Smartphones souverän nutzen

Wie man im Handy-Dschungel die kontrolle behält

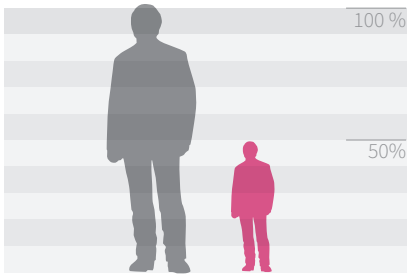
Hintergründe, Fakten und Praxiswissen für Schüler, Eltern und Lehrer

Mit Checklisten und praktischen Tipps für Übungen

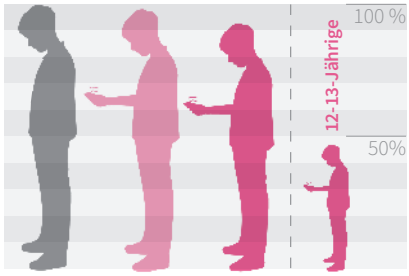
MOBILSICHER

Grußwort

50 % der Deutschen haben ein Smartphone (2014).

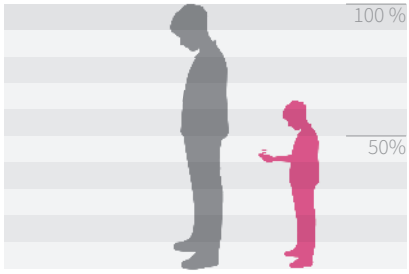


98 % der Jugendlichen zwischen 12 und 19 Jahren haben ein Handy, davon **92 %** Smartphones (Stand 2015). **47 %** der 6-bis-13-Jährigen haben ein Handy.



alle Jugendlichen
Jugendliche mit Handy
Jugendliche mit Smartphone

62 % der 12-bis-13-Jährigen haben eine Flatrate und können auch unterwegs ins Internet.



alle 12-13-Jährigen
12-13-Jährige mit Smartphone

Liebe Leserinnen, liebe Leser,

Ob WhatsApp oder Snapchat, Pokémon Go oder Spotify: Smartphones sind aus dem Alltag von Jugendlichen – und zunehmend auch Kindern – nicht wegzudenken. Sie sorgen vor allem für Spielspaß und Vernetzung mit anderen.

Wer den sinnvollen Umgang mit ihnen unterstützen möchte, muss aber auch die Risiken kennen: Kinder und Jugendliche kommen mit Hass und Gewalt in Kontakt oder tappen in Kostenfallen. Oder es geht einfach nur das Gerät verloren – und 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. Gibt es Handysucht überhaupt? Wie groß ist die Gefahr, online gemobbt oder verfolgt zu werden? 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 Projekt mobilsicher.de des Berliner Vereins iRights e.V., das vom Bundesministerium der Justiz und für Verbraucherschutz gefördert wird, bietet eine Handreichung speziell für Lehrerinnen und Lehrer, Eltern und Jugendliche. Wir freuen uns sehr, dass die Stiftung Berliner Sparkasse – von Bürgerinnen und Bürgern für Berlin dieses Projekt unterstützt. Sie hat es sich zum Ziel gesetzt, das Gemeinwohl in Berlin zu fördern. Die Bildung und Chancengleichheit von Kindern und Jugendlichen sind ihr dabei ein besonderes Anliegen. Dazu zählt auch die Förderung von Medienkompetenz.

Ich wünsche eine spannende und interessante Lektüre!

Gerd Billen

Staatssekretär im Bundesministerium der Justiz
und für Verbraucherschutz

Inhalt

Handystress und Handysucht

Pornografie und Sexting

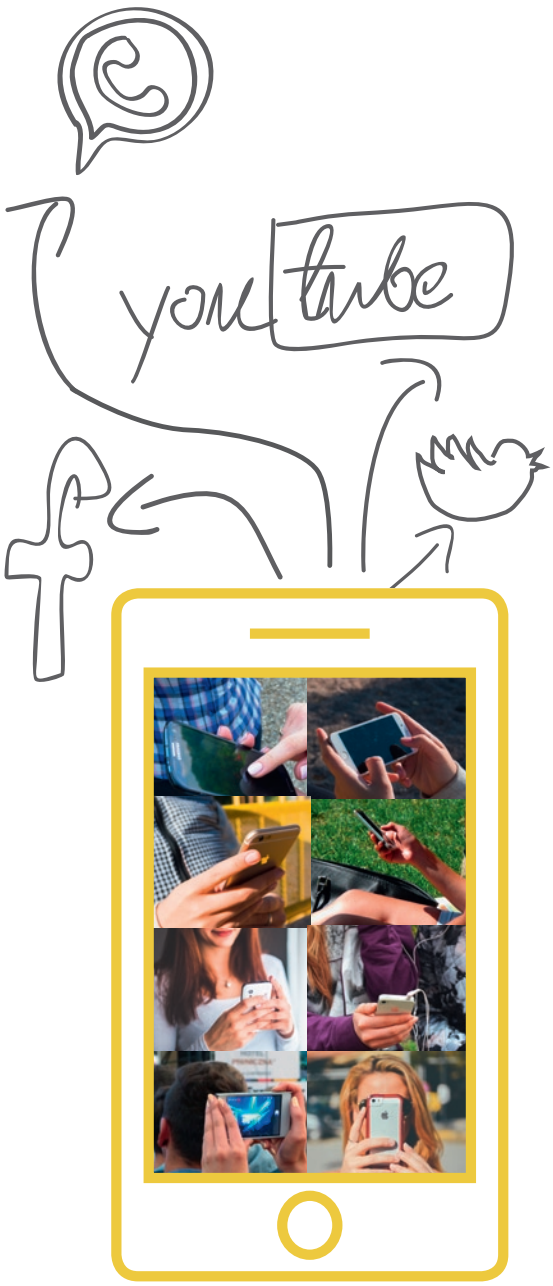
Hass, Gewalt, Volksverhetzung

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 Facebook 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 Altersgenossen 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 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 verschiedene suchtartig genutzte 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 und 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-5 wird vom US-amerikanischen Fachverband „American Psychiatric Association“ herausgegeben und gilt auch in Deutschland als Standardwerk für die Diagnose mentaler Erkrankungen.

Anerkannte klinische Diagnosekriterien nach DSM-5 gibt es bislang aber nur für die „internetbezogene Spielesucht“, also die Kategorie „Gaming“. Dabei ist es egal, ob die Betroffenen auf Computer, Konsole oder Smartphone spielen.

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.

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.

Eine „Handy-Sucht" im strengen Sinne gibt also nicht, weil alle diese Tätigkeiten auf Smartphone oder Computer stattfinden können. Da aber soziale Netzwerke und Messenger vorwiegend auf Mobilgeräten genutzt werden, sind diese Varianten stark mit der Verbreitung und Nutzung von Smartphones assoziiert.

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 fast ausschließlich Jungen und Männer betroffen. Bei den anderen Anwendungen ist das Geschlechterverhältnis in etwa ausgeglichen. 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. So setzen Betroffene eher wichtige Lebensgrundlagen, wie zum Beispiel den Job, aufs Spiel.

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.

Inzwischen gibt es solche anerkannten Diagnosekriterien (nach DSM-5) auch für die internetbezogene Spielesucht. Sie sind denen der substanzbezogenen Sucht sehr ähnlich.

Da viele Fachleute davon ausgehen, dass die Diagnose für die nicht spielebezogene Internetsucht ganz ähnlich aussehen werden, wollen wir sie hier vorstellen. Danach liegt eine internetbezogene Spielesucht dann vor, wenn fünf von diesen neun Kriterien über einen Zeitraum von zwölf Monaten erfüllt sind.

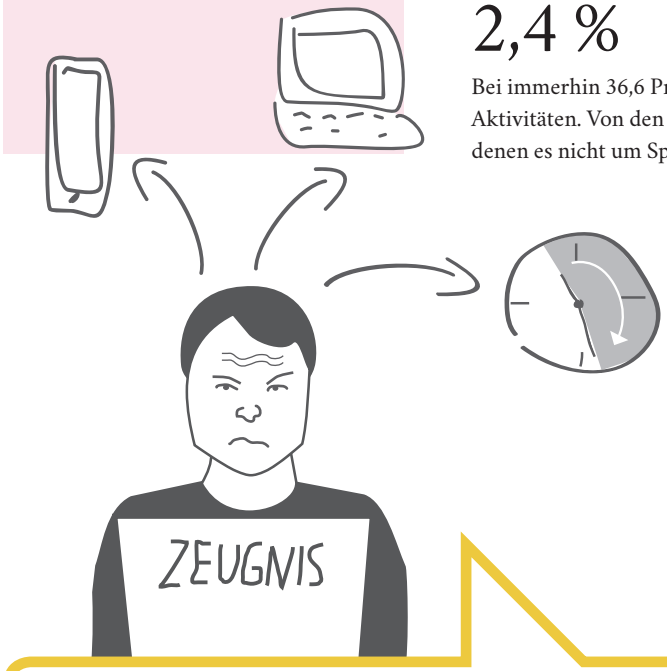
- Gedankliche Vereinnahmung: Betroffene beschäftigen sich in Gedanken ständig mit dem Spiel und haben ein starkes Verlangen danach weiterzuspielen.
- Entzugssymptome: Betroffene sind zum Beispiel nervös oder gereizt, wenn sie nicht spielen können.
- Toleranzentwicklung: Sie müssen immer mehr Zeit mit 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.
- Obwohl sie wissen, dass sich das Spielen negativ auf ihren Job oder die Schule auswirkt, können Betroffene nicht aufhören.

