Datenschutz TIPPS

für Jugendliche

So sind deine Daten
im Internet sicher

klicksafe.de

Mehr Sicherheit im Internet
durch Medienkompetenz

Datenschutz TiPPS

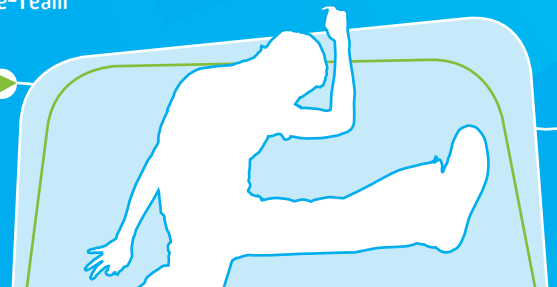
für Jugendliche

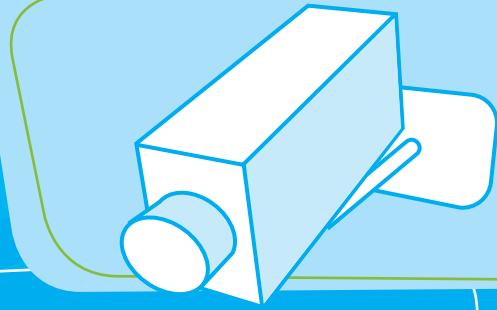
Du glaubst, Datenschutz ist langweilig und geht dich nichts an? Lass dich vom Gegenteil überzeugen! Wenn du das Internet nutzt, lohnt sich Weiterlesen in jedem Fall.

Denn wenn du surfst, hinterlässt du Spuren - immer. Sobald du im Internet unterwegs bist, werden Daten über dich gesammelt. Manche verrätst du freiwillig, bei anderen ist dir oft gar nicht bewusst, dass sie gesammelt werden.

Wir sagen dir, was du für den Schutz deiner Daten tun kannst.

Dein klicksafe-Team





1

Datenschutz ist cooler als du denkst

Datenschutz – das klingt ziemlich trocken, kann dir aber Ärger ersparen und hilft dir, dich im Web frei zu bewegen. Denn beim Datenschutz geht es um dich! Nicht alle Informationen über dich und dein Leben gehen jeden etwas an, oder?

Alle Daten, die etwas mit dir und deiner Person zu tun haben, zum Beispiel deine Adresse, dein Alter oder deine Interessen, sind **„personenbezogene Daten“**. Sie verraten viel über dich und sind kostbar. Für Unternehmen bedeuten sie bares Geld, und sie können von anderen missbraucht werden. Schützt du deine Daten, heißt das Privatsphäre, Anonymität und mehr Sicherheit für dich! Einfach unbezahlbar.

- Die schöne neue Welt der Überwachung www.panopti.com.onreact.com
- Bildergeschichte Datenschutz www.handysektor.de/index.php/bildergeschichten/datenschutz/

2 Datenschutz ist dein gutes Recht

§

Durch das **„Recht auf informationelle Selbstbestimmung“** sind deine persönlichen Daten (wie Name, Adresse, Telefonnummer) sogar per Gesetz vor unerlaubter Verwendung geschützt.
Das bedeutet: Niemand darf deine 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. Das gilt sogar für Fotos, auf denen dein Gesicht verfremdet wurde, du aber durch andere Merkmale (wie die Körperhaltung oder eine Tätowierung) eindeutig zu erkennen bist. Ausnahmen gelten für Bilder, auf denen du Teil einer Menschenmenge oder nur „Beiwerk“ bist (Beispiel: Jemand macht ein Foto vom Reichstag und du stehst zufällig daneben).
Im Internet kannst du von den Betreibern eines Webangebotes schriftlich die Löschung deiner persönlichen Daten verlangen, zum Beispiel deines Profils mit sämtlichen Bildern und Texten.

Übrigens: Wenn du jünger als 18 Jahre alt bist, haben deine Eltern bzw. deine Erziehungsberechtigten bei Veröffentlichungen mitzuentscheiden.
Bist du jünger als 14 Jahre, musst du deine Erziehungsberechtigten in jedem Fall um Erlaubnis fragen!

- Checked4you – Deine Rechte im Web (Klick auf Computer + Internet, dann auf Internet) www.checked4you.de

3 Sei fair mit den Daten anderer

Achte nicht nur auf dich, sondern wahre auch die Persönlichkeitsrechte anderer. Jeder hat ein Recht am eigenen Wort und am eigenen Bild. Also, keine Bilder, Filme und Infos von anderen ins Netz stellen, es sei denn, du hast ihre Erlaubnis. Es ist verboten, falsche Daten über jemanden zu veröffentlichen. Das wäre Rufschädigung und kann sogar bestraft werden. Überlege dir auch immer, ob du selbst mit der Veröffentlichung entsprechender Fotos, Filme oder Infos einverstanden wärst. Wenn das nicht der Fall ist, dann lass es! Das ist ein Zeichen von **Respekt**. 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!

- Logisch, dass **peinliche** Fotos, Filme und persönliche Infos nichts im Netz zu suchen haben. Sie verraten viel über dich, können dich den Ausbildungsplatz kosten oder mächtig Ärger bringen.
- Überlege auch, was eine **Gruppenmitgliedschaft** über dich aussagt. Die Gruppe „Saufen bis der Arzt kommt“ ist vielleicht nicht die beste 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 innerhalb der Community austauschst. Auch deine private E-Mail-Adresse solltest du nicht jedem geben.
- Setz deine **Profileinstellungen** auf privat. Nur Freunde sollten die Angaben sehen.
- Prüfe auch, ob du all deine **„Online-Freunde“** wirklich gut genug kennst, um ihnen freien Zugang zu deinen privaten Fotos und Daten zu geben. Du weißt nie, was sie mit den Informationen machen!

Das heißt aber nicht, dass du ganz auf Informationen über dich verzichten musst. Entscheidend ist die Auswahl der richtigen Infos. Überlege: Welche Daten willst du der Welt auf ewig präsentieren? 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.

- So schützt du deine persönlichen Daten in einzelnen Netzwerken (Klick auf Hilfe + Tutorials): www.watchyourweb.de
- Zum Schutz vor Missbrauch kannst du dein Profilfoto witzig verfremden (Klick auf Workshops + Profilbilder und Icons): www.netzcheckers.de
- Tipps für mehr Privatsphäre in schüler- und studiVZ zum Download: „Big brother is watching you!” www.jugendinfo.de/pass-auf-dich-auf

5

Das Internet vergisst nicht

Persönliche Infos, Texte, Filme und Fotos, die du von dir ins Netz stellst, sind ab da nicht mehr privat. Einmal im Netz, beginnen deine Daten ein **Eigenleben**. Sie verbreiten sich, gelangen in Suchmaschinen und Online-Archive, werden von anderen Nutzern kopiert und weitergereicht. Alles wieder rückgängig machen und löschen? Nahezu unmöglich. Daher: Vorher überlegen, was wirklich alle von dir wissen dürfen!

- Das Internet-Archiv „WayBack Machine“ speichert Websites 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/index.html

6 Elektronische Daten-Spuren hinterlässt du unbemerkt

- Technische Daten werden automatisch übertragen, ohne dass du es merkst. Zwei Beispiele:
  - Jeder Computer, der sich ins Internet einloggt, erhält eine **IP-Nummer** – eine Art „Telefonnummer für das Internet“. Damit lässt sich genau nachvollziehen, wann, wie lange und auf welchen Seiten du im Netz unterwegs warst. Über die IP-Nummer kann die Polizei bei Straftaten, wie zum Beispiel illegalen Musikdownloads, den Täter ermitteln.
  - Du surfst auf der Seite deiner Lieblingsband und siehst kurze Zeit später auf einer anderen Seite eine Werbung für ihre neue CD. Wie kommt das? Schuld daran können **Cookies** („Kekse“) sein. Cookies sind kleine Datenpakete, die auf deinem Rechner gespeichert werden und sich merken, welche Seiten du dir angeschaut hast. So können Unternehmen dich beim Surfen beobachten und herausfinden, welche Interessen du hast.

! Check deine Browser-Einstellungen und lass dir darüber anzeigen, wann eine Seite ein Cookie setzen will. So kannst du selbst entscheiden! Die Einstellungen findest du unter:
Internet Explorer: Extras › Internetoptionen › Datenschutz
Firefox: Extras › Einstellungen › Datenschutz

7 Nutze Nicknames und surfe unerkannt

- Gib dir einen guten **Nick** („Decknamen“), wenn du im Internet surfst. Sei hierbei erfinderisch – dein Deckname sollte deinem richtigen Namen nicht zu ähnlich sein. Verwende ihn zum Beispiel in Blogs, Chats und Foren. Verstecke dich aber nicht hinter einem Nick und gib dich nicht als jemand anderer aus, um andere gezielt zu beleidigen. Das ist unfair und kann bestraft werden! Auch wenn du in Netzwerken wie zum Beispiel schülerVZ gefunden werden willst, solltest du zumindest deinen Nachnamen abkürzen und nicht voll ausschreiben.

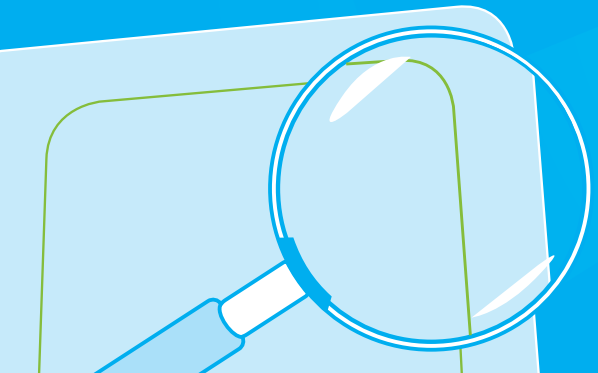
! Je mehr du im Web aktiv unterwegs bist, umso sicherer ist es, wenn du verschiedene Nicks nutzt. So bietest du weniger Angriffsfläche für Beleidigungen, Abzocke und anderen Datenmissbrauch.

