BLM
Bayerische
Landeszentrale für
neue Medien

Sicher online unterwegs

TIPPS & TRICKS ZUM SELBSTDATENSCHUTZ

Sicher online unterwegs
Tipps und Tricks zum Selbstdatenschutz

Jeden Tag gehen Menschen mit ihren Smartphones, Tablets, PCs, Notebooks und sogar dem Fernseher ins Internet. Viele denken nicht darüber nach, dass jeder Klick, jede Suche, jeder Chat, jedes Foto, jeder Post und jedes Streaming eine Datenspur hinterlassen. Die Daten können von Unternehmen für gezieltes Onlinemarketing und Marktforschung erfasst und ausgewertet werden. Sie dienen etwa als Basis für individuelle Nutzungs-, Kauf- oder Bewegungsprofile.

Ein bewusster und selbstbestimmter Umgang mit den eigenen Daten ist daher für alle Nutzerinnen und Nutzer wichtig. Wie aber kann ich selbst aktiv werden, um meine Privatsphäre im Internet zu schützen? Auf welche Einstellungen muss ich achten? Welche Risiken möchte ich in Kauf nehmen, welche eher nicht? Hierzu finden Sie in unserer Broschüre zum Thema Selbstdatenschutz zahlreiche Tipps und Hinweise.

Die Broschüre informiert nicht nur über Risiken und Hintergründe, sondern zeigt Möglichkeiten einer sicheren Internet- und Social-Media-Nutzung. Sie nimmt aktuelle Themen wie „Selbstdarstellung auf Social Media", „Streaming" sowie „Meeting- und Lernplattformen" in den Blick. In jedem Kapitel bietet zudem ein eigener Abschnitt Eltern und Lehrkräften praxisnahe Anregungen, damit sie auch Kinder und Jugendliche zu einem souveränen Umgang mit persönlichen Daten erziehen und anleiten können.

Wir wünschen Ihnen eine informative Lektüre und viel Erfolg bei der praktischen Umsetzung der Tipps!

Dr. Thorsten Schmiege
Präsident der Bayerischen Landeszentrale für neue Medien (BLM)

Inhaltsverzeichnis

Einleitung S. 4

1. Technik und Geräte S. 7
- Zugangssperren
- Standort, Router und Verschlüsselung
- Installation von Apps
- Elternhaus und Schule

2. Kommunikation im Internet S. 16
- Messenger-Dienste
- E-Mails
- Elternhaus und Schule

3. Selbstdarstellung auf Social-Media-Plattformen S. 22
- Finanzierung
- Anmeldemöglichkeiten
- Problematische Inhalte
- Elternhaus und Schule

4. Unterhaltung über Streamingdienste S. 28
- Anmeldung und Nutzung
- Kostenfreie Angebote
- Kostenpflichtige Angebote
- Elternhaus und Schule

5. Meeting- und Lernplattformen S. 34
- Hinweise zur Nutzung
- Sicherheitsvorkehrungen
- Elternhaus und Schule

6. Online unterwegs S. 38
- IP-Adresse
- Cookies
- Suchmaschinen
- Elternhaus und Schule

Glossar S. 44

Stichwortverzeichnis S. 46

Impressum S. 47

Selbstdatenschutz – was ist das?

Kaum ein Mensch erlaubt einer unbekannten Person ohne Grund Einblicke in seine persönlichen Notizen, privaten Urlaubsfotos oder Bankdaten. Nichts davon wird Fremden oder Neugierigen einfach gezeigt.