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?“



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

- 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.

Zahlen und Fakten

Der Medienpädagogische Forschungsverbund Südwest (mpfs) erhebt seit 1998 jährlich die Mediennutzung in Deutschland bei Jugendlichen zwischen 12 und 19 Jahren. In dieser sogenannten JIM-Studie von 2015 wurden 1.200 Jugendliche telefonisch befragt.

25 % der Befragten gaben an, dass sie häufig oder gelegentlich zu Hause Ärger wegen ihrer Handynutzung bekommen.

10 % der Befragten gaben an, dass sie häufig oder gelegentlich in der Schule Ärger wegen ihrer Handynutzung bekommen.

Die aktuellsten Zahlen zur Verbreitung von Internetabhängigkeit stammen von der PINTA und PINTA-DIARI-Studie, die im Auftrag des Bundesministeriums für Gesundheit an der Universität Lübeck von 2011 bis 2012 durchgeführt wurde. Darin wurden 15.000 Personen deutschlandweit befragt.

1 % der Deutschen zwischen 14 und 64 Jahren leiden danach an Internetsucht nach DSM-5 Kriterien.

2,4 % sind es bei Jugendlichen zwischen 14 und 24.

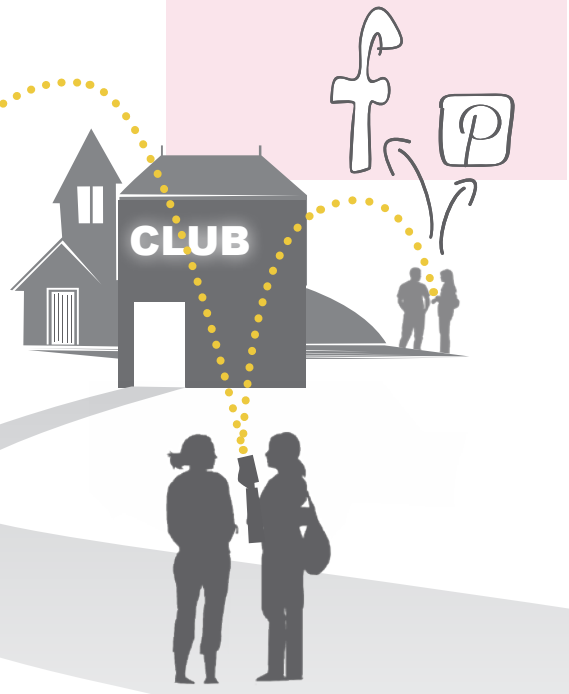
Bei immerhin 36,6 Prozent aller Betroffenen handelte es sich um spielebezogene Aktivitäten. Von den Spielern waren 90 Prozent männlich. Bei den Anwendungen, bei denen es nicht um Spiele geht, sind tendenziell etwas mehr Frauen betroffen.

Wichtige Begriffe

- **Phubbing:** Abgeleitet aus den englischen Wörtern „Phone“ und „to snub“, was so viel heißt wie „brüskieren, abblitzen lassen, rüffeln“. Wenn jemand im Gespräch oder am Esstisch auf sein Telefon schaut, anstatt sich mit seinem Gegenüber zu unterhalten, nennt man das „Phubbing“.
- **FoMo (Fear of Missing out):** Übersetzt „Angst, etwas zu verpassen“ oder „Angst, ausgeschlossen zu sein“. Ein Gefühl von Nervosität und sozialem Stress aufgrund der Vermutung, dass in sozialen Netzwerken und anderen Plattformen gerade interessante Dinge geschehen, die man verpassen könnte, wenn man nicht ständig online ist.

Hilfe und Beratung

- **Fachverband Medienabhängigkeit e.V.:** Dort gibt es Informationsmaterial, Referenten und eine umfassende Adressliste mit Beratungsangeboten deutschlandweit.



Vorbeugen und behandeln

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

Wissenschaftlich erprobte Vorbeugemaßnamen setzen an den Risikofaktoren an (siehe Kasten "Sucht: Wer ist gefährdet?"). Bei der Internetsucht würden Psychologen mit Betroffenen zum Beispiel trainieren, 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.

Vorbeugekonzepte gegen Internetsucht für Jugendliche, die auf wissenschaftlichen Erkenntnissen beruhen, werden in Deutschland derzeit entwickelt. Zum Beispiel arbeiten Wissenschaftler der pädagogischen Hochschule Heidelberg an einem Konzept für Schulen, mit dem besonders gefährdete Jugendliche im Vorfeld gestärkt werden sollen.

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

▷ Tipps und Übungen

Die meisten NutzerInnen 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.
- ▷ Online-Status in sozialen Netzwerken und Messengern ausschalten: Wenn keiner sehen kann, ob man online ist oder nicht, kann man sich mit einer Antwort auch mal Zeit lassen.
- ▷ Nutzung protokollieren: Oft merkt man nicht, wie viel Zeit man am Smartphone verbringt. Es gibt inzwischen Apps, die das anschaulich mitschneiden. An der Universität Bonn haben Wissenschaftler zum Beispiel die App „Menthal“ entwickelt, mit der man seine Handy-Nutzung kontrollieren kann. Die Daten werden ausschließlich für die Forschung verwendet. Andere Apps dieser Art finanzieren sich oft dadurch, dass sie Nutzerdaten an Werbefirmen verkaufen.

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 NutzerInnen 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 NutzerInnen 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. Manche Medienwissenschaftler sprechen schon von der „Generation Porno“.

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 einer Studie von 2009 führten Wissenschaftler vom Institut für Publizistik der Universität Mainz eine Onlinebefragung mit 352 Jugendlichen zwischen 16 und 19 Jahren zum Umgang mit Pornografie im Internet durch. Die Zahlen decken sich in etwa mit anderen Studien.

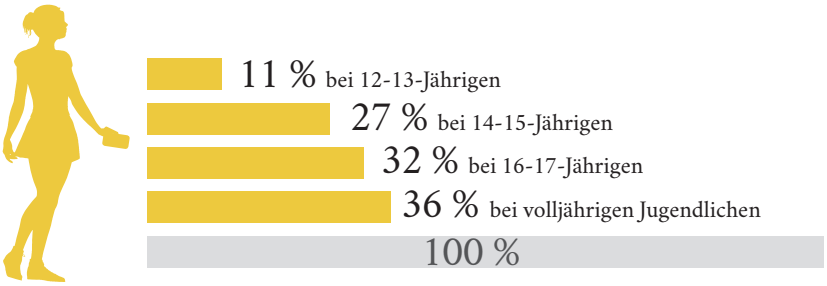
Mädchen		Jungen
33 %	haben schon pornografische Videoclips oder Filme im Internet angeschaut.	89 %
8 %	haben sexuell explizite Videoclips auf dem Smartphone angeschaut.	27 %
3 %	gaben an, fast täglich oder häufiger pornografische Videos und Filme anzusehen (auch Fernsehen).	47 %
25 %	haben sexuell explizite Videos oder Filme zumindest ab und zu gemeinsam mit Freunden angesehen (auch Fernsehen).	25 %

Wie in der Tabelle zu sehen ist, schauen sehr viel mehr Jungen pornografische Inhalte als Mädchen. Das durchschnittliche Einstiegsalter liegt bei 14 Jahren. Ein auffälliges Ergebnis verschiedener Studien ist, dass Jugendliche Pornografie oft nicht alleine, sondern mit Freunden oder dem Partner anschauen.

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

Neben dem reinen Konsum verschicken Jugendliche sexuell explizite Nachrichten – mit und ohne Bilder (sogenanntes Sexting). In der JIM-Studie 2014 gaben 27 Prozent der Befragten an, Sexting im Bekanntenkreis schon einmal mitbekommen zu haben. Dabei gibt es starke Altersunterschiede:



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 Juristen fällt darunter zum Beispiel auch, wenn man solches Material auf dem Handybildschirm anderen zeigt. Der bloße Besitz von pornografischen Materialien ist nicht strafbar.

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

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).

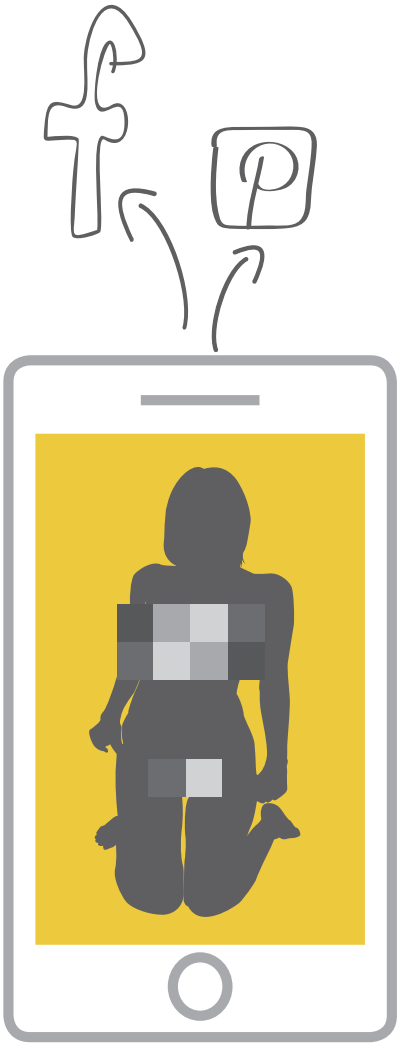
Jugendliche können sich in extremen Fällen auch strafbar machen, wenn sie pornografische Bilder oder Videos von sich selbst anfertigen. Für sie gilt in diesem Fall das Jugendstrafrecht. Kinder unter 14 Jahre sind hingegen schuldunfähig und werden nicht gerichtlich verfolgt.

