,
kompetent,
unabhängig.

Diese Broschüre wurde gefördert durch

Gefördert durch:

Bundesministerium der Justiz und für Verbraucherschutz

aufgrund eines Beschlusses des Deutschen Bundestages

klicksafe Die EU-Initiative