Jessica Wawrzyniak

Vertrauenswürdige Webangebote und Apps

einfach selbst prüfen und bewerten

digitalcourage

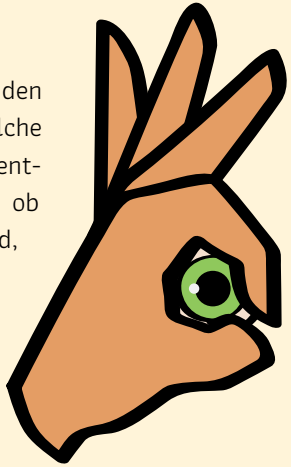
KURZ&MÜNDIG

Art d'Ameublement

Band 13

KOSTENFREI

Innerhalb von Sekunden entscheiden Sie, welche Website sie aufrufen, welche App Sie installieren. Sie wissen: Eigentlich sollten Sie genauer hinschauen, ob die Angebote vertrauenswürdig sind, welche Daten von Ihnen gespeichert werden und welche persönlichen Informationen Ihre Apps erschnüffeln.



Meistens hinterfragen Sie kritisch, was Sie einer App erlauben oder nicht. Aber das Kleingedruckte von jedem Angebot zu prüfen: total unrealistisch.

Wir zeigen Ihnen, wie Sie vertrauenswürdige Webangebote und Apps erkennen und schnell und einfach selbst prüfen können.

Impressum

1. Auflage 09-21, Art d'Ameublement, cc-by 4.0, ISBN 978-3934636-41-5

Autorin: Jessica Wawrzyniak, kidsdigitalgenial.de

Redaktion: Katrin Schwahlen, katrinschwahlen.de

Layout: Isabel Wienold, iwi-design.de

Bildlizenzen: S. 30 Jessica Wawrzyniak cc-by 4.0; S. 31 Fabian Kurz cc-by 4.0; alle weiteren Bilder: iwi-design.de, Isabel Wienold cc-by 4.0

Lernen Sie, Datensammler zu meiden und Ihr Recht auf informationelle Selbstbestimmung zu wahren.

Minimaler Zeitaufwand – maximaler Überblick:

Sie wollen schnell und ohne Zuschauer.innen Ihren Online-Einkauf erledigen, Nachrichten lesen und die Öffnungszeiten Ihres Bürgeramts erfahren. Anbieter hoffen darauf, dass Sie dabei nicht so genau hinschauen, was mit Ihren Daten passiert. Deshalb empfehlen wir Ihnen Folgendes.

- **Kontrolle behalten:** Eingebaute Cookies und Tracker analysieren Ihr Nutzungsverhalten und spähen aus, was Sie an Ihrem Gerät noch tun. Oft geben Sie persönliche Daten weiter, weil Sie überhastet zugestimmt haben.

- **Bewusstsein schärfen:** Durch die Tipps können Sie ein Gespür entwickeln, welche Websites und Apps mehr oder weniger angemessen mit Ihrer Privatsphäre umgehen. Entscheiden Sie selbstständig und bewusst, welchen Dienst Sie nutzen möchten – mit allen Konsequenzen und möglichst gutem Gewissen. Das braucht ein wenig Training, aber je öfter Sie einen Kurzcheck machen, desto geschulter wird Ihr Blick.

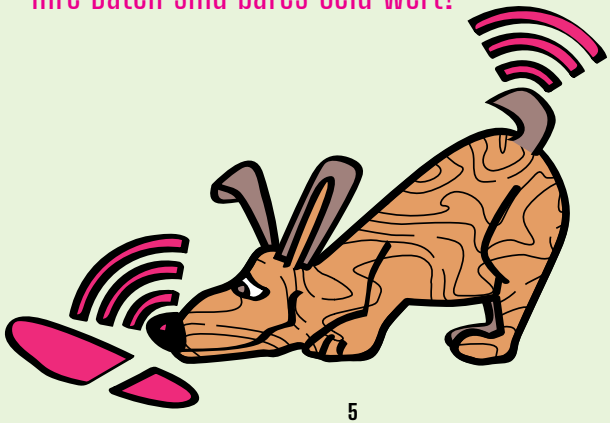
Wir starten mit einem ersten, sehr wichtigen Tipp:

Online-Shops, Nachrichtenportale, Streaming-Dienste und zahlreiche andere Anbieter stellen ihre Dienste oft als Webangebot und über eine App zur Verfügung. Probieren Sie zuerst, ob der Dienst im Browser funktioniert, bevor Sie die entsprechende App installieren. Das spart Speicherplatz, und Sie behalten besser die Kontrolle über ihre Daten, da Sie keine potenzielle Spähsoftware auf Ihrem Gerät installieren. Im Browser können Sie zum Beispiel einen Werbe- und Trackingblocker einbauen [▸ Seite 28] und so einen Großteil der Schnüffelei direkt unterbinden.

Die grösste Schnüffelei: Cookies, Tracker und Werbung

Das Aufrufen von Webangeboten kostet in der Regel zunächst kein Geld. Sie bezahlen höchstens für die Nutzung des Internets sowie für Dienste und Produkte, die sie explizit einkaufen (Abonnements, Premium-Accounts, Filme, Games und andere Produkte). Die meisten Anbieter möchten aber an Ihrem Websitebesuch verdienen, ihr Angebot mit Ihrer Hilfe optimieren und von Ihnen profitieren, selbst wenn Sie nichts kaufen (können, weil es sich um Informationsseiten, Videoplattformen usw. handelt). Die Anbieter verdienen an Ihnen, weil sie Ihre Daten sammeln und an Dritte weitergeben, z.B. Informationen über Ihr Surfverhalten, Ihre Person, Ihre Interessen.

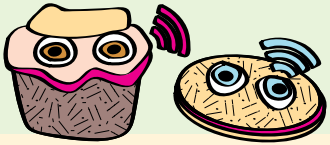
Ihre Daten sind bares Geld wert!



So profitieren Webanbieter von Ihren Daten:

Cookies

- Kleine Textdateien, die Informationen über Sie und Ihr Surfverhalten speichern (z.B. Log-in-Daten, Sprache, Seiten-Einstellungen).
- Durch Cookies „erinnert“ sich die Seite beim nächsten Besuch an Sie, und auch andere Seiten erkennen Sie an Ihren Cookies.
- Für manche Funktionen sind Cookies zwingend notwendig, z.B. beim Online-Shopping. Sie merken sich, welche Produkte in Ihrem Warenkorb sind, während Sie weiterstöbern.
- Cookies speichern aber oft auch Ihre IP-Adresse, Passwörter und Angaben, die Sie in Online-Formularen gemacht haben. Und natürlich Ihre Interessen.
- Diese Informationen können vom Anbieter selbst analysiert oder an Dritte verkauft werden (z.B. an Versicherungen, Werbefirmen, Verkäufer).



Tracker

- Viele Cookies verfolgen gezielt Ihre Surfaktivitäten. Diese sogenannten Tracking-Cookies oder Tracker „markieren“ Sie als Nutzer.in. Der Anbieter kann so sehen, wie Sie sich über seine Seiten bewegen und diese Infos für Optimierungen oder Marketing nutzen.
- Anbieter erlauben aber auch anderen Unternehmen (Drittanbietern), Tracking-Cookies (Third-Party-Cookies) zu platzieren. Beispiel: Der „Gefällt-mir“-Button von Facebook schnüffelt auf allen Seiten, wo der Button eingebunden ist und kommt an Daten von Ihnen, auch wenn Sie Facebook selbst nicht nutzen und den Button nicht mal anklicken.
- Wenn Sie die Cookies in Ihrem Browser nicht löschen oder die Einbindung von Drittanbieter-Cookies in Kauf nehmen, können sehr genaue Profile über Ihre Person erstellt werden.

Werbung

- Anbieter verdienen Geld, indem sie anderen Unternehmen Werbeplätze zur Verfügung stellen. Entweder zu Festpreisen oder nach Klickzahlen bezahlt.
- Wirklich lohnend ist aber das Geschäft der personalisierten Werbung: Informationen über Sie werden ausgewertet, um gezieltere Werbung für Sie zu schalten.
- Entweder nutzt der Anbieter diese Strategie, um eigene Produkte besser zu verkaufen oder gibt die Informationen an viele andere Werbetreibende (Drittanbieter) weiter.
- Die erforderlichen Daten werden hauptsächlich über Cookies und Tracker gesammelt.

Finden Sie heraus, welche Daten von Ihnen gespeichert werden

Datenschutzerklärung

Sie enthält folgende Informationen: Welche Daten werden zu welchem Zweck und wo gespeichert? Wie werden sie verarbeitet und an wen werden sie weitergegeben?

- Die Datenschutzerklärung ist meist klein und versteckt am Ende der Seite zu finden. Finden Sie keine, sollten bei Ihnen die Alarmglocken klingeln, denn:
- Jede Website speichert personenbezogene Daten (mindestens die IP-Adresse), auch wenn es bei datensparsamen Angeboten nur wenige sind. Daher ist eine Datenschutzerklärung fast immer Pflicht.

Allgemeine Geschäftsbedingungen (AGB) / Nutzungsbedingungen

Die vertraglichen Bedingungen für die Nutzung des Angebots müssen von den Nutzer.innen ausdrücklich akzeptiert werden.

Die AGB sind oft extra kompliziert verfasst, um abschreckende Bedingungen zu verschleiern oder Leser.innen zum ungelesenen Akzeptieren zu verleiten. Neben versteckten Kosten können sich dort auch Datenfallen verstecken.

- Lesen Sie mindestens die AGB von Webdiensten, bei denen Sie Kaufverträge oder Abonnements abschließen. Kontrollieren Sie Zahlungsbedingungen, Widerspruchsmöglichkeit, Reklamationsrecht, Kündigungsfristen usw.
- Verwenden Sie die Tastenkombination Strg + F, um auf der Seite nach Schlagworten zu suchen. Schauen Sie auch nach dem Stichwort „Daten“. Nutzungsbedingungen ersetzen jedoch keine Datenschutzerklärung.

- Stimmen Sie keinen AGB zu, die in einer Sprache verfasst sind, die Sie nicht verstehen.

Impressum

Betreiber von Webangeboten sind verpflichtet, eine ladefähige Adresse und mindestens zwei Kontaktmöglichkeiten anzugeben. Im Impressum können Sie sehen, welche Firma sich hinter dem Angebot verbirgt und ob das Angebot im Geltungsbereich der Europäischen Datenschutz-Grundverordnung (DSGVO) liegt. Weitere Infos dazu auf Seite 11.

Datenauskunft nach Art. 15 DSGVO

Sie können jedes Unternehmen und jeden Anbieter anschreiben, um Auskunft darüber zu bekommen, welche Daten von Ihnen gespeichert werden und diese bei Bedarf berichtigen oder löschen lassen. Damit ist gesetzlich geregelt, dass Sie Ihre Daten auch noch kontrollieren können, wenn Sie diese bereits abgegeben haben.

- Nutzen Sie dieses Recht! Schreiben Sie die Unternehmen an, bei denen Sie als Kundin registriert sind.
- Im Netz finden Sie Musterschreiben, die Sie schnell anpassen, ausdrucken und wegschicken können.

Tipp: Sie haben eine wichtige Stelle in der Textwüste ausgemacht, verstehen aber nicht alle Wörter? Schlagen Sie sie nach! So wächst Ihre Sicherheit im Umgang mit AGB und Datenschutzerklärungen.

Hinweis:

Texte, die voller Rechtschreib- oder Übersetzungsfehler sind, lassen an der Professionalität des Anbieters und der „Echtheit“ der Seite zweifeln. Auch fehlerhafte oder sehr kryptische URLs deuten auf betrügerische Seiten hin. Wie Sie außerdem die Echtheit einer Seite prüfen können, erfahren Sie auf Seite 16.

Prüfen Sie die Rechtslage (DSGVO)

Wir haben in der Europäischen Union das Glück, dass es mit der Datenschutz-Grundverordnung (DSGVO) Gesetze gibt, die Datenschutzrechte und -pflichten von Unternehmen und Organisationen gegenüber Kundinnen/Patienten/Klientinnen regeln: Ohne den Schutz von personenbezogenen Daten würden große Gefahren für Bürgerinnen und Bürger, aber auch für die Demokratie und Gesellschaft entstehen.

In China werden alle Bürger.innen auf Schritt und Tritt durch Videokameras und andere Überwachungsinstrumente kontrolliert. Wer eine rote Ampel überquert oder nicht viele „Freunde“ in sozialen Netzwerken hat, kann im sogenannten Sozialkreditsystem heruntergestuft werden und so zum Beispiel die Möglichkeit auf einen guten Job zu verlieren.

In den USA gibt es keine umfassenden Datenschutzgesetze, sondern nur branchenspezifische. Außerdem hebeln (Sicherheits-)Behörden und Geheimdienste die Schutzvorkehrungen wieder aus, um den Zugang zu allen Daten behalten.

Auch wenn Sie sich in einem EU-Land befinden: Sie nutzen die Angebote zu den Konditionen der Anbieter. So sind unsere Daten beispielsweise nicht vor dem Zugriff durch US-amerikanische Behörden geschützt, auch dann nicht, wenn die Server der Anbieter in der EU stehen (Mehr dazu erfahren Sie, wenn „Schrems-II-Urteil“ recherchieren).

Aber Achtung! Nicht alle Angebote, die mit „DSGVO-konform“ werben, sind als gute Angebote einzustufen.