Ganz anders ist das bei vielen Menschen, wenn sie im Internet unterwegs sind: Nach dem Motto „Ich habe doch nichts zu verbergen" werden Daten und damit häufig große Teile der Privatsphäre freiwillig öffentlich gemacht. Hinzu kommt, dass die Personalisierung von Internet- bzw. Social-Media-Angeboten und die damit verbundene Preisgabe von Daten einen höheren Nutzungskomfort bzw. auch eine Selbstbestätigung in Form von sozialer Anerkennung (digitale Zustimmung, Lob, Sichtbarkeit, Zugehörigkeitsgefühl) verspricht. Zwischen gewohnheitsmäßiger Bequemlichkeit und dem partiell vorhandenen Wissen um die Risiken der Preisgabe von privaten Daten besteht oftmals ein Widerspruch. Ist diese öffentliche Preisgabe von persönlichen Daten wirklich ohne Risiko? Sicherlich nicht – jedoch sind die Konsequenzen auf den ersten Blick weniger offensichtlich als bei einer direkten Begegnung mit neugierigen Mitmenschen, bspw. einer Sitznachbarin oder einem Sitznachbarn in der U-Bahn, die/der neugierig mit in das (fremde) Smartphone schaut.

Gesetze, wie das Bundesdatenschutzgesetz, und die europäischen Regelungen, wie die Datenschutz-Grundverordnung* (DSGVO), dienen dem bestmöglichen Schutz unserer Daten. Dennoch gilt: Wir alle können und sollten selbst etwas für den Schutz unserer persönlichen Daten tun. Begriffe wie „Selbstdatenschutz" und „Digitale Selbstverteidigung" bestätigen: Auch wenn die Preisgabe persönlicher Daten in der digitalen Welt nicht ganz vermieden werden kann, so sind wir als Mediennutzende nicht völlig wehr- und schutzlos der Datenerhebung ausgeliefert.

Diese Broschüre möchte Sie in einigen wichtigen Punkten für den Selbstdatenschutz sensibilisieren. Sie erhalten Tipps, wie Sie bei der Nutzung digitaler Medien bestmöglich die Kontrolle über Ihre Daten behalten können.

*Mit * gekennzeichnete Begriffe werden ab Seite 44 in einem Kurzglossar erläutert. Ein ausführliches Glossar zum Thema Selbstdatenschutz finden Sie, wenn Sie den QR-Code scannen oder online auf den Link klicken.*

Stand aller Links und QR-Codes: Dezember 2022.

BLM – Glossar
„Sicher online unterwegs"

Warum muss ich mich schützen?

Datenpreisgabe kann ungewollte Konsequenzen haben. Bei jedem Bezahlvorgang mit Kunden-, Kredit- oder Bankkarte, bei jedem zurückgelegten Weg über GPS*-Daten und bei jedem Austausch in Social-Media-Angeboten hinterlassen wir Datenspuren.

Konto gehackt?

Sie haben nicht viel eingekauft und trotzdem leert sich Ihr Bankkonto? Konto- und Kreditkartendaten können durch Leichtsinn oder gezielte Hackerangriffe in falsche Hände geraten. Dann werden z. B. Zahlungen umgeleitet oder Bestellungen auf anderer Leute Kosten getätigt. Schauen Sie also genau hin, bevor Sie Ihre Konto- und Kreditkartendaten im Internet verwenden und überprüfen Sie Ihre Kontoauszüge.

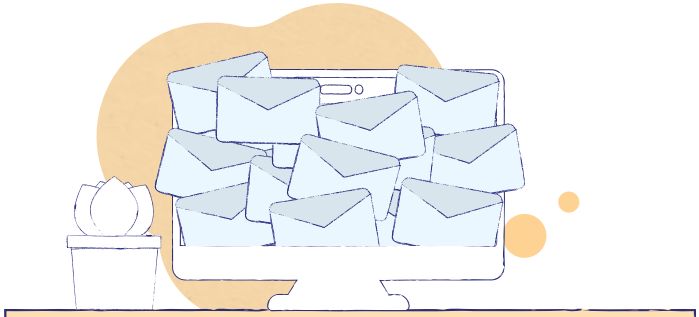
Datensparsamkeit und Datenachtsamkeit

Sobald Daten – insbesondere in Verbindung mit dem Internet – gesammelt werden, gibt es keinen absoluten Schutz vor Zugriffen mehr. Das richtige Verhalten lässt sich daher auf eine einfache Grundformel bringen: Geben Sie nur so viele Daten wie nötig und so wenige Daten wie möglich von sich preis.

Oftmals werden mehr persönliche Daten bei einer Anmeldung auf Plattformen oder Apps im Internet abgefragt als notwendig. Für die Verarbeitung von persönlichen Daten muss (nach der Datenschutz-Grundverordnung – DSGVO) in der Regel eine Einwilligung gegeben werden, die jederzeit widerrufen werden kann. Es ist nicht immer erforderlich, bestimmte Angaben zur eigenen Person zu machen, wenn man dazu aufgefordert wird. Unterscheiden Sie zwischen Pflichtangaben und freiwilligen Angaben: Pflichtangaben sind häufig mit einem Stern * gekennzeichnet.

Beispiele für persönliche bzw. personenbezogene Daten:

- Name, Alter, Familienstand, Geburtsdatum, Staatsangehörigkeit
- Anschrift, Telefonnummer, E-Mail-Adresse
- Konto- und Kreditkartennummer
- Kraftfahrzeugnummer, Kfz-Kennzeichen
- Personalausweis- und Sozialversicherungsnummer
- Vorstrafen
- genetische und Krankendaten
- Werturteile bzw. Leistungsnachweise (z. B. Zeugnisse)
- Kunden- und Personaldaten
- religiöse oder weltanschauliche Überzeugung
- Fotos, Videos

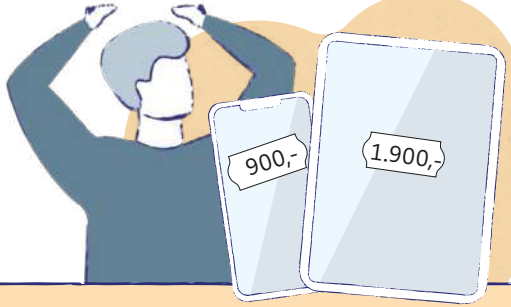


Zugespamt?
Ihr Briefkasten enthält plötzlich viel mehr Werbesendungen und auch Ihr E-Mail-Konto ist voller Spam? Möglicherweise haben Sie ein Kundenkonto bei einem unseriösen Online-Händler eröffnet und Ihre Daten wurden weiterverkauft. Vielleicht haben Sie Ihre E-Mail-Adresse auch selbst auf Ihrer Website oder auf Ihrem Social-Media-Profil veröffentlicht.

Fragen Sie sich, ob Sie für bestimmte Bonusangebote von Supermärkten (z. B. Payback) und Online-Shops mit den eigenen Daten bezahlen wollen, die dann für gezielte Werbesendungen eingesetzt werden. Bei der Verbraucherzentrale erhalten Sie weitere Informationen:

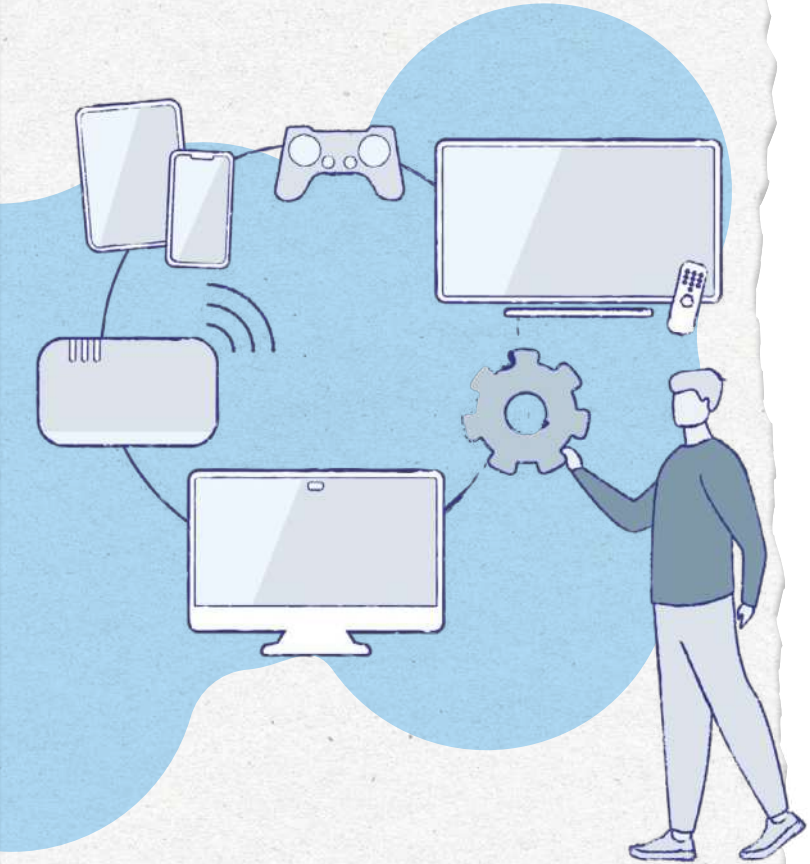
Verbraucherzentrale – Kundenkarten

Es ist nicht abzusehen, was die umfassenden Datensammlungen und Auswertungen mittels Algorithmen von heute für zukünftige Konsequenzen haben. Klar ist, sie können weitreichende Vor- und Nachteile mit sich bringen (Big Data). Wichtig ist, die eigenen persönlichen Daten und Fotos sowie erst recht die Daten anderer Menschen (z. B. von Partnerinnen und Partnern, Kindern oder Freundinnen und Freunden) als persönliches „Kapital" zu verstehen, mit dem man nicht verschwenderisch, sondern sparsam umgehen sollte. „Meine Daten gehören mir!" – das ist ein Slogan, der immer wichtiger wird.



Zu viel bezahlt?
Sie erfahren, dass Ihre Bekannte über das Internet die gleiche Reise beim selben Anbieter gebucht, aber wesentlich weniger bezahlt hat. „Preisdiskriminierung" ist im Internet an der Tagesordnung. Dabei geht es beispielsweise um Preiszuschläge für Nutzerinnen und Nutzer teurer Geräte oder für Bewohnerinnen und Bewohner teurer Wohnviertel – denn die Informationen, über welches Endgerät und aus welcher Gegend Sie online bestellen, gehen oft automatisch an die Anbieter und bestimmen den für Sie gültigen Preis.

1. Technik und Geräte



Das Smartphone, das Tablet und auch die Spielkonsole nutzen wir als digitale Mediengeräte mobil – überall und jederzeit. Sie sind Kommunikationsplattform, Navigationsgerät, Fahrkartenautomat, mobiles Shoppingcenter usw. und mit jedem neuen Modell kommen neue Anwendungsmöglichkeiten hinzu. Das bedeutet: Es werden immer mehr Datenspuren erzeugt und hinterlassen. Wer dies einschränken will, muss sich regelmäßig über aktuelle Schutzmaßnahmen informieren.

TIPPS

- **Überprüfen** Sie bei neuer Technik und neuen Geräten sowie Apps immer die **Datenschutzeinstellungen.** Die von den Anbietern festgelegten Voreinstellungen entsprechen in aller Regel nicht dem eigenen Sicherheitsbedürfnis, sondern ermöglichen häufig umfangreiche Datenerhebungen.
- Löschen Sie regelmäßig Ihren Browserverlauf und die Cookies* (→ siehe ab Seite 38)

Zugangssperren

Datendiebstahl geschieht nicht nur online. Verhindern oder erschweren Sie das Aufrufen von Daten bei einem Gerätediebstahl oder bei Abwesenheit (etwa am Arbeitsplatz). Sie können nahezu alle digitalen Geräte mit einer Zugangssperre versehen.

TIPPS

Richten Sie Zugangssperren ein, z. B.:
- **Display-Sperre bzw. Sperrbildschirm oder Bildschirmsperre.** Aktiv nach dem Hochfahren und nach Inaktivität des Geräts.
- **PIN-Schutz der SIM-Karte**. Aktiv beim Hochfahren bzw. Wiedereinschalten des Geräts.

Überlegen Sie, welche Sicherheitsstufe für die Zugangssperre sinnvoll ist:

- **Geringe bis mittlere Sicherheit**
  Unterschrift auf dem Display des Smartphones, Muster auf den Bildschirm streichen
- **Mittlere Sicherheit**
  - Geheimzahl, PIN (Persönliche Identifikationsnummer), oft nur vierstellige Zahlenkombination
  - Gesichtserkennung: kann bei einigen Kameras durch Foto überwunden werden
- **Höhere Sicherheit**
  Passwort/Kennwort: Buchstaben-, Zahlen- und Zeichenkombination, höhere Sicherheit bei Beachtung der Regeln für ein sicheres Passwort
- **Höchste Sicherheit**
  Iris-Scan, Fingerabdruck-Scan, intelligenter Scan (Kombination aus Gesichts- und Iris-Scan): alles sehr persönliche Daten

Der Weg zur Einrichtung eines Sperrbildschirms ist je nach Gerät bzw. Betriebssystem unterschiedlich: Es genügt, die „Einstellungen" bzw. „Settings" anzuwählen. Hier liegt in der Regel der Menüpunkt „Sperrbildschirm".

Handysektor – Bildschirmsperre

Passwortcheck

Ob bei Ihrem E-Mail-Account, Ihrem Online-Banking oder dem Einkaufsportal im Netz, meist werden Sie gebeten, ein Passwort zu vergeben. Wählen Sie ein sicheres Passwort und überprüfen Sie es mit einem Passwortcheck. Achten Sie auf seriöse Anbieter.

Loggen Sie sich nicht in unbekannten Umgebungen ein (z. B. offene Netzwerke, Internet-Cafés) und verschicken Sie Passwörter nicht per E-Mail. Verwenden Sie unterschiedliche Passwörter für verschiedene Apps und Geräte und speichern Sie Passwörter nicht im Browser* oder auf den Geräten (Ausnahme: Verwendung eines eigenständigen, seriösen Passwort-Managers*). Geben Sie die Passwörter nicht an andere weiter.

Weitere Informationen unter:

BSI – Sichere Passwörter erstellen

BLM – Passwortschutz

Die verschiedenen Zugangssperren:


Muster


PIN


Gesichts-Scan


Passwort


Iris


Intelligenter Scan


Fingerabdruck

Standort, Router und Verschlüsselung

Funknetze und drahtlose Zugänge wie WLAN*, Bluetooth* und NFC* sind praktisch. Sie ermöglichen aber auch Eindringlingen den Zugriff auf Ihre Geräte bzw. Daten. Daher sollte man diese Funktionen nur für den Zugang zu verschlüsselten, sicheren Netzwerken (= passwortgeschützt, WPA2- oder neuer WPA3-Standard*) und für den Austausch mit bekannten Geräten aktivieren. Bei offenen Netzwerken (Hotspots) ist Vorsicht geboten – hier können Ihre Daten leicht von Dritten mitgelesen werden. Nehmen Sie die Warnung vor einer unsicheren Verbindung ernst!

Achten Sie auf die Einstellung zu Ihrem **Standort**. Ein grobes Bewegungsprofil kann über die Einwahl des mobilen Gerätes in die jeweiligen Funkzellen des Mobilfunknetzwerkes erstellt werden. Auch eingeschaltetes WLAN und Bluetooth ermöglichen eine Positionsbestimmung – es sei denn, das Telefon ist ausgeschaltet oder im Flugmodus. Wesentlich genauere Standortdaten liefern die Daten des Satellitennavigationssystems (GPS).

TIPP

GPS-Funktion
GPS-Funktion nicht immer aktiviert lassen. Bedenken Sie: Viele Apps – und damit Unternehmen – sammeln Ihre Standortdaten, wenn Sie den Zugriff auf diese Informationen erlauben, selbst wenn Sie die App gerade nicht verwenden.

TIPP

WLAN, Bluetooth und NFC
Deaktivieren Sie nicht benötigte Dienste. Damit schonen Sie auch den Akku.

Über den „Flugmodus" können Sie schnell alle ausgehenden Signale abschalten und sich „unsichtbar" machen.

Beim Android-Smartphone vom oberen Displayrand nach unten wischen: Durch Antippen **WLAN, GPS** bzw. **Standort** und **Bluetooth** aktivieren oder deaktivieren.

Beim iPhone unter **Einstellungen → Datenschutz & Sicherheit → Ortungsdienste** können Sie die Standort-Abfrage über einen Schalter ein- und ausschalten.

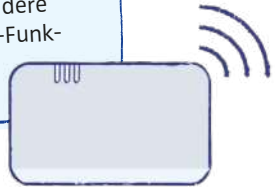
Ihr Internet-Router* ist das zentrale Element in Ihrem Heimnetzwerk. Da er meistens viele Geräte mit der „Außenwelt“ verbindet (z. B. mobile Geräte, Computer, Smart-TV), sollten Sie ihn in puncto Sicherheit nicht vernachlässigen.

TIPPS

Um Ihr Heimnetzwerk gut abzusichern, benötigen Sie zwei starke Passwörter:

- ein Gerätepasswort für Ihren **Router** (mindestens 15 Zeichen): Behalten Sie nicht das voreingestellte Passwort des Herstellers, das oft auf der Rückseite des Gerätes steht. Um das Gerätepasswort zu ändern, müssen Sie im Router angemeldet sein und den Bereich „Kennwort ändern“ aufsuchen.
- ein Passwort für Ihr **WLAN** (mindestens 20 Zeichen): Auch das WLAN-Passwort stellen Sie in Ihrem Router ein.

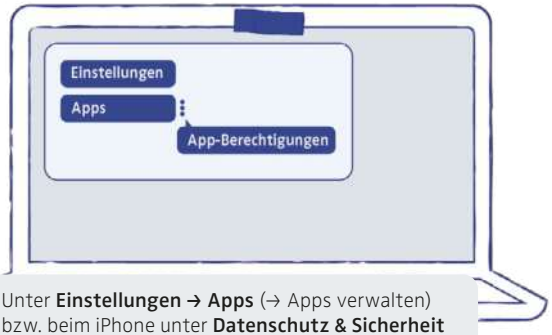
Sie können Ihr WLAN zusätzlich auch für andere unsichtbar machen (z. B. „Name des WLAN-Funknetzes sichtbar“ deaktivieren).



Das voreingestellte FRITZ!Box-Kennwort für den Zugang zu den Einstellungen Ihres Routers sollten Sie beim Erstzugang unter **System → FRITZ!Box-Benutzer** ändern.

Unter **WLAN → Sicherheit** wählen Sie den sicheren WPA-Modus „WPA2“ aus und richten dann einen sicheren Netzwerkschlüssel („WLAN-Passwort“) ein.

Eingebaute **Kameras** und **Mikrofone** können gehackt und zum Ausspionieren der Privatsphäre verwendet werden (z. B. Blick ins Wohnzimmer). Man kann die Kamera am Laptop mit einem Sticker oder Post-it überkleben, wenn man sie gar nicht braucht. Bei bestimmten Anwendungen (Videokonferenzen, Internet-Telefonie) und im alltäglichen Gebrauch von Smartphones sind Kamera und Mikrofon zumeist notwendig. Wird bei der Installation von Apps der Zugriff auf Kamera oder Mikrofon jedoch grundlos eingefordert, sollte man misstrauisch sein und auf die App verzichten.



Unter **Einstellungen → Apps** (→ Apps verwalten) bzw. beim iPhone unter **Datenschutz & Sicherheit** können Sie die **App-Berechtigungen** ändern.

TIPP

Überprüfen Sie bei Smartphones und Tablets, welche Gerätekomponenten (z. B. Standort/GPS, Kamera, Mikrofon, aber auch Kontakte, Kalender oder Speicher) für welche Apps freigegeben sind. In den Auswahlmenüs unter App-Berechtigungen können Sie bequem Berechtigungen sperren oder freigeben.

Eine Verschlüsselung* der Datenübertragung im Internet erkennt man in der Adresszeile des Browsers am **Schlosssymbol**, je nach Browser in Verbindung mit dem Kürzel **„https://" (Hyper Text Transfer Protocol Secure)**.

Es steht für ein sicheres Hypertext-Übertragungsprotokoll (anstelle des ungesicherten „http://", wobei inzwischen in vielen Browsern eine Warnung vor dem Besuch einer nicht gesicherten Website erscheint). Unter „https" werden die Daten über ein sicheres Übertragungsprotokoll transportiert. In manchen Browsern erscheint das Kürzel „https" nicht mehr, sondern nur das „Schlosssymbol".

Achtung: Das Schlosssymbol bietet keinen Schutz vor Phishing*, also dem Abgreifen von Daten über Mails oder Webseiten. Mittlerweile sind auch eine Vielzahl der Phishing-Seiten mit einem korrekten Zertifikat und dem Schlosssymbol ausgewiesen. Informieren Sie sich beim Bundesamt für Sicherheit in der Informationstechnik:

BSI – Verschlüsselung und Zertifikate

TIPP

Aktuelle Browser rufen inzwischen entweder automatisch https-Seiten auf oder können unter „Einstellungen" – „Datenschutz und Sicherheit" – ggf. „Erweitert" entsprechend eingestellt werden („Immer sichere Verbindungen verwenden").

Falls dies nicht geht: Über „Add-ons*" können Sie in fast jedem Browser die Sicherheits-Erweiterung „https-Everywhere" installieren. Damit wird – wenn möglich – immer automatisch die verschlüsselte Version eines Internetangebots aufgerufen.

Über den Bereich „Erweiterungen" können Sie in Ihrem Browser (z. B. Chrome, Firefox, Safari) kleine Sicherheitstools – Add-ons – installieren bzw. aktivieren.

Eine **Schutz-Software** ist Pflicht, denn es gibt ständig neue digitale Schädlinge wie Viren, Spyware, Trojaner oder Würmer. Sie können z. B. Geräte schädigen, persönliche Daten ausspionieren und zu kriminellen Zwecken missbrauchen. Achten Sie daher auch auf die Aktualität der grundlegenden Software (Firmware) bzw. des Betriebssystems.

TIPP

Auf allen Geräten – auch auf dem Smartphone – **Anti-Viren-Software** und eine Firewall* installieren und den automatischen Update-Modus einstellen.

CHIP – Sicherheit & Hilfe

Heise – AntiVirus

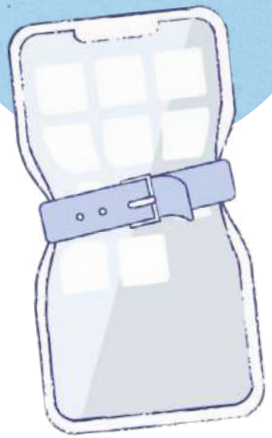
Installation von Apps

Seien Sie vor einer Installation besonders kritisch bei scheinbar kostenlosen Apps. Hier „bezahlen" Sie mit Werbeeinblendungen und mit Ihren Daten, die Anbieter zur Finanzierung ihrer Angebote nutze (→ siehe auch S. 22 zur Finanzierung von Social-Media-Plattformen).

TIPPS

Beachten Sie drei Schritte bei der Installation von Apps:

- **Vor einer Installation**
  Benötigen Sie die App wirklich?
  Installieren Sie die App nur aus einer vertrauenswürdigen Quelle. Das sind z. B. die App-Stores von Google, Apple oder Samsung. Sie sind auf dem Gerät vorinstalliert. Hier werden Apps vor der Bereitstellung auf ihre Sicherheit geprüft.
- **Während der Installation**
  Welche Berechtigungen fordert die App?
  Welche Daten auf Ihrem Gerät wollen Sie für die Verwendung der App freigeben und ist dies unbedingt notwendig?
- **Nach der Installation**
  Welche Privatsphäre-Einstellungen sind voreingestellt und sind diese ausreichend?
  Ändern Sie die Einstellungen gegebenenfalls.
  Wenn Sie eine App nicht mehr benötigen oder nur zum Testen heruntergeladen haben, deinstallieren Sie diese wieder.



App-Diät

Eine einfache Möglichkeit, um sich zu schützen, ist die Beschränkung auf seriöse und für Sