Datenschutz TIPPS

für Jugendliche

So sind Deine Daten im internet sicher

Kinder- und Jugendtelefon
0800-111 0 333
nummergegenkummer.de

klicksafe.de

Mehr Sicherheit im Internet durch Medienkompetenz

Datenschutz TiPPS

für Jugendliche

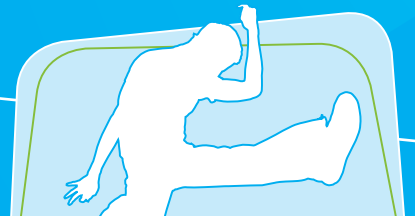
Du glaubst, Datenschutz ist langweilig und geht Dich nichts an? Lass Dich vom Gegenteil überzeugen!

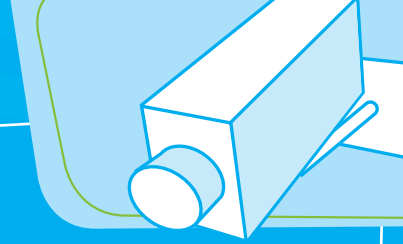
Wenn Du im Internet surfst, hinterlässt Du Datenspuren. Manches verrätst Du freiwillig. Häufig merkst Du aber auch gar nicht, dass persönliche Daten von Dir gesammelt werden. Zum Beispiel greifen viele Apps (Spiele oder kleine Programme) während der Nutzung auf Deine Kontakte, Dein Telefonbuch oder andere Daten zu.

Aber nicht alle Informationen über Dich und Dein Leben gehen jeden etwas an, oder?

Wir sagen Dir, was Du für den Schutz Deiner Daten tun kannst.

Dein klicksafe-Team





1

Datenschutz macht Sinn

Persönliche Daten, zum Beispiel Deine Adresse, Dein Alter oder Deine Interessen, nennt man auch **personenbezogene Daten**. Sie verraten viel über Dich und sind kostbar. Für Unternehmen bedeuten sie bares Geld, und sie können von anderen missbraucht werden.

Man könnte denken: Was soll's, ich habe doch nichts zu verbergen! Aber das Internet hat ein langes Gedächtnis. Und Dinge, die Du heute gut findest, gefallen Dir in ein paar Jahren vielleicht überhaupt nicht mehr. Aber im Internet stehen sie dann immer noch.

Das heißt aber nicht, dass Du ganz auf persönliche Infos im Netz verzichten musst. Entscheidend ist die richtige Auswahl. Überlege **vor** dem Hochladen: Wie willst Du Dich im Internet (im schlimmsten Fall) auf ewig präsentieren? Auch die „Oma-Regel" kann Dir bei der Entscheidung helfen: Was würde meine Oma dazu sagen?

- Die schöne neue Welt der Überwachung www.panopti.com.onreact.com
- Infos zum Thema „Datenschutz, Apps und Smartphones" gibt es auf www.handysektor.de.

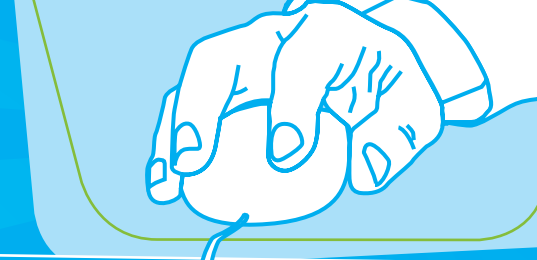
2 Datenschutz ist Dein gutes Recht

Durch das **Recht auf informationelle Selbstbestimmung** sind Deine persönlichen Daten (Name, Adresse, ...) sogar per Gesetz geschützt. Das bedeutet: Niemand darf diese Daten **ohne** Deine Einwilligung speichern, veröffentlichen oder weitergeben. Ausnahmen gibt es für einige staatliche Einrichtungen, wie zum Beispiel Meldeämter oder die Polizei.

Was aber gilt für Fotos und Filme? Hier gibt es das **Recht am eigenen Bild**: Du entscheidest, welche Bilder von Dir veröffentlicht werden dürfen. Ein Bekannter darf also nicht einfach so ein Bild von Dir in einem Sozialen Netzwerk hochladen.

Übrigens: Bist Du jünger als 12 Jahre, musst Du Deine Eltern (oder Erziehungsberechtigten) vor dem Hochladen eines Fotos fragen. Aber auch danach solltest Du Dir vor dem Hochladen überlegen, was das Bild über Dich aussagt und ob es Dir in ein paar Jahren vielleicht peinlich sein könnte.

- www.checked4you.de – Deine Rechte im Web (Klick im Bereich „Themen“ unter dem Punkt „Computer + Internet“ auf „Internet“.)



3 Sei fair mit den Daten anderer

Denk nicht nur an Dich, beachte auch die Rechte anderer! Also keine Bilder, Filme oder private Infos von Freunden, Bekannten oder anderen Personen ins Netz stellen – außer Du hast ihre Erlaubnis. Wenn das nicht der Fall ist, dann lass es! Das ist auch ein Zeichen von **Respekt**.

Auch die Info, wo Du Dich gerade befindest, ist kostbar. Willst Du Deinen Aufenthaltsort trotzdem im Internet veröffentlichen, solltest Du Dich begleitende Freunde vorher fragen, ob Du sie mit angeben darfst.

Absolut verboten ist es, falsche Daten über jemanden zu veröffentlichen. Verletze nicht die Rechte anderer – egal ob im Internet oder in der wirklichen Welt.

- Unter www.irights.info findest Du weitere Infos zum Thema „Urheberrecht in der digitalen Welt“.
- Auf www.chatiquette.de werden Tipps und Benimmregeln fürs Chatten vorgestellt.

4

Sei ein Datenprofi in Sozialen Netzwerken

Für den Schutz Deiner Privatsphäre bist Du auch selbst verantwortlich. Achte darauf, wie Du Dich im Netz zeigst!

- Ein Foto darf ruhig auch mal lustig sein. Allzu **peinliche** oder **beleidigende** Fotos oder Meinungen haben in Sozialen Netzwerken aber nichts zu suchen. Sie können auch Jahre später wieder im Netz auftauchen und Dich sogar den Ausbildungsplatz kosten.
- Überlege auch, was eine **Gruppenmitgliedschaft** über Dich aussagt. Die Gruppe „Saufen bis der Arzt kommt“ ist keine gute Werbung für Dich. Hassgruppen, in denen andere gezielt beleidigt werden, gehen gar nicht.
- Sei sorgsam mit Deinen **Profil-Daten**: Lass Anschrift, Telefon- oder ICQ-Nummern weg. Sie sind nicht nötig, wenn Du Dich mit anderen austauschst. Auch Deine private E-Mail-Adresse solltest Du nicht jedem geben.
- Überprüfe regelmäßig Deine **Privatsphäre-Einstellungen**. Hier helfen Dir die klicksafe-Leitfäden (siehe unten).
- Prüfe genau, wem Du freien Zugang zu Deinen **privaten** Fotos und Daten gibst. Du weißt nie, was sie mit den Informationen machen!

- Die „Leitfäden für die Kommunikation im Netz“ zeigen Dir, wie Du Deine Daten in Sozialen Netzwerken schützen kannst: www.klicksafe.de/materialien
- Zum persönlichen Schutz kannst Du auch Dein Profilfoto witzig verändern: www.netzcheckers.de (Klick auf „Workshops“, dann auf „Profilbilder und Icons“.)
- Flyer „Big brother is watching you!“ Download unter: www.jugendinfo.de/pass-auf-dich-auf

5

Das Internet vergisst nicht

Im Internet veröffentlichte Infos, Filme oder Fotos sind ab da nicht mehr privat. Einmal im Netz, beginnen Deine Daten ein **Eigenleben**. Sie verbreiten sich, gelangen in Suchmaschinen und Online-Archive. Sie werden von anderen kopiert und weitergereicht. Alles wieder rückgängig machen und löschen? Nahezu unmöglich. Daher: **Vorher** überlegen, was wirklich alle von Dir wissen dürfen!

Wenn Du ein Soziales Netzwerk nicht mehr nutzen willst, dann solltest Du Deine Mitgliedschaft beenden und Deine Profildaten löschen. So erschwerst Du das Auffinden Deiner Daten.

- Das Internet-Archiv „WayBack Machine“ speichert Webseiten als Zeitdokumente dauerhaft ab www.archive.org
- Videos „Think Before You Post“ www.smiley-ev.de/think_before_you_post.php
- Videos auf www.klicksafe.de/spots

6 Elektronische Daten-Spuren hinterlässt Du unbemerkt

- Technische Daten werden automatisch übertragen, ohne dass Du es merkst.
  Zwei Beispiele:
  - Jeder Computer im Internet hat eine **IP-Nummer**. Das ist eine Art „Telefonnummer für das Internet“. Damit erkennen Experten wann, wie lange und auf welchen Seiten Du im Netz unterwegs warst. Über diese Nummer werden zum Beispiel illegale Musikdownloads ermittelt.
  - Du besuchst die Seite Deines Lieblings-Stars. Später siehst Du auf einer anderen Seite Werbung für seine neue CD. Wie kommt das? Schuld daran können **Cookies** (wörtlich „Kekse“) sein. Cookies sind kleine Dateien, die auf Deinem Rechner gespeichert werden. Sie merken sich genau, welche Seiten Du Dir angeschaut hast. So können Unternehmen Dich beim Surfen beobachten und herausfinden, welche Interessen Du hast.

Mehr Tipps zum Thema „Cookies“ findest Du auf www.klicksafe.de (Suchbegriffe „Cookies und Spyware“).

7 Nutze Nicknames und surfe unerkannt

- Gib Dir einen guten **Nick** („Decknamen“), wenn Du im Internet surfst. Sei hierbei erfinderisch! Der Nick sollte Deinem richtigen Namen nicht zu ähnlich sein oder Dein Alter enthalten. Verwende ihn zum Beispiel in Blogs, Chats und Foren. Verstecke Dich aber nicht hinter Deinem Nick oder gib Dich als jemand anderer aus, um andere gezielt zu beleidigen. Das ist unfair und kann bestraft werden!

Je mehr Du im Web aktiv unterwegs bist, umso sicherer ist es, wenn Du verschiedene Nicks nutzt. So bietest Du weniger Angriffsfläche für Beleidigungen, Abzocke und anderen Datenmissbrauch.

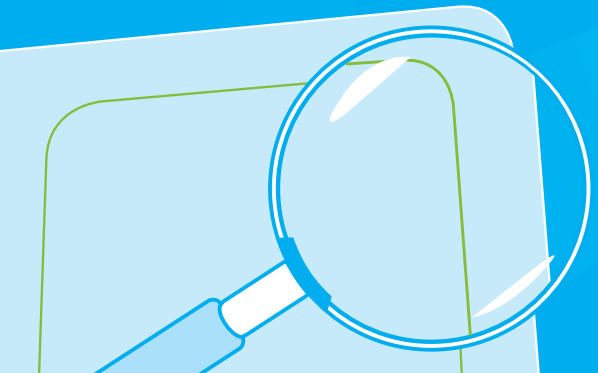
8 Behalte die Kontrolle über Deine Daten

Je mehr Daten Du von Dir verrätst, umso weniger Kontrolle hast Du darüber. **Datensparsamkeit** zahlt sich aus und schützt vor bösen Überraschungen. Hast Du Deine Daten (noch) im Griff?

Manchmal haben aber auch andere etwas über Dich veröffentlicht. Wie steht's um Deinen **Online-Ruf**?

- Gib Deinen Namen in verschiedene Suchmaschinen ein.
- Prüf die Profile und Fotoalben Deiner Freunde, wie Du dort erscheinst.

Personensuchmaschinen: www.yasni.de www.123people.de



9 Die AGBs – Was der Anbieter mit Deinen Daten machen darf

Oft schwer zu lesen, aber superwichtig: Das sind die AGBs, die Allgemeinen Geschäftsbedingungen eines Internet-Angebots. Sie enthalten auch eine **Datenschutzerklärung**. Hier erfährst Du, was mit Deinen Daten passiert, also was gespeichert, weitergegeben oder für Werbung genutzt wird.

Mit Deiner Anmeldung stimmst Du den AGBs automatisch zu! Schau Dir die AGBs deshalb **vorher** genau an. Wenn Du sie nicht verstehst, dann hole Dir Hilfe. Im Zweifel lieber auf eine Anmeldung verzichten – auch wenn es häufig schwerfällt.

Hier **zwei Beispiele** von vielen – Schon gewusst?

- Viele **Apps** (kurz für „Applications", also Programme) in Sozialen Netzwerken oder auf Handys greifen auf Deine privaten Daten zu. So können Freundeslisten, Deine Interessen, Dein Telefonbuch und weitere Daten während der Nutzung an den Hersteller geschickt werden.
- Viele kostenlose **E-Mail-Anbieter** lesen die Inhalte Deiner E-Mails nach Schlüsselwörtern aus, um Dir dazu passende Werbung zu senden.

Auf www.watchyourweb.de findest Du unter „Unsere Themen – Handysicherheit" auch Infos zu „Handy-Apps und Datenschutz".

10 Man macht sich ein genaues Bild von Dir

Unternehmen wollen möglichst viel von Dir erfahren. Sie haben ein Interesse daran, die Klicks und Angaben, die Du auf verschiedenen Seiten gemacht hast, zu verknüpfen.

Alle Daten, die sich über Dich finden lassen, können zu einem **Nutzerprofil** zusammengestellt werden. So können Unternehmen Dir passende Werbung zeigen, oder Dich mit Werbemails zuschütten. Denn wen man gut kennt, den kann man zielgenau umwerben. Diese **personalisierte Werbung** ist häufig so geschickt, dass Du gar nicht merkst, wie man Dich vom Kauf bestimmter Produkte überzeugen will.

- Infos und Tipps zum Thema „Datenschutz im Internet“: www.datenparty.de
- Mehr Infos zum Thema „Werbung“ gibt es auf www.klicksafe.de (Klick auf „Themen“, dann unten links auf „Werbung“).

11 Vor Datenmissbrauch ist niemand geschützt

Wenn Du im Internet unerwünschte Daten, Infos oder Bilder von Dir findest, dann gehe dagegen vor. Sage auch Deinen Eltern oder älteren Geschwistern Bescheid, damit Dir diese helfen können.

- Weißt Du, wer die Infos oder Bilder im Internet veröffentlicht hat? Dann bitte diese Person, die Inhalte so schnell wie möglich zu löschen. Nenn am besten auch ein Datum, bis zu dem dies erledigt sein soll.
- Wenn dies nichts bringt, informiere den Betreiber der Seite und bitte um Löschung (Du findest die Kontaktdaten im Impressum der Internetseite oder über www.whois.net und www.denic.de). In Sozialen Netzwerken gibt es hierfür spezielle Melde-Buttons.
- Die „Datenschutz-Aufsichtsbehörden der Länder“ (siehe unten) können Dir bei Datenschutzverletzungen ebenfalls mit Rat und Tat zur Seite stehen.
- In schlimmen Fällen (schwere Beleidigungen, problematische Bilder, die schnell entfernt werden sollen) kannst Du auch die Polizei einschalten.
- Bei verbotenen oder jugendgefährdenden Inhalten (z. B. pornografische Bilder) helfen Dir die Beschwerdestellen www.jugendschutz.net und www.internet-beschwerdestelle.de.

! Als Beweis solltest Du einen **Screenshot** („Foto“ vom Bildschirm) machen. Drücke hierzu die Taste „Druck“ auf Deiner Tastatur, füge das Bild mit den Tasten „STRG“ + „V“ in ein Bildbearbeitungsprogramm ein und speichere es ab.

! Sag Deinen Freunden und Bekannten Bescheid, wenn Du im Internet komische oder peinliche Fotos und andere Infos von ihnen findest.

- Die Adressen der Datenschutz-Aufsichtsbehörden findest Du auf www.bfdi.bund.de (Klick auf „Datenschutz“, „Anschriften und Links“ dann auf „Aufsichtsbehörden für den nicht-öffentlichen Bereich“).
- Virtuelles Datenschutzbüro www.datenschutz.de

12

Sicherheitstipps – So schützt Du Deine Daten

- Benutze **sichere Passwörter** (mindestens 8-stellig, Mischung aus Groß- und Kleinschreibung, Ziffern und Sonderzeichen) und nicht immer das gleiche. Ein Passwort sollte nicht leicht zu erraten sein (also nicht der Name Deines Haustieres oder Dein Spitzname). Merksätze können Dir dabei helfen, die Passwörter nicht zu vergessen.
- Gib Deine Passwörter nicht weiter. So verhinderst Du, dass Fremde auf wichtige Daten von Dir zugreifen können.
- Installiere ein **Anti-Virenprogramm** und aktualisiere es regelmäßig.
- Schütze Deinen Computer mit einer **Firewall** („Brandwand"). Eine Firewall schützt vor Angriffen und unberechtigten Zugriffen aus dem Internet und sollte nie ausgeschaltet werden.
- Sichere Dein **WLAN-Netzwerk** über eine verschlüsselte Verbindung (am besten WPA2). Wenn Du unterwegs kabellos surfst, verschicke möglichst keine wichtigen Daten.
- Schalte WLAN und Bluetooth aus, wenn Du sie nicht brauchst.
- Führe regelmäßig **Sicherheitsupdates** Deines Betriebssystems durch. Am besten stellst Du es so ein, dass Du wichtige Updates automatisch erhältst. So werden Sicherheitslücken geschlossen.

- Öffne keine E-Mails mit **unbekanntem** Absender, vor allem keine Datei-Anhänge.
- **Antworte nicht** auf unerwünschte E-Mails. Weitere nervige Mails wären die Folge!
- Am besten legst Du Dir zwei verschiedene **E-Mail-Adressen** zu. Eine gibst Du nur an gute Freunde und Bekannte weiter. Die andere verwendest Du für Anmeldungen, Online-Shopping und so weiter.

- www.handysektor.de: Infos zum Thema „Sicherheit in mobilen Netzen"
- www.klicksafe.de: Unter „Themen – Datenschutz – Grundlagenwissen" findest Du weitere Infos und ein spannendes Quiz zu diesem Flyer. Nimmst Du die Herausforderung an?

Bist Du ein Datenprofi im Internet?

Mach das Quiz unter
www.klicksafe.de/quiz

Die Initiative klicksafe ist ein Projekt im Rahmen des Programms „Mehr Sicherheit im Internet“ (Safer Internet Programme) der Europäischen Union. klicksafe wird gemeinsam von der Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz (Projektkoordination) und der Landesanstalt für Medien Nordrhein-Westfalen (LfM) umgesetzt.

Es wird darauf hingewiesen, dass alle Angaben in diesen Tipps trotz sorgfältiger Bearbeitung ohne Gewähr erfolgen und eine Haftung des Herausgebers ausgeschlossen ist.

Unveränderte nichtkommerzielle Vervielfältigung und Verbreitung ist ausdrücklich erlaubt unter Angabe der Quelle klicksafe und der Webseite www.klicksafe.de.
Siehe: http://creativecommons.org/licenses/by-nc-nd/3.0/de/

Herausgeber:

klicksafe
c/o Landesanstalt für Medien
Nordrhein-Westfalen (LfM)
Zollhof 2
D-40221 Düsseldorf

T: +49 (0)211-77 00 7- 0
F: +49 (0)211-72 71 70
E: klicksafe@lfm-nrw.de
W: www.klicksafe.de

klicksafe wird gefördert von der Europäischen Union

- Aktualisierte Auflage 2013 -