Ist Porno-Konsum 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 sexuell verrohen könnte oder Wertevorstellungen von Liebe und Bindung verliert. Außerdem transportieren die meisten Pornos ein einseitiges 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.



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 zum Beispiel 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 Medienpädagogen 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 die Schuld zugewiesen wird – fälschlicherweise.

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 sich dabei für moralisch überlegen halten.

Anstelle von Sexting-Abstinenz empfiehlt es sich also eher, Jugendlichen den verantwortungsvollen Umgang mit Sexting zu vermitteln. Einvernehmliches Sexting sollte wie einvernehmlicher Sex toleriert werden. Dazu gehört, die Heranwachsenden vor sexuellen Übergriffen und Mobbing besser zu schützen und ihnen einvernehmliches Verhalten besser zu vermitteln und vorzuleben.

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

Hilfe und Beratung

- Anonyme und kostenlose Beratung durch Mitarbeiter 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
- Onlineforum für Jugendliche mit seriöser, kostenloser und anonymer Beratung von Experten.
  www.aok4you.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
- Beratung im Forum, per Chat und einzeln für Kinder und Jugendliche bis 21 Jahre, nicht nur zum Thema Liebe und Sexualität, sondern auch zu Themen wie Familie, Schule und Ausbildung.
  www.kids-hotline.de
- Anlaufstelle für Betroffene von sexualisierten Übergriffen und sexueller Gewalt sowie Informationen zu dem Thema.
  www.zartbitter.de

▷ 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.
- ▷ Finden Sie eine Sprache für das Thema Sexualität und Pornografie. Worüber gesprochen werden kann, das kann reflektiert werden.
- ▷ 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 NutzerInnen 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 gesperrt.
- ▷ Es gibt Suchmaschinen für Kinder, die nur für Kinder geeignete Webseiten als Ergebnisse anzeigen – zum Beispiel „FragFINN". Auf Smartphones und Tablets gibt es sie auch als Apps. Bei jüngeren Kindern sollte eine solche App den Browser ersetzen. Der Standard-Browser (Safari bei iOS, Chrome bei Android) kann deaktiviert werden.
- ▷ Speziell für iOS: Hier gibt es die Möglichkeit, einen Jugendschutzfilter für den Browser „Safari" einzurichten. Diese Funktion findet sich unter Einstellungen > Allgemein > Einschränkungen.

Für Pädagogen: Arbeitsmaterial

Das Landesmedienzentrum Baden-Württemberg hat Arbeitsblätter mit Übungen und Diskussionsleitfäden für den Unterricht zum Thema Pornografie und Sex im Internet vorbereitet. Zum Download:

www.lmz-bw.de/broschuere-lets-talk-about-porno.html

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.

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

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 „Cybermobbing“ 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.

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.

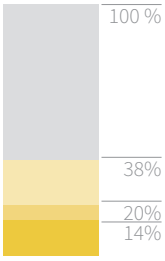
Auch das sogenannte Cyberstalking – hartnäckige Versuche der Kontaktaufnahme oder Verfolgung durch andere (Fremde, aber oft auch ehemalige Partner) – wird einfacher, wenn Menschen jederzeit digital erreichbar sind.

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 das Aufnehmen und das Verbreiten von solchem Material.

Zahlen und Fakten

Mobbing und unerlaubte Bildweitergabe



38 % der Internet-NutzerInnen haben schon einmal erlebt, dass jemand innerhalb des eigenen Bekanntenkreises online regelrecht fertiggemacht wurde.

20 % davon sind zwischen 18 und 19 Jahre alt.

14 % der Internet-NutzerInnen berichten, dass von ihnen peinliche oder beleidigende Videos und Bilder ohne vorherige Erlaubnis online gestellt wurden.

Quelle: JIM-Studie 2014

Weitere Informationen

- **Arbeitsgemeinschaft Kinder- und Jugendschutz der Landesstelle Nordrhein-Westfalen:** Hat unter anderem die Broschüre „Gewalt auf Handys“ herausgegeben, in der der Jurist Sebastian Gutknecht anschaulich die juristischen Hintergründe bei der Nutzung für Smartphones erklärt.
  www.handysektor.de/fileadmin/user_upload/downloads/Gewalt_auf_Handy_lfm.pdf

- **Hochschule der Medien Stuttgart:** Hier wurde die Studie „Gewalt im Web 2.0“ durchgeführt, in der Verbreitung und soziologische Hintergründe von Gewaltinhalten unter Jugendlichen untersucht werden.
  www.nlm.de/fileadmin/dateien/aktuell/Studie_Prof._Grimm.pdf

- **Klicksafe:** EU-finanziertes Informationsangebot zu Sicherheit und Jugendschutz im Internet. Hat unter anderem die Broschüre „Rechtsextremismus hat viele Gesichter“ herausgegeben, mit einem Zusatzmodul zum Thema speziell für Lehrkräfte.
  Zusatzmodul für Lehrkräfte
  www.klicksafe.de/rechtsextremismus/

Gewalt und Volksverhetzung

In einer Studie der Hochschule der Medien in Stuttgart von 2009 wurden 804 Jugendliche zwischen 12 und 19 Jahren zum Thema Gewalt im Internet befragt.

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 2015 registrierte das Kompetenzzentrum für Jugendschutz im Internet, Jugendschutz.net, 6.000 Verstöße gegen das Jugendschutzgesetz.

15 % davon kamen aus dem Bereich politischer Extremismus. Sowohl islamistischer als auch rechter Extremismus nehmen laut Jugendschutz.net zu.

Rechtliches

Gewaltdarstellung

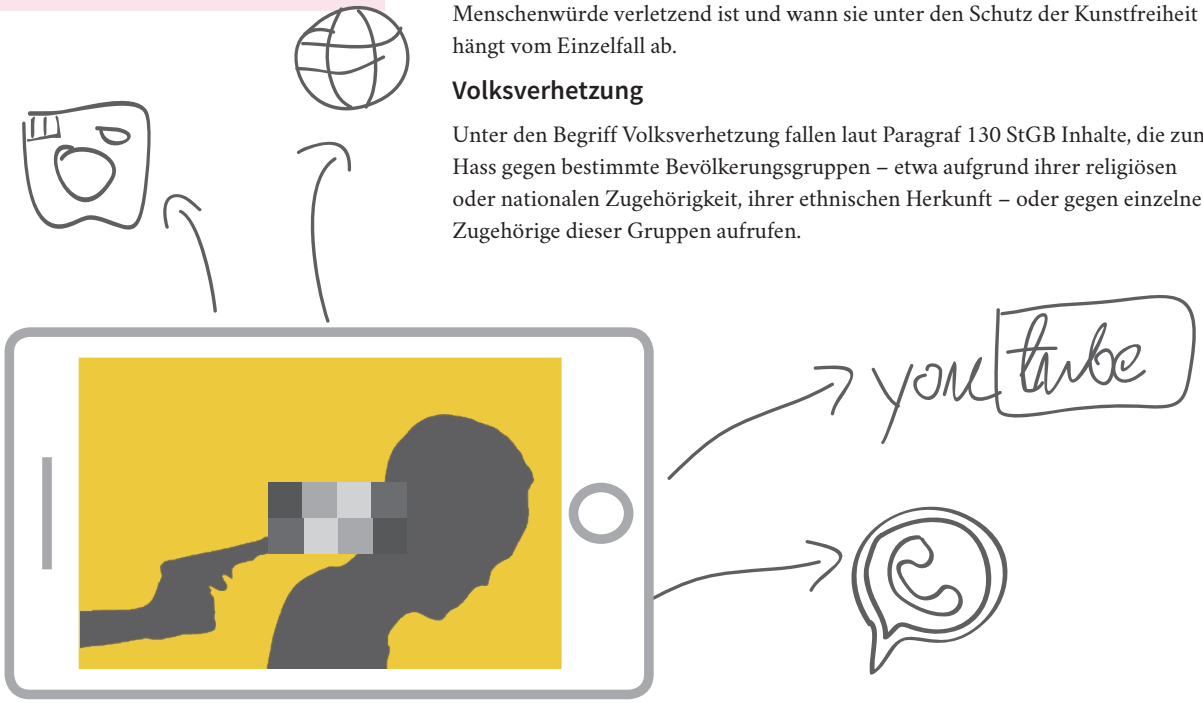
Unter die strafbaren Gewaltdarstellungen fällt laut Paragraf 131 Strafgesetzbuch (StGB) jeder Inhalt, der „grausame oder sonst unmenschliche Gewalttätigkeiten gegen Menschen oder menschenähnliche Wesen in einer Art schildert, die eine Verherrlichung oder Verharmlosung solcher Gewalttätigkeiten ausdrückt 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.

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.



Hilfe und Beratung

www.nummergegenkummer.de

Das Angebot bietet telefonische Beratung für Eltern, Kinder und Jugendliche sowie Online-Beratung für Kinder und Jugendliche. Nicht nur zu Sorgen oder Problemen aus dem Onlinebereich, sondern aus allen Lebensbereichen, sei es Schule, Stress mit den Eltern oder Sexualität.