1. Wo kein Kläger, da keine Richterin: Grundsätzlich kann zunächst jede.r behaupten, sein/ihr Angebot entspräche den EU-Gesetzen. Halten Sie sich an die weiteren Prüfkriterien, die wir Ihnen hier an die Hand geben und überzeugen Sie sich selbst.

2. Auch wenn Daten DSGVO-konform erhoben werden, muss das nicht so bleiben. Es können Fehler in der IT-Sicherheit gemacht oder Daten (samt dem Unternehmen) verkauft werden. Die Konsequenzen können verheerend sein. Nutzen Sie also möglichst datensparsame Dienste.

3. Viele Angebote, z.B. US-amerikanische, bewegen sich in rechtlichen Graubereichen. Die Nutzung müssen Sie mit Ihrem eigenen Gewissen ausmachen. Bleiben Sie realistisch: Der Schutz Ihrer Daten wird womöglich nur rechtlich geschickt zu Ihren Ungunsten ausgelegt.

Lassen Sie sich nicht zu einer Registrierung zwingen

Bei vielen Angeboten wird Ihnen vorgeschlagen, ein Benutzerkonto anzulegen. Verzichten Sie darauf, wann immer es geht. Wählen Sie lieber „ohne Registrierung fortfahren“ oder „als Gast einkaufen“. Denn sobald Sie mit einem Account eingeloggt sind, werden Ihre Aktivitäten weitaus präziser zusammengeführt, was genauere Analysen und Profilbildung über Sie zulässt.

Verzichten Sie auf die vermeintlich praktischen Anmeldeprozedere mittels Single-Sign-On, also über andere Accounts, die Sie bereits verwenden (z.B. über ein Facebook- oder Twitter-Log-in). Dies führt nur dazu, dass diese Unternehmen Nutzungsdaten auf Seiten abfischen können, auf die sie sonst keinen Zugriff hätten.

Sie MÜSSEN sich registrieren, denn die Vorteile sind u n v e r z i c h t b a r ? Hinterfragen Sie zumindest, ob die Erhebung der Daten, die Sie bei der Anmeldung angeben sollen, wirklich notwendig ist. Und: Prüfen Sie immer den Bereich „Mein Konto“ oder „Einstellungen“, wo Sie im eingeloggten Zustand verschiedene Datenschutz-Einstellungen vornehmen können. Die Voreinstellungen sind meist die unvorteilhaftesten für Ihre Privatsphäre.

Holen Sie Einschätzungen von Expert.innen ein

Sie müssen das Rad nicht neu erfinden. Haben andere bereits etwas über diesen Anbieter oder das Angebot herausgefunden?

Aber verlassen Sie sich nicht auf Kundenrezensionen oder Sternebewertungen, denn die sind oft gefälscht – zumindest die guten Bewertungen. Geben Sie stattdessen zum Namen des Webdienstes Schlagworte wie „Datenschutz“, „Sicherheit“ und „Bewertung“ in die Suchmaschine ein. Schauen Sie nach Expertisen von Verbraucherzentralen, Datenschutzbehörden, Juristinnen und Informatikern. Auch IT-Magazine und techniknahe Nachrichtenportale veröffentlichen oft Bewertungen einzelner Angebote und Anbieter.

Webseiten: Schnellprüfung in 5 Minuten

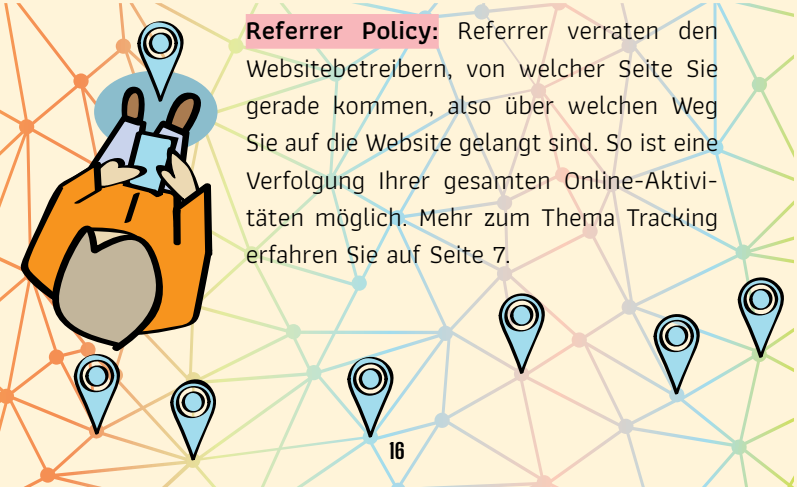
Verschaffen Sie sich mit dem Tool Webbkoll [webbkoll.dataskydd.net] einen schnellen Überblick, wie verantwortungsvoll Anbieter mit Ihren Daten und Ihrer Privatsphäre umgehen. Sie müssen dazu nur die URL eintragen, die Sie prüfen möchten. Webbkoll simuliert den Aufruf einer Website ohne Werbe- und Trackingblocker, ohne diese tatsächlich zu besuchen.

Screenshots Stand: 21.09.21

Erklärungen:

HTTPS als Voreinstellung: ist ein Verschlüsselungsstandard. Wenn dieser richtig konfiguriert ist, werden beim Surfen anfallende Metadaten geschützt, die Manipulation dieser Daten verhindert und gewährleistet, dass es sich um eine „echte“ Website handelt, die nicht Teil einer Betrugsmasche ist. Beginnt die URL einer Seite mit http (ohne das „s“ für secure/sicher), fehlt die Verschlüsselung.

Content Security Policy: beschreibt eine zusätzliche Sicherheitsebene, die vor unberechtigten Zugriffen, Datendiebstahl und Verbreitung von Schadsoftware schützt. Diese Ebene entspricht einem hohen Sicherheitsstandard und sollte zumindest bei Online-Bankgeschäften und ähnlich sensiblen Transaktionen erfüllt sein.



Referrer Policy: Referrer verraten den Websitebetreibern, von welcher Seite Sie gerade kommen, also über welchen Weg Sie auf die Website gelangt sind. So ist eine Verfolgung Ihrer gesamten Online-Aktivitäten möglich. Mehr zum Thema Tracking erfahren Sie auf Seite 7.

Cookies: Webbkoll prüft, ob und wenn ja, welche Cookies gespeichert werden. Mehr über Cookies erfahren Sie auf Seite 6.

Drittanfragen: An der Stelle sehen Sie, wie viele Drittanbieter Zugriff auf Ihre Daten bekommen. Mehr über Drittanbieter erfahren Sie auf Seite 6/7.

Serverstandort: beschreibt den Ort, an dem Ihre Daten gespeichert werden. Hier können Sie prüfen, ob die Daten im Geltungsbereich der Datenschutz-Grundverordnung gespeichert werden. Mehr zur DSGVO erfahren Sie auf Seite 11/12.

Sie können auch die Website „Privacy Score“ (privacyscore.org) für eine **Websiteprüfung** nutzen. Allerdings befindet sich das Tool in einer noch nicht ganz zuverlässigen Beta-Version (Stand August 2021).

Apps prüfen

Wenn Sie einen Dienst ohne Webangebot nutzen möchten, sollten Sie auch bei der Installation der App die Prüfkriterien beachten, die für Angebote im Web gelten:

- Lassen Sie sich nicht zu einer Registrierung zwingen.
- Prüfen Sie den Umgang mit Ihren Daten.
- Prüfen Sie den Geltungsbereich der DSGVO.
- Holen Sie eine Einschätzung von Expert.innen ein.

Zusätzlich sollten Sie bei der App-Nutzung weitere Aspekte beachten, die sich auf Art und Funktionen der Software beziehen. Informationen dazu finden Sie schon vor Installation in der Beschreibung der App.

Software kann grob in drei Arten unterteilt werden

- **quelloffen:** Um eine möglichst gute Kontrolle über Ihre Daten zu haben, sollten Sie mindestens quelloffene Software einsetzen, auch Open-Source-Software genannt. Sie zeigt transparent, wie Ihre Daten verarbeitet werden.
- **frei:** Die beste Kontrolle haben Sie, wenn Sie Freie Software nutzen, auch Free-Open-Source-Software genannt (FOSS). Sie entspricht freiheitlich-demokratischen Werten und sollte vor allem dann genutzt werden, wenn sehr sensible Daten oder Personengruppen geschützt werden müssen (siehe auch Seite 29).
- **proprietär:** Dabei handelt es sich um geschlossene Software, also Programme, die einer Firma oder einem Konzern gehören (proprietär = im Eigentum befindlich). Nutzen Sie diese möglichst nicht, denn Sie wissen nicht, was im Verborgenen passiert. Die Algorithmen gelten als Firmengeheimnis, Kundengewinnung und -bindung (mit manchmal zweifelhaften Mitteln) sind häufig oberstes Ziel.
- Mehr Informationen zu Freier Software finden Sie in der KURZ&MÜNDIG-Broschüre „Homeoffice – mit Datenschutz und freier Software“ (k&m Band 7)

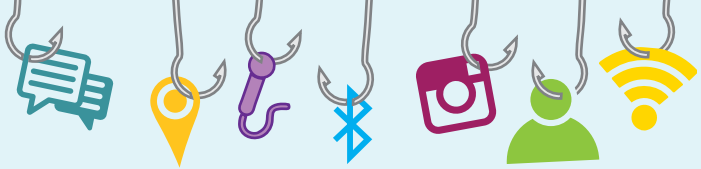
Kriterien zur Unterscheidung von Software

	Freie Software	Quelloffene Software	Proprietäre Software
Offener Quellcode (Bauplan der Software)	ja	ja	nein
Fehler und Datenflüsse lassen sich von außen erkennen.	ja	ja	nein
Quellcode kann frei verwendet, beliebig angepasst, weiterentwickelt und weitergegeben werden.	ja	nein	nein
Nutzer.innen bleiben unabhängig von einzelnen Marken/ Produktlinien.	ja	unter-schiedlich	nein
Zufriedenheit der Nutzer.innen kommt vor wirtschaftlichen Interessen.	ja	unter-schiedlich	nein

Schon der Weg zur App ist wichtig

Wer den Play-Store von Google oder den App-Store von Apple nutzt, tut dies zu Googles bzw. Apples Bedingungen [mehr dazu auf Seite 12]. Das heißt: Schon die App zum Herunterladen von anderen Apps sammelt Daten von Ihnen. Daher ist es fair von den Anbietern, wenn Sie zusätzlich ein Webangebot mit mobiler Ansicht (geeignet für Smartphones und Tablets) anbieten. Diese Variante sollten Sie vorziehen, um die Kontrolle über Ihre Daten zu behalten.

Empfehlung: Es gibt für Android einen unabhängigen Store für Freie Software: F-Droid. Schauen Sie doch dort mal nach, ob Sie Apps finden, mit der Sie proprietäre Software auf Ihrem Gerät ersetzen können. Mehr über F-Droid finden Sie auf der Webseite 🔗digitalcourage.de/f-droid



Die Tücken von App-Berechtigungen

Besonders sensible Zugriffe sind die auf Kamera, Mikrofon, Standort, GPS, Bluetooth, Kontakte, Körpersensoren, SMS. Im Grunde genommen kann jeder Zugriff für Ihre Privatsphäre gefährlich werden. Smartphones werden nicht ohne Grund als „Spion in der Hosentasche“ bezeichnet.

Prüfen Sie die Berechtigungen deshalb mit Sinn und Verstand.

Natürlich braucht ein Programm für Videokonferenzen Zugriff auf Ihre Kamera und für Sprachnachrichten wird das Mikrofon benötigt. Aber brauchen diese Apps auch Zugriff auf GPS oder Bluetooth?

Entscheiden Sie sich für Programme, die möglichst wenige Zugriffe möchten.

Muss Ihr Mail-Programm auf Ihr Telefonbuch zugreifen, wenn Sie Ihre Kontakte dort gar nicht nicht hinterlegen möchten? Braucht eine Taschenrechner-App Zugriff auf Ihre Kamera?

Tipps:

Bei aktuellen Betriebssystemen für Smartphones oder Tablets können Sie in den Haupteinstellungen des Geräts nachträglich Berechtigungen für Apps erteilen oder entziehen. Erteilen Sie so wenige Zugriffsrechte wie möglich. Falls dadurch nützliche Funktionen eingeschränkt werden, können Sie die App-Berechtigungen mit wenigen Klicks anpassen.

Prüfen Sie hin und wieder die Zugriffsrechte für Ihre installierten und bereits vorinstallierten Apps. Manchmal werden die Einstellungen durch Updates verstellt.

Apps: Schnellprüfung in 5 Minuten

Prüfen Sie Android-Apps mit dem Tool „Exodus Privacy“ [reports.exodus-privacy.eu.org/de/]. Geben Sie dazu einfach den Namen der App ein.

Wenn ein Bericht zu der App veröffentlicht wurde (und es gibt bereits viele Berichte), erhalten Sie eine Übersicht, welche Tracker in die App eingebaut sind und welche Berechtigungen die Software verlangt. Die kritischsten Berechtigungen werden mit einem „!“ gekennzeichnet.

Eine Wecker-App mit 48 Trackern...

Checkliste: Haben Sie an alles gedacht?

Vertrauenswürdige Webangebote und Apps speichern möglichst wenig personenbezogene Daten, geben diese nicht an Dritte weiter, verfolgen nicht Ihr Surfverhalten oder andere Aktivitäten am Gerät, erfordern keine Registrierung, wenn diese keine klaren Vorteile bringt, und liegen rechtlich im Bereich der DSGVO.

Webangebote

5-Minuten-Übersicht:

- ☐ Schnellprüfung mit Webbkoll (Sicherheitsstandards, Cookies, Tracker, Drittanbieter und Serverstandort prüfen)

Umfassender Überblick in 30 Minuten:

- ☐ Wer bietet den Dienst an? Liegt das Angebot im Geltungsbereich der DSGVO?
- ☐ Welche Bindungen gehe ich ein, wenn ich das Angebot nutze?
- ☐ Muss ich mich registrieren? Und wenn ja, mit welchen Daten? Bringt die Registrierung nennenswerte Vorteile?
- ☐ Welche Daten werden erhoben, zu welchem Zweck und an wen werden sie weitergegeben?
- ☐ Gibt es bereits fachliche Meinungen von Expert.innen?

Apps

5-Minuten-Übersicht:

- [ ] Schnellprüfung mit Exodus Privacy (Tracker und App-Berechtigungen)

Umfassender Überblick in 30 Minuten:

- [ ] Wer bietet den Dienst an? Liegt das Angebot im Geltungsbereich der DSGVO?
- [ ] Welche Bindungen gehe ich ein, wenn ich das Angebot nutze?
- [ ] Muss ich mich registrieren? Und wenn ja, mit welchen Daten? Bringt die Registrierung nennenswerte Vorteile?
- [ ] Welche Daten werden erhoben, zu welchem Zweck und an wen werden sie weitergegeben?
- [ ] Gibt es bereits fachliche Meinungen von Expert.innen?
- [ ] Um welche Software-Art handelt es sich? Ist die App quelloffen, zur Weiterentwicklung freigegeben und Store-unabhängig beziehbar?
- [ ] Müssen zweifelhafte Berechtigungen erteilen werden?
- [ ] Gibt es ein entsprechendes Webangebot?

Prüfung erledigt: Angebot ist nicht vertrauenswürdig. Und jetzt?

Jetzt kommen Ihre Schutzvorkehrungen ins Spiel; denn während Sie bei der Nutzung von Apps kaum Möglichkeiten haben, Datenschutzeinstellungen vorzunehmen, können Sie auf Webseiten ein wenig nachhelfen.

Cookie-Banner einstellen: Wenn Sie eine Website aufrufen, werden Sie meist gefragt, welche Drittanbieter- und Tracking-Cookies Sie zulassen wollen. Ein nettes Werkzeug zur Kontrolle über die eigenen Daten? Nein. Denn viele Banner sind nicht DSGVO-konform, weil Sie z.B. nicht alle Tracker ablehnen können. Oft werden auch miese Maschen genutzt, um Ihre Zustimmung zur Datenerhebung und -weitergabe an Drittanbieter zu bekommen, z.B. sogenannte Dark Pattern oder Antimuster, die entgegen dem intuitivem Klickverhalten angelegt sind. Heißt: Dort, wo Sie bestimmte Buttons wie „meine Einstellungen speichern“ vermuten, weil Sie es von anderen Seiten so kennen, befindet sich beispielsweise der Button „allen Cookies zustimmen“. Lehnen Sie so viele datensammelnde Optionen ab, wie Sie können.

Challenge: Finden Sie die versteckten Optionen! Sie werden staunen, welche Firmen ein „berechtigtes Interesse“ an Ihren Daten haben, obwohl dieses völlig abwegig ist.

Ändern Sie Ihre Browser-Einstellungen:

- Blockieren Sie einige Cookie-Kategorien.
- Deaktivieren Sie die Aktivitätenverfolgung (blockiert einige seitenübergreifende Tracker).
- Schalten Sie „Do Not Track“ ein. Damit bitten Sie Websitebetreiber, Sie nicht zu tracken. Mehr ist es leider nicht; denn es gibt keine rechtliche Verpflichtung.
- Surfen Sie, wenn möglich, im „privaten Modus“.
- Der effektivste Schutz: Installieren Sie Tracking- oder Werbeblocker. Informieren Sie sich vorher über deren Qualität; denn manchmal kaufen sich Anbieter aus den Blockinglisten frei (z.B. bei „AdBlock Plus“). Nutzen Sie im Firefox-Browser das Add-on „uBlock Origin“.

Funfact: Wenn Sie ALLE Cookies blockieren, blockieren Sie auch das Cookie, in dem gespeichert ist, dass Sie keine Cookies wünschen.

- Auf Mobilgeräten: Klicken Sie sich durch Ihre Einstellungen bis Sie bei „Google → personalisierte Werbung“ oder „Datenschutz → Tracking“ landen und schalten Sie diese ab.

Sind besonders sensible Daten besonders gefährdet?

In einigen Bereichen ist es sehr wichtig, Grundrechte wahrende Angebote zu nutzen, denn Datenschutz ist Menschenschutz.

Informationen über die ethnische und kulturelle Herkunft, politische, religiöse und philosophische Überzeugungen, Gesundheit, Sexualität und Gewerkschaftszugehörigkeit müssen stärker geschützt werden als andere Informationen, da sie eine erhöhte Angriffsfläche für Anfeindungen oder gesellschaftlichen Ausschluss bieten (Art. 9 DSGVO). Außerdem müssen Daten von Kindern besonders geschützt werden (Art. 8 und ErwGr.38 DSGVO). Das betrifft generell die Bereiche Schule und Jugendarbeit. Aber auch andere Berufsfelder, Personengruppen und Anwendungsbereiche sind besonders angehalten, auf Datenschutz zu achten: Anwälte, Journalistinnen, Therapeutinnen und alle, die vermehrt mit den genannten schützenswerten Informationen zu tun haben.

Für Schulen gibt es eine umfassende Liste von guter Software, und Hilfestellungen zur Nutzung, auf 🔗digitalcourage.de/netzwerk-freie-schulsoftware. Außerdem finden Sie gute Alternativen auf 🔗digitalcourage.de/digitale-selbstverteidigung.

Die Autorin

Jessica Wawrzyniak ist Medienpädagogin (M.A.) und arbeitet im Team von Digitalcourage e.V. für den Schutz der Daten und Privatsphäre von Kindern und Jugendlichen.

Ihr Ziel: Kinder, Eltern, Lehrkräfte und Behörden aufklären und auf Augenhöhe bringen.

Ihr Angebot: Gesprächsgruppen, Seminare, Vorträge, redaktionelle Beiträge

Sie freut sich über Anfragen mit Angaben zur Zielgruppe, gewünschtem Themenfokus und Honorarvorstellung.

Kontakt: jessica.wawrzyniak@digitalcourage.de

Die Autorin hat in dieser Reihe bereits veröffentlicht:

Datenschutzrechte durchsetzen
Tipps für Lehrkräfte und Eltern (k&m Band 2)

Digitale Bildung
10 Leitlinien, um Schule frei und ganzheitlich zu gestalten (k&m Band 4 gemeinsam mit Leena Simon)

Die KURZ&MÜNDIG-Reihe wird herausgegeben von:

digitalcourage e.V. engagiert sich seit 1987 für Grundrechte, Datenschutz und eine lebenswerte Welt im digitalen Zeitalter. Wir sind technikaffin, doch wir wehren uns dagegen, dass unsere Demokratie „verdatet und verkauft“ wird. Seit 2000 verleihen wir die BigBrother-Awards. Digitalcourage ist gemeinnützig, finanziert sich durch Spenden und lebt von viel freiwilliger Arbeit.

Mehr zu unserer Arbeit finden Sie auf 🔗digitalcourage.de und 🔗bigbrotherawards.de

In der KURZ&MÜNDIG-Reihe sind bisher erschienen:

01 **Digitale Mündigkeit**
02 **Datenschutzrechte in Schulen durchsetzen**
03 **Faire Websites**
04 **Leitlinien für digitale Bildung in Schulen**
05 **Uploadfilter**
06 **Stalking, Hass, Kontrolle**
07 **Homeoffice**
08 **Digitale Bildungsangebote selbst erstellen**
09 **Digitale Angiffe im Büro**
10 **Digitale Sicherheit für Frauenhäuser**
11 **Versammlungsfreiheit**
12 **Nichts zu verbergen?**
13 **Apps selbst prüfen und bewerten**

Dieses KURZ&MÜNDIG-Minibuch ist auch als komfortables interaktives PDF erhältlich. Es kostet nur 5,00 Euro und ist wie alle KURZ&MÜNDIG-Ausgaben (auch als Printversion) erhältlich unter: 🔗digitalcourage.de/kum

Nehmen Sie sich Zeit, um Ihre Daten zu schützen?

Hier finden Sie Tipps, um Websites und Apps in fünf Minuten zu prüfen.

Sie wollen tiefer eintauchen?

In nur 30 Minuten bekommen Sie einen umfassenden Überblick über die Vertrauens-würdigkeit Ihres Anbieters.

Drum prüfe, wer Dich ewig bindet.

Digitalcourage e.V.
Marktstraße 18 | 33602 Bielefeld
mail@digitalcourage.de | digitalcourage.de
T: +49 521 1639 1639

9 783934 636415 >
5,00 Euro
4,00 SFR
ISBN 978-3934636-41-5

digitalcourage
k&m 13 Apps bewerten