8 Behalte die Kontrolle über deine Daten

Je mehr Daten du von dir verrätst, umso weniger Kontrolle hast du darüber. Nimm dir nicht selbst dein Recht auf informationelle Selbstbestimmung (siehe Punkt 2)! **Datensparsamkeit** zahlt sich aus und schützt vor bösen Überraschungen. Du hast es in der Hand, welche Daten du über dich ins Netz stellst. Hast du deine Daten (noch) im Griff?

Manchmal haben aber auch andere etwas zu deiner Person veröffentlicht. Wie steht's um deinen **Online-Ruf**? Check it! Gib deinen Namen in Suchmaschinen ein und überprüfe, wie du im Netz erscheinst.

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



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**. Du erfährst hier, was mit deinen Daten passiert, was gespeichert, weitergegeben oder für Werbung genutzt wird. Bevor du dich auf ein Web-Angebot einlässt, prüfe genau, welche Angaben der Anbieter zum Datenschutz macht. Wenn du die AGBs nicht verstehst, dann hole dir Hilfe. Im Zweifel lieber auf eine Nutzung des Angebots verzichten – auch wenn es häufig schwerfällt.

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

- Bei vielen **Instant Messengern** (Programme zum Nachrichtenaustausch in Echtzeit) gibst du durch die Nutzung sämtliche Rechte an allen versendeten Inhalten ab. Damit darf der Anbieter des Programms deine an Freunde verschickten Nachrichten speichern, bearbeiten und sogar veröffentlichen.
- Viele kostenlose **E-Mail-Anbieter** lesen die Inhalte deiner E-Mails nach Schlüsselwörtern aus, um dir dazu passende Werbung zu senden.

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, miteinander 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

11 Vor Datenmissbrauch ist niemand geschützt

Deine Daten sind im Netz nie völlig sicher. Daten können in falsche Hände geraten. Es gibt Hacker, die Daten stehlen, Computerfehler und Datenpannen. Bei einem großen deutschen Schüler-Netzwerk wurden bereits rund eine Million Profildaten gehackt und illegal weitergegeben. Auch deshalb: Überlege gut, was du ins Netz stellst.

Solltest du von Datenschutzverletzungen wissen oder selbst betroffen sein, zögere nicht, diese zu melden und dagegen anzugehen! 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.

- Weißt du, wer die problematischen Infos oder Bilder im Internet veröffentlicht hat? Dann bitte diese Person, die Inhalte so schnell wie möglich zu löschen.
- 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). Sage auch deinen Eltern, älteren Geschwistern oder anderen Erwachsenen, denen du vertraust, Bescheid.
- Bei falschen Behauptungen oder Beleidigungen gegen Personen kannst du auch die **Polizei** einschalten.
- Die **Datenschutz-Aufsichtsbehörden** der Länder können dir bei Datenschutzverletzungen ebenfalls mit Rat und Tat zur Seite stehen.
- Bei verbotenen oder jugendgefährdenden Inhalten (z. B. pornografische Bilder) kannst du auch **Beschwerdestellen**, wie etwa www.jugendschutz.net oder www.internetbeschwerdestelle.de, um Hilfe bitten.

Die Adressen der Datenschutz-Aufsichtsbehörden der Länder findest du auf www.bfdi.bund.de (Klick auf Datenschutz + Anschriften und Links + Aufsichtsbehörden für den nicht-öffentlichen Bereich)

Virtuelles Datenschutzbüro www.datenschutz.de

12 Sicherheitstipps – So sicherst du deine Daten

- Folgende Sicherheitstipps helfen, deine Daten zu schützen:
- Benutze **sichere Passwörter** (mindestens 8-stellig, Mischung aus Groß- und Kleinschreibung, Ziffern und Sonderzeichen wie „+-$§%&“) und nicht immer das gleiche. Es sollten nicht der Name deines Haustieres, dein Spitzname oder ähnliche leicht zu erratende Wörter sein. 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.
- Gehst du zu Hause kabellos ins Internet? Dann sichere dein **WLAN-Netzwerk** über eine verschlüsselte Verbindung. Wenn du unterwegs kabellos surfst, verschicke möglichst keine wichtigen Daten. Schalte dein WLAN aus, wenn du es 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.

- handysektor.de – „12 wichtige Tipps vom handysektor“ (Klick auf Tipps)
  http://www.handysektor.de
- www.klicksafe.de

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.

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