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“ (§201a Strafgesetzbuch) auf Antrag strafrechtlich verfolgt.

Bei einer Veröffentlichung im Internet haben Betroffene zudem 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 Erziehungsberechtigten gestellt werden. Dies setzt voraus, dass die betroffenen Jugendlichen sich ihren Eltern anvertrauen können.

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

▷ 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 NutzerInnen ungewollt auf erschreckende Inhalte stoßen.

- Bei Youtube kann man im Menü eine Option wählen, die „Eingeschränkter Modus“ heißt. Dadurch werden sexuelle und gewalthaltige Inhalte nicht angezeigt.
- Es gibt Suchmaschinen, die nur für Kinder geeignete Webseiten als Ergebnisse anzeigen – zum Beispiel „FragFINN“. Viele dieser Angebote gibt es auch als App für Tablet oder Smartphone. Bei jüngeren Kindern sollte eine solche App den Browser ersetzen. Der Standard-Browser (Safari bei iOS, Chrome bei Android) kann deaktiviert werden.
- Speziell für iOS: Hier gibt es die Möglichkeit, einen Jugendschutzfilter für den Browser „Safari“ einzurichten. Diese Funktion findet sich unter Einstellungen > Allgemein > Einschränkungen.

Sozialkompetenz stärken

Um Mobbing und Cybermobbing zu verhindern, muss vor allem der sozialverträgliche Umgang miteinander gestärkt und geschult werden. Übungsmaterialien dazu gibt es zum Beispiel bei Klicksafe, einem umfangreichen Informationsangebot in deutscher Sprache, das seit 1999 von der EU-Kommission finanziert wird.

- Ratgeber „Cybermobbing“ www.klicksafe.de/service/materialien/broschueren-ratgeber/ratgeber-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-Anbietern, Videoplattformen und den Betreibern sozialer Netzwerke können rechtsextreme Beiträge, Hassaufrufe, Mobbing oder gewalthaltige Inhalte gemeldet werden. 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. Unter dem Video, das gemeldet werden soll, klicken Sie auf das Fähnchen-Symbol und wählen den Meldegrund aus. In einem weiteren Schritt können Sie das Video „zur Überprüfung einreichen".

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

Bei Gruppen: Auf der Profilseite der Gruppe, die gemeldet werden soll, klicken Sie auf das Dreieck neben dem Button „Nachricht senden" am rechten Bildrand. Es öffnet sich ein Fenster, in dem Sie „Seite melden" auswählen können. Folgen Sie dann dem Dialog.

Bei einzelnen Postings: Oben rechts in der Ecke gibt es bei jedem Post auf Facebook ein Symbol, das aussieht wie ein etwas breiteres V. 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.

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 gemeldet werden.
- Internet-Beschwerdestelle: wird vom Industrieverband eco und der Freiwilligen Selbstkontrolle Multimedia-Diensteanbieter e.V. (FSM) betrieben. Auch dort kann man anstößige Inhalte melden. 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. Läuft in Deutschland auf etwa 79 Prozent aller Smartphones (Q2 2016).
- **iOS:** Betriebssystem für mobile Geräte der Firma Apple. Läuft ausschließlich auf iPhones und iPads von Apple. Marktanteil in Deutschland etwa 14 Prozent (Q2 2016).
- **IP-Adresse:** Jedes Gerät, das mit dem Internet verbunden ist, hat eine eindeutige IP-Adresse. Die IP-Adresse gibt ungefähre Auskunft über den Standort – also in welcher Stadt man sich befindet. Der Internet-Provider kann der IP-Adresse auch den Inhaber des Internet-Anschlusses zuordnen.

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 NutzerInnen nicht erkennbar.

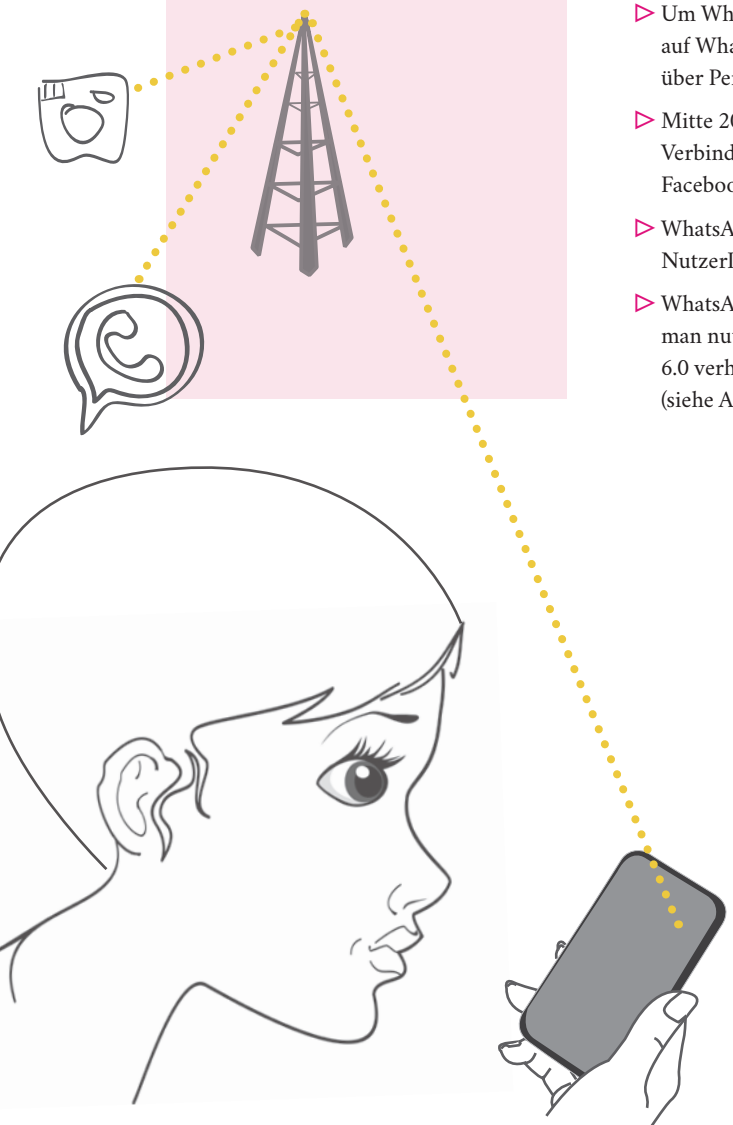
Die meisten NutzerInnen wissen in der Regel wenig über die Hersteller ihrer Apps und welches Geschäftsmodell dahintersteht. Nicht selten besteht es leider darin, Nutzerdaten zu sammeln und zu verkaufen.

In der Befragung des Medienpädagogischen Forschungsverbundes Südwest von 2015 (JIM-Studie) sollten die Jugendlichen auch 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 großem Abstand. Diese fünf Apps sind WhatsApp, Facebook Messenger, Instagram, Snapchat und Youtube.

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.

Im Internet Surfen: Auch Browser sind Apps

- Etwa 82 Prozent der Jugendlichen surfen laut JIM-Studie 2015 regelmäßig mit dem Smartphone im Internet. Eine App wurde dabei nicht genannt.
- Viele NutzerInnen nehmen den Browser, mit dem sie ins Internet gehen, nicht als App wahr. Tatsächlich ist es aber eine, die für Privatsphäre und Sicherheit beim Surfen sehr wichtig ist. Und: Man kann den Browser genauso wie auf dem PC aussuchen und austauschen.
- Der Browser Firefox von Mozilla (für Android) schützt die Privatsphäre von NutzerInnen besser als die Standard-App. Wie man Firefox richtig konfiguriert, lesen Sie auf https://mobilsicher.de/ratgeber/firefox-konfigurieren-android.



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 2015 nannten neunzig Prozent der befragten Jugendlichen WhatsApp als eine der drei wichtigsten Apps auf ihrem Smartphone, 33 Prozent nannten den Facebook-Messenger.

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 Anfang 2016 eine Milliarde NutzerInnen.
- Seit April 2016 werden alle Nachrichten Ende-zu-Ende verschlüsselt versendet. WhatsApp beziehungsweise Facebook kann die Nachrichten selber nicht entschlüsseln.
- Um mit jemandem zu kommunizieren, muss man dessen Handynummer kennen.
- Die Nutzung ist laut allgemeinen Geschäftsbedingungen erst ab 16 Jahren erlaubt.

Privatsphäre WhatsApp

- Die App verlangt Zugriff auf Kamera, Kontakte, Standort, Mikrofon, Telefon, SMS, Internet.
- 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.
- Mitte 2016 kündigte WhatsApp an, alle Nutzerdaten, also Telefonnummer, Verbindungsdaten, Statusnachrichten und vieles mehr, mit dem Mutterkonzern Facebook zu teilen.
- WhatsApp räumt sich das Recht ein, die Telefonnummer und E-Mail-Adresse von NutzerInnen an Dritte weiterzugeben.
- 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).

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. Details unter mobilsicher.de
- **AppGuard:** Mit AppGuard der Firma SRT kann man auch auf älteren Android-Versionen die Zugriffsrechte von übergriffigen Apps einschränken. Details unter mobilsicher.de
- **Obscuracam:** App zum Entfernen von Metadaten aus Bildern. Details unter mobilsicher.de
- **Messenger:** Es gibt einige sichere Messenger, die kaum Daten sammeln, zum Beispiel „Wire“, „Signal“ oder „Telegram“. Details unter mobilsicher.de
- **Firewall (Nur Android):** Egal ob alte oder neue Android-Version: Fast alle Apps erhalten inzwischen 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 NoRoot Firewall oder NetGuard. Details unter mobilsicher.de

Eckdaten Facebook-Messenger

- Betreiber und Hersteller ist Facebook Inc. Firmensitz ist in Kalifornien, USA.
- Der Facebook-Messenger hatte nach Firmenangaben Anfang 2016 eine Milliarde NutzerInnen.
- Die Verschlüsselung der Nachrichten ist seit 2016 möglich, muss aber manuell aktiviert werden.
- Um mit anderen zu kommunizieren, muss man keine Handynummer kennen, sondern nur den Namen, mit dem sie im Messenger angemeldet sind.
- Die Nutzung ist laut allgemeinen Geschäftsbedingungen ab 13 Jahren erlaubt.

Facebook-Messenger Privatsphäre

- Die App verlangt Zugriff auf Kalender, Kamera, Kontakte, Mikrofon, SMS, Standort, Telefon, Internet.
- Für den Messenger gilt die Datenschutzerklärung von Facebook. Das heißt, Facebook sammelt alle Inhalte, die über den Messenger gesendet werden, und wertet sie aus.
- Informationen über NutzerInnen können mit Informationen aus anderen Diensten der Facebook-Gruppe (etwa Facebook-, Instagram- oder WhatsApp) oder zugekauften Informationen verknüpft werden.
- Erfasst werden Verbindungsdaten, IP-Adresse, Gerätetyp, Betriebssystem 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)“.
- Facebook verfolgt auch das Surfverhalten außerhalb der Facebook-Seiten. Wer eine Webseite besucht, die einen Facebook-Button enthält, der teilt Facebook diesen Besuch mit.

Bilder teilen

In der JIM-Studie 2015 nannten dreißig 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 NutzerInnen teilen kann. 16 Prozent nannten „Snapchat“, einen Dienst zum Versenden von Bildern.

Eckdaten Instagram

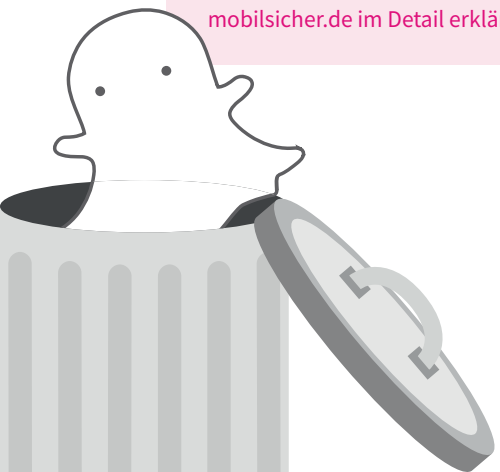
- Betreiber ist die „Instagram LLC“, die seit 2012 im Besitz von Facebook ist. Firmensitz ist in Kalifornien, USA.
- Laut Firmenangabe nutzten im Juni 2016 300 Millionen NutzerInnen die App täglich.
- NutzerInnen können sich mit E-Mail-Adresse, Facebook-Konto oder Telefonnummer anmelden.
- Laut Geschäftsbedingungen darf Instagram ab 13 Jahren genutzt werden.
- Der Dienst blendet auch Werbeanzeigen ein.

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.



Instagram Privatsphäre

- Die App verlangt Zugriff auf Kamera, Kontakte, Mikrofon, SMS, Standort, Telefon, Internet.
- In der Standardeinstellung wird das eigene Adressbuch regelmäßig zu den Instagram-Servern übertragen und dort gespeichert.
- Verbindungsdaten, IP-Adresse, Browser und Gerätetyp sowie Standortdaten werden gespeichert.
- Die App teilt Nutzerinformationen mit Unternehmen der Facebook-Gruppe.
- Die App teilt Ortsdaten, Gerätekennung und Verbindungsdaten mit Dritten.
- Personen auf Bildern können von anderen NutzerInnen mit Namen versehen werden und sind dadurch leichter auffindbar.

Tipps zur sicheren Nutzung:

- Man kann das eigene Instagram-Konto auf „privat“ stellen. Dadurch können nur NutzerInnen die Bilder sehen, die Sie vorher ausgewählt haben.
- 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.
- Achtung Metadaten: Auch wenn den Fotos keine Ortsangabe angefügt wird, ist der Aufnahmeort eventuell in der so genannten Exif-Datei des Bildes vorhanden. Wer sich das Bild dann von Ihrem Instagram-Account herunterlädt, kann den Ort aus der Exif-Datei auslesen. Mit der App „Obscuracam“ kann man die Metadaten vorher entfernen.

Eckdaten Snapchat

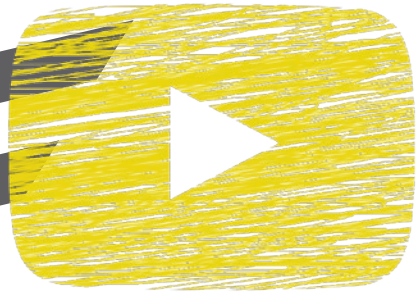
- Betreiber ist Snap Inc., Firmensitz ist in Kalifornien, USA.
- Snapchat hat 150 Millionen aktive NutzerInnen pro Tag (Stand September 2016).
- Snapchat ist ein Dienst, mit dem Bilder und kurze Videos vom Smartphone oder Tablet an andere NutzerInnen des Dienstes über das Internet verschickt werden können. 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

- Die App verlangt Zugriff auf Kamera, Kontakte, Mikrofon, SMS, Standort, Telefon und Internet.
- NutzerInnen müssen sich mit Namen und Geburtsdatum registrieren.
- Erfasst Gerätetyp, Betriebssystem, Browser, die eigene Telefonnummer, Mobilfunkprovider, Standort und sämtliche Nutzungsdaten, also was man wann an wen gepostet hat, welche Bilder man angesehen hat, mit wem man Kontakt hat.
- Wertet alle diese Informationen aus, auch Ortsdaten, um interessenbezogene Werbung und Dienste anzuzeigen.
- Speichert alle versendeten Bilder und anderen Inhalte auf seinen Servern, auch wenn sie für Nutzer oder Nutzerinnen gleich wieder verschwinden.
- Räumt sich für den Dienst „Live Stories“ auch ein, den Namen des Nutzers zu veröffentlichen.

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.



Videos schauen

Die App des Videoportals Youtube gehört laut JIM-Studie 2015 für 23 Prozent der Befragten zu den drei wichtigsten Apps. Youtube ist ein Video-Portal im Internet. NutzerInnen 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 gibt es mehr als eine Milliarde eindeutige NutzerInnen pro Monat (Stand 2013).

Youtube Privatsphäre

- Die App verlangt Zugriffsrechte auf Kamera, Kontakte, Mikrofon und Internet.
- 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.
- Android: In der Standard-Einstellung wird der Such- und Wiedergabe-Verlauf 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:

- In den Aktivitätseinstellungen kann man deaktivieren, dass Youtube den Suchverlauf und den Wiedergabeverlauf speichert.
- Nutzt man Youtube auf dem Browser, empfiehlt es sich, den Browser-Verlauf regelmäßig zu löschen.

Zugriffsrechte anzeigen und einschränken

Ob Adressbuch, Anrufliste, oder Ortsdaten – Smartphones speichern zahlreiche sensible Daten. Zusätzlich ermitteln eingebaute Sensoren ständig weitere Daten wie Umgebungstemperatur, Höhe oder den Neigungswinkel des Gerätes.

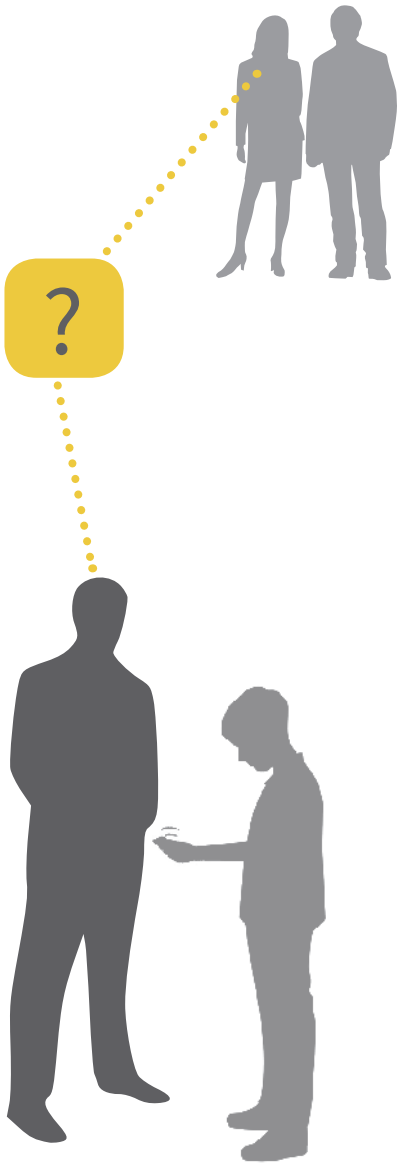
Aus diesen Daten lassen sich viele Rückschlüsse über NutzerInnen ziehen. Zum Beispiel, wo sie arbeiten, mit wem sie befreundet sind, wie alt und wie zahlungskräftig sie sind. Für solche Nutzerdaten existiert ein eigener Markt. Viele Apps, vor allem kostenlose Spiele, werden eigens dafür programmiert, um Nutzerdaten zu sammeln, die anschließend verkauft werden.

Daher sollte nicht jede App Zugriff auf alle Daten und Funktionen des Gerätes bekommen. Die Betriebssysteme von Smartphones – die meistgenutzten sind Android und iOS – sind so programmiert, dass Apps besondere Berechtigungen brauchen, um auf die bestimmte Funktionen und Informationen des Gerätes zugreifen zu können.

- iOS: NutzerInnen von Apple-Geräten können einzelnen Apps einzelne Zugriffsrechte entziehen. Die Punkte finden sich unter „Einstellungen“. Dort findet man eine Liste der Apps. Wenn man sie anklickt, erscheinen die Zugriffsrechte, die man bearbeiten kann.
- Android: Ab der Version 6.0 (Marshmallow) kann man ebenfalls einzelne Rechte einschränken. Aber Achtung, das neue System hat seine Tücken. Einige kritische Berechtigungen, wie zum Beispiel den Zugriff auf Ortsdaten und Adressbuch, kann man zwar verbieten. Alle Apps bekommen aber automatisch Zugriff auf das Internet. Diese Berechtigung wird nicht mehr angezeigt.
- Android 5.1 und älter: NutzerInnen haben nicht viel Einfluss auf die Rechtevergabe: Entweder stimmen sie bei der Installation allen abgefragten Rechten zu oder verzichten auf die Installation der App.

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

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



▷ Tipps und Übungen

Eltern und Lehrer: Einfach mal aus probieren

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 auf Ihrem Gerät, legen Sie ein Test-Konto an und versuchen Sie sich mit ein paar Posts. Tun Sie sich mit anderen Eltern oder Freunden zusammen, um der Erfahrung der Jugendlichen möglichst nahezukommen.

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 braucht.

Kleine App-Werkstatt

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

- ▷ Alle TeilnehmerInnen lassen sich anzeigen, wie viele Apps auf ihrem Gerät installiert sind.
- ▷ Bei wie vielen Apps ist der Hersteller/Betreiber bekannt?
- ▷ Bei wie vielen Apps ist die Funktion bekannt?
- ▷ Welche Merkmale sollte eine „gute“ App haben? (In Sinne von Datenschutz, Transparenz, Sicherheit, Vertrauenswürdigkeit)

Welche Apps nutzen die TeilnehmerInnen für

- ▷ das Surfen im Internet
- ▷ die Suche im Internet
- ▷ Nachrichten senden (Messenger)
- ▷ E-Mail
- ▷ den Kalender
- ▷ die Foto-Verwaltung

- ▷ 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/Ixquick, DuckDuckGo
- ▷ Nachrichten senden: Wire, Telegram, Signal
- ▷ Mail: K9 (Nur Android)
- ▷ Kalender: Etar (Nur Android)
- ▷ Foto-Verwaltung: LeafPic (Nur Android)

Details zu diesen Apps finden Sie online bei mobilsicher.de in dem Beitrag „Vorinstallierte Apps ersetzen“.

Wichtige Begriffe

- **IMEI:** Sie identifiziert jedes Mobilfunk-Gerät weltweit eindeutig. Sie wird beim Kontakt zum Mobilfunknetz an den Netzbetreiber übertragen. Einige Netzbetreiber sperren Geräte anhand der IMEI, wenn diese als gestohlen gemeldet werden (in Deutschland derzeit nur Vodafone).
  Die Polizei kann sichergestellte Geräte anhand der IMEI eindeutig identifizieren. 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 sehr effektiver Schutz gegen Diebstahl ist der sogenannte Kill-Switch oder die „Aktivierungssperre“. Ein Smartphone lässt sich damit nur in Betrieb nehmen, wenn der Nutzer oder die Nutzerin einen entsprechenden Code eingibt. Beim iPhone ist das zum Beispiel die Apple-ID.
  Apple hatte im englischsprachigen Raum 2013 eine Kill-Switch-Funktion eingeführt, die standardmäßig aktiv ist. Da die Geräte selbst nach dem Zurücksetzen auf Werkseinstellungen nicht ohne die Apple-ID in Betrieb genommen werden können, sind sie für Diebe wertlos.
  Die Diebstahlquote für Smartphones fiel im Jahr nach der Einführung in London um 50 Prozent.
  Im deutschsprachigen Raum ist die Funktion bei iPhones und auch bei einigen Android-Geräten verfügbar, aber nicht standardmäßig aktiv.

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 Zeitgenossen ernsthaften Schaden anrichten können. Das kann von gekaperten Online-Konten über teure Handyrechnungen bis hin zu Erpressung führen.

Die meisten NutzerInnen sind sich nicht bewusst, was mit einem geklauten Handy alles angestellt werden kann, wenn es nicht vernünftig gesichert ist.

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 wie ein persönliches Tagebuch fungieren. Wer sein Smartphone unversperrt auf dem Küchentisch, der Schulbank oder im Büro liegen lässt, macht sich gegenüber neugierigen Klassenkameraden, Kollegen oder Geschwistern verletzlich. 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

236.000 Smartphones wurden 2014 in Deutschland als gestohlen gemeldet.
Die Dunkelziffer dürfte noch höher sein. (Studie von Deutscher Telekom und dem Softwarehersteller Lookout)

14 % aller Handynutzer haben ihr Gerät schon einmal verloren. (Umfrage des IT-Dachverbands Bitkom von 2015)

Laut einer nicht repräsentativen Umfrage aus den USA von 2012 ist die Wahrscheinlichkeit, ein verlorenes Gerät zurückzubekommen, nicht sehr groß:

50 % aller Finder geben ein Smartphone nicht zurück.

89 % aller gefundenen Smartphones werden vom Finder nach persönlichen Daten durchsucht.

60 % der Finder lasen E-Mails und sahen sich die Konten bei sozialen Netzwerken der Smartphone-Besitzer an.

Nach einer repräsentativen Umfrage des Branchenverbandes Bitkom von 2016 scheint der Blick auf ein fremdes Smartphone verbreitet zu sein:

27% der Deutschen gaben an, schon einmal heimlich in ein fremdes Smartphone geschaut zu haben.

28% wollten nicht verraten, ob sie das schon einmal getan haben.

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 Notdienste und die Polizei mit Gerichtsbeschluss durchführen.

Was passiert mit gestohlenen Handys?

In der Regel landen gestohlene Geräte auf dem Gebrauchtwarenmarkt, nachdem sie auf die 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 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

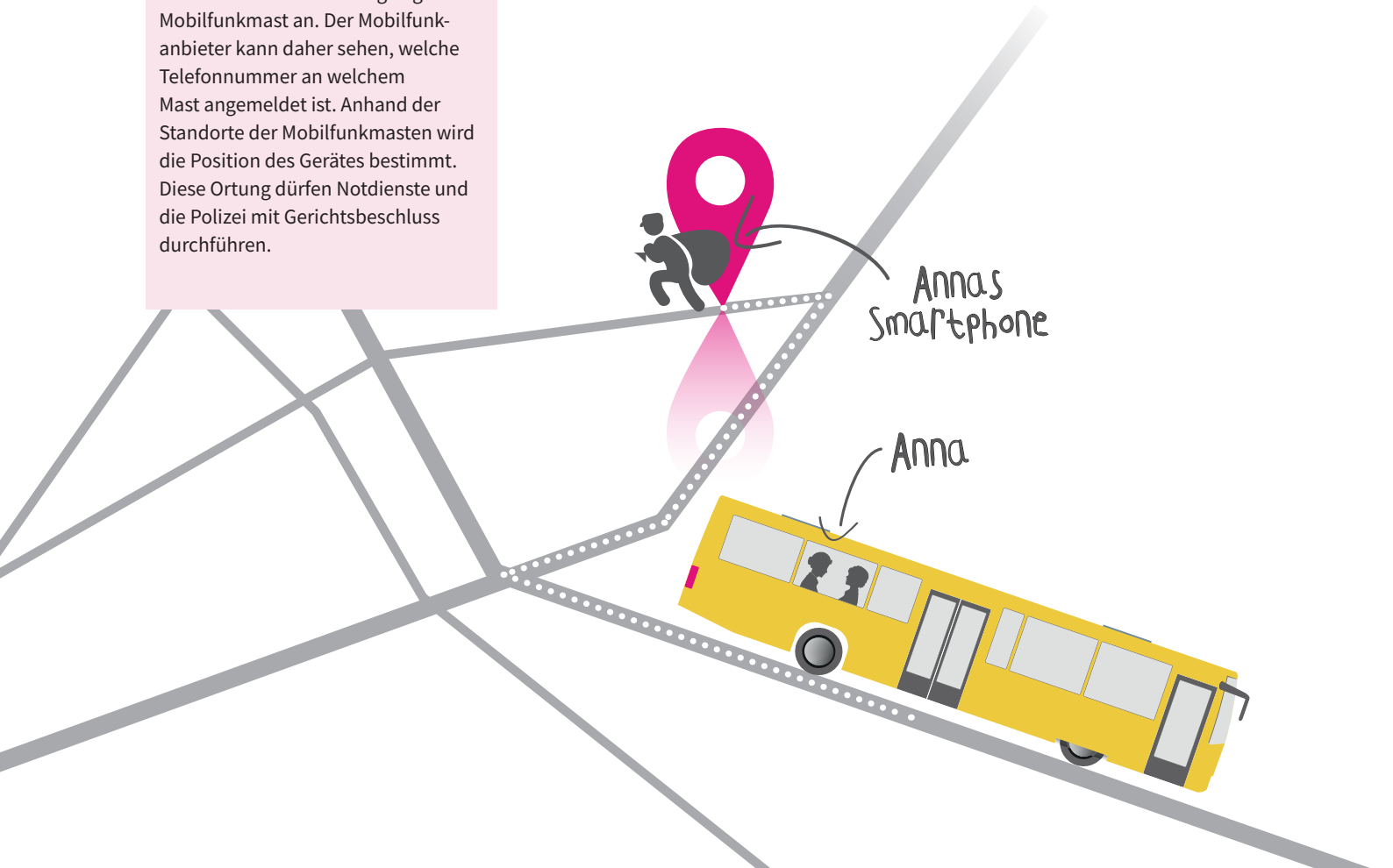
Die E-Mail-Adresse ist nicht nur zum Austausch von Nachrichten wichtig, sondern auch für die Anmeldung bei Online-Diensten. Wer ein Facebook-, Twitter-, oder Snapchat-Konto eröffnet, muss dabei eine E-Mail-Adresse angeben. An diese Adresse wird bei der Registrierung eine E-Mail mit einem Link geschickt,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

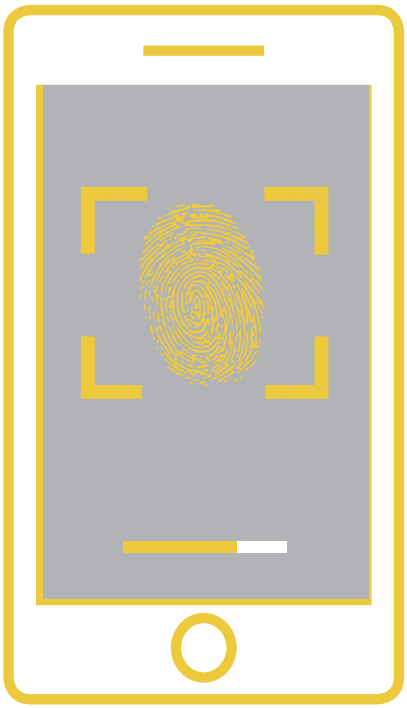
Wenn man sein Passwort vergisst, wird der Link für das neue Passwort auch an die registrierte E-Mail-Adresse geschickt. Fast alle Online-Dienste nutzen diese Funktion.

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-, Google- 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 einzurichten. 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. Für 2015 war es die Kombination „123456". An vierter Stelle kam „password".

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 stärker akzeptiert.

Inzwischen gibt es zahlreiche Laptops und Smartphones mit Fingerabdruckscanner auf dem Markt. Sie bieten eine einfache Alternative, damit nur berechtigte NutzerInnen auf ein Gerät zugreifen können. In der Testphase sind auch Verfahren wie Bilderkennung via Kamera oder Stimmerkennung.

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. Solange NutzerInnen unsichere Passwörter benutzen, bieten sie aber zusätzliche Sicherheit.

Große Hoffnung setzt man auf Algorithmen, die das typische Bewegungsmuster von NutzerInnen erkennen sollen, zum Beispiel, wenn man auf dem Bildschirm wischt. Diese Methode dürfte schwieriger zu fälschen sein, ist aber noch nicht ausgereift.

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

Diebstahl-Schutz

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 der „Android-Device-Manager" vorinstalliert. Die App von Google fragt den Standort des Gerätes regelmäßig ab und sendet ihn an einen Server von Google.

NutzerInnen, die sich in ihrem Google-Konto eingeloggt haben, können diese Standortdaten einsehen. Dort können sie nachträglich auch eine Bildschirmsperre für ein Gerät installieren, falls es noch keine hat. Ist das Gerät verschwunden, können sie so gegebenenfalls feststellen, wo es sich befindet, und es sichern. 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 im Internet angezeigt zu bekommen oder eine Sperre einzurichten.

Viele Hersteller von Anti-Viren-Software haben inzwischen auch Apps zur Diebstahl-sicherung herausgebracht. Einige davon haben den Vorteil, dass sie den Standort auch per SMS mitteilen können und damit auch geortet werden können, wenn keine Internetverbindung besteht.

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 Polizei-Meldung 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.**

Bei all diesen Lösungen muss man beachten, dass der Hersteller der entsprechenden Sicherheitssoftware auf jeden Fall 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. Die Ortung findet also auf dem Gerät selbst statt und wird dann an den Nutzer oder die Nutzerin geschickt.

Weder Polizei noch Provider suchen ein gestohlenes Smartphone über Funkzellenortung (GSM, siehe Kasten). 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 Ausdrucken.

▷ Fragen Sie die TeilnehmerInnen, welche Sicherheitsmaßnahmen sie auf ihrem Gerät aktiviert haben.

Lösungsvorschlag: In unserem Merkblatt „Smartphone weg – vorbeugen“ am Ende dieses Heftes haben wir die wichtigsten Maßnahmen aufgelistet. Einige Punkte können Sie sofort erledigen.

Übung zwei: Passwort-Werkstatt

▷ Fragen Sie die TeilnehmerInnen, 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, s durch 5 usw. Das ergibt dann: e@6Ec!e@uNcR. Das ist ein sehr sicheres Passwort.

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

Vorsicht, falsche Freunde

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

Dabei muss der Nutzer oder die Nutzerin seine Telefonnummer eingeben und bekommt daraufhin eine SMS mit einem Code. Diesen Code muss er wiederum für den Kauf eingeben.

Es gibt seit einigen Jahren einen Trick, um NutzerInnen zu veranlassen, ihre Mobilfunknummer und den zugesendeten Code einer TAN-SMS 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 schreibt dann etwas wie „Kannst du mir den Code schicken? Ich erklär es dir später.“

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

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 Playstore oder in Apples App-Store zu hinterlegen und damit zum Beispiel Apps zu kaufen oder sogenannte In-App-Käufe zu tätigen.

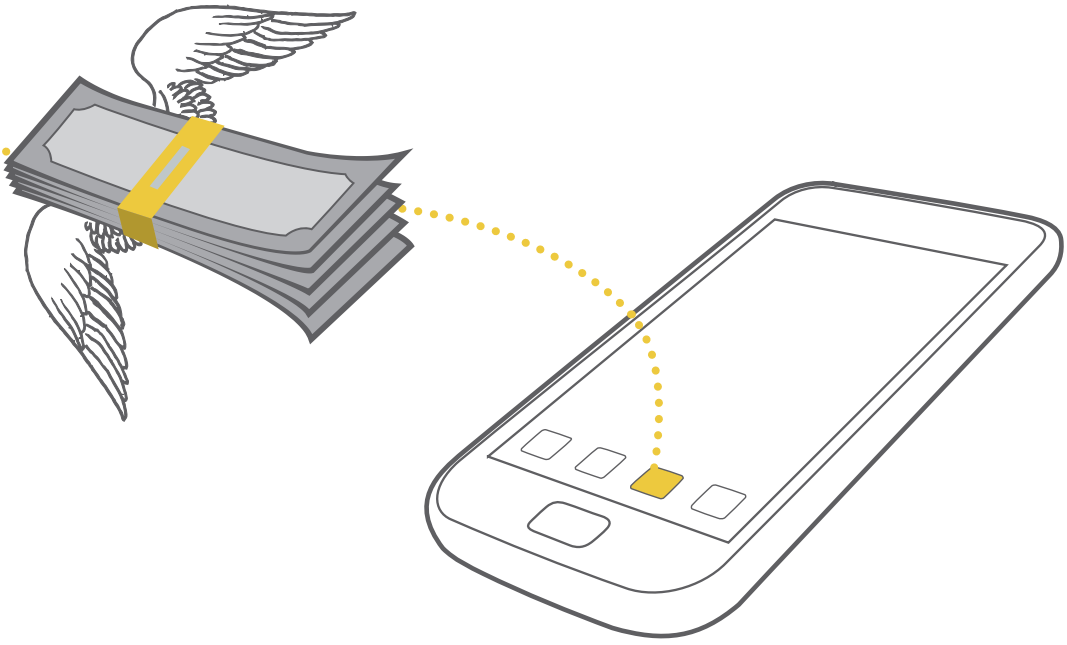
Dabei kann man leicht den Überblick über die Kosten verlieren. Wo verbergen sich die Kostenfallen und wie kann man sich dagegen schützen?

Direct 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 Billing“ – direkte Abrechnung.

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 auch Beträge für Dinge auf, die man nie bewusst gekauft hat. In der Vergangenheit sind solche Fälle oft aufgetreten, weil manche Anbieter auf ihren Webseiten nur unzureichend gekennzeichnet haben, dass durch Antippen ein Kauf abgeschlossen wird – teils bewusst, teils aus Unkenntnis.



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 und Rechtsanwälte. Dabei geht man allerdings das Risiko ein, dass der Mobilfunkbetreiber den Anschluss sperrt. Normalerweise dürfen die Anbieter 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.

Seit Juni 2016 findet der eigentliche Kaufabschluss beim Direct Billing bei fast allen Angeboten auf einer Extraseite statt, die vom Mobilfunkanbieter selbst gestaltet und kontrolliert wird. So soll sichergestellt werden, dass die gesetzlichen Regelungen zur korrekten Kennzeichnung eingehalten werden. Die Maßnahme ist das Ergebnis einer gemeinsamen Initiative der Mobilfunkanbieter, deren Ziel es ist, die Drittanbieter-Problematik zu beseitigen. Nach Angaben der Anbieter ging die Zahl der Beschwerden wegen Drittanbieter-Kosten seitdem um rund 50 Prozent zurück.

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)
- **0137** (Massenverkehrsdienste, Preisansage vorgeschrieben)
- **0180** (Servicedienste, höchstens 14 Cent/Minute aus dt. Festnetz, 20 Cent aus Handynetz)
- **012** (Neuartige Dienste oder Kurzwahldienste, Preisansage ab 2 Euro pro Minute vorgeschrieben)

Zeiten in der Warteschleife dürfen nicht abgerechnet werden. Unter Kurzwahldienste fallen zum Beispiel SMS, die man an eine fünfstellige Nummer schickt.

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 aber 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 NutzerInnen, 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 NutzerInnen „Juwelen" kaufen können, um den Spielfortschritt zu beschleunigen.

Inzwischen kennzeichnen die Betreiber der App-Stores 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 die vielen Apps für Kinder, bei denen mit wenigen Klicks In-App-Käufe getätigt werden können.

Hilfe und Beratung

- **Verbraucherzentrale Nordrhein-Westfalen:** Hier gibt es einen Musterbrief für eine solche Kündigung. www.verbraucherzentrale.nrw/media218141A.pdf
- **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).

Rechtliches

Es gibt eindeutige gesetzliche Regelungen dazu, wie ein gültiger Vertrag beim Direct 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.
- 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 Billing kaufen die Mobilfunkanbieter die Forderungen vom Inhalteanbieter auf. Rechtlich gesehen sind sie auch der Ansprechpartner, wenn es Streitigkeiten gibt. In der Vergangenheit haben die Mobilfunkanbieter NutzerInnen aber immer wieder an die Inhalteanbieter verwiesen. Inzwischen geben sie zumindest offiziell an, dass sie das nicht mehr so praktizieren.

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.
- **Drittanbieter-Sperre einrichten:** Damit Drittanbieter nicht direkt über die Mobilfunkrechnung Dienstleistungen abrechnen können, kann man bei seinem Mobilfunkanbieter eine sogenannte Drittanbietersperre aktivieren. Die verschiedenen Gesellschaften haben dabei unterschiedliche Verfahren. Bei Fragen dazu muss man sich an seinen Mobilfunkbetreiber wenden.
- **Regelmäßig die Rechnung überprüfen:** Klingt banal, aber viele tun es nicht: Regelmäßig überprüfen, ob die Posten auf der Handyrechnung ihre Richtigkeit haben. 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 Googles Play-Store kann man ein Passwort einrichten, das jedes Mal eingegeben werden muss, wenn man etwas im Play-Store kauft. Das geht in der Play-Store-App unter:
  Menü (drei horizontale Striche oben links) → Einstellungen→ Authentifizierung für Käufe erforderlich
  Bei iOS finden Sie die Funktion unter:
  Einstellungen→ Allgemein→ Einschränkungen.
- **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.

Merkzettel Handydiebstahl: Vorbeugen

Geht ein Mobilgerät verloren, ist meist nicht nur der Kaufwert weg, sondern auch viele wichtige Daten. Mit diesen Tipps sind 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“.
Drittanbieter-Sperre einrichten	In der Regel genügt dafür ein formloses Schreiben per Mail an den Provider. Damit sind Sie vor Kosten durch Sonderrufnummern oder Direct Billing effektiv geschützt.
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. Wer danach das Passwort verliert, kommt nicht mehr an seine Daten. iPhones sind standardmäßig verschlüsselt, NutzerInnen 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 eventuell auch die Bildschirmsperre Ihres Telefons umgehen oder ändern. Verwenden Sie ein starkes Passwort oder Zwei-Faktor-Authentifizierung.
Mailadresse zur Wiederherstellung	Richten Sie für Google-Konto oder iCloud eine Mailadresse 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.
Optional: Sicherheitsfunktionen oder -Apps nutzen	Sie können damit Ihr Gerät im Verlustfall orten und sperren. Android: Android Device Manager, iOS: Mein iPhone suchen
Wichtige Informationen notieren	IMEI-Nummer (eindeutige Identifikationsnummer des Gerätes): Wird angezeigt, wenn Sie *#06# wählen. Codes für Ihre Sicherheits-Apps, falls Sie welche verwenden, etwa das Codewort für die Sperr-SMS. Zentraler Kartensperrdienst: 116 116, oder aus dem Ausland: +49 30 4050 4050.

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 zur Fernsperrung 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 den Android Geräte-Manager nutzen, rufen Sie diese Webseite auf: www.google.com/android/devicemanager. Sie benötigen dafür die Login-Daten Ihres Google-Kontos. 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 andere Mailkonten sichern	Loggen Sie sich in Ihr Google-Konto ein und ändern Sie das Passwort. Falls Sie E-Mail-Konten auf Ihrem Smartphone eingerichtet haben, ändern Sie auch die Passwörter dieser Konten.
Optional: Kreditkarten sperren	Falls Sie keinen Zugriff mehr auf Ihre Mail-Konten haben, weil die Passwörter bereits geändert wurden, dann sperren Sie alle Bankkonten und Kreditkarten, die Sie im Internet für Bezahlvorgänge verwendet haben, und auch Ihr Paypal-Konto.
Internet-Konten sichern	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 NutzerIn nicht 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?
Geschäftsmodell:	Womit verdient der Hersteller Geld? Wie werden die Kosten für das Bereitstellen der App bzw. 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 NutzerInnen bewertet werden. Oft lohnt sich ein Blick in die Kommentare, um von verbreiteten Problemen mit der App zu erfahren.
Open Source:	Es ist immer von Vorteil, wenn der Programmcode einer App für jedermann zugänglich ist. Der Fachbegriff dafür ist Open Source (Offene Quellen). So können unabhängige Fachleute den Code auf Schwachstellen und versteckte Funktionen überprüfen. Der F-Droid-Store für Android verbreitet 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.

MOBILSICHER

Wer sich Fragen zur Sicherheit bei Mobilgeräten stellt, erlebt viele Überraschungen. Denn im Gegensatz zu einfachen Mobiltelefonen sind Smartphones und Tablets Computer im Taschenformat. Durch Kameras, Ortsbestimmung, Beschleunigungssensoren und vieles mehr haben sie meist einen Funktionsumfang, der den von PCs bei weitem übertrifft.

Für Nutzerinnen und Nutzer hat das Vor- und Nachteile. Zwar können sie sich von ihrem Smartphone durch fremde Städte navigieren lassen, zugleich wissen sie oft nicht, welche Daten das Gerät gerade wohin überträgt. Auch die Datensicherung ist ein Problem: Wer Kontakte, Kalenderdaten und E-Mails in der Jackentasche mit sich herumträgt, aber weder eine Zugangssperre eingerichtet noch eine Datensicherung hat, steht beim Verlust des Telefons oder Tablets vor riesigen Problemen.

Wir wollen nicht mit erhobenem Zeigefinger über das Risiko von Smartphones belehren, sondern sachlich erläutern, wo mögliche Gefahren liegen – und vor allem zeigen, wie man sie verringern kann. Das tun wir mit Hintergrundartikeln, die erläutern, wie App-Stores und Browser funktionieren, welche Daten Telefone sammeln und vieles mehr. In Ratgebern und Bilderstrecken erklären wir Schritt für Schritt, welche Einstellungen Nutzerinnen und Nutzer vornehmen können, um ihre Sicherheit zu erhöhen. Mit unseren Checklisten zeigen wir schnell und verständlich auf, welche Informationen Sie im Blick haben sollten.

mobilsicher.de wird gefördert vom Bundesministerium der Justiz und für Verbraucherschutz und betrieben vom gemeinnützigen iRights e.V.

mobilsicher.de

Stiftung Berliner Sparkasse
von Bürgerinnen und Bürgern für Berlin

Die „Stiftung Berliner Sparkasse – von Bürgerinnen und Bürgern in Berlin“ ist eine gemeinnützige Einrichtung, die sich für das Gemeinwohl der Stadt Berlin engagiert. Sie versteht sich als eine fördernde Institution, die die ihr zur Verfügung stehenden Mittel ausschließlich für Projekte einsetzt, die innerhalb der Stadt Berlin initiiert und realisiert werden. Die Stiftung unterstützt engagierte Bürgerinnen und Bürgern und deren Initiativen und bietet die Möglichkeit, sich finanziell und ehrenamtlich langfristig zu engagieren.

Mit den Aktivitäten der Stiftung zeigt die Berliner Sparkasse, die seit 1818 im öffentlichen Auftrag arbeitet, ihr gesellschaftliches Engagement. Für ein öffentlich-rechtliches Kreditinstitut wie die Berliner Sparkasse ist nachhaltiges soziales Engagement ein wesentlicher Bestandteil der unternehmerischen Identität.

Die Satzung der Stiftung Berliner Sparkasse lässt ein breites Spektrum sozialer, kultureller, ökologischer sowie bildungs- und erziehungsbezogener Aktivitäten zu. In diesem Rahmen setzt die Stiftung in ihrer konkreten Arbeit Schwerpunkte bei der Förderung von Kindern und Jugendlichen.

Die Stiftung finanziert sich durch Spenden und die Erträge aus dem Stiftungskapital, dessen langfristiger Aufbau durch Zustiftungen die Kontinuität der Stiftungsarbeit für gemeinnützige und mildtätige Zwecke gewährleistet.

Die Ziele und die Aktivitäten der Stiftung Berliner Sparkasse werden transparent gemacht und öffentlich dargestellt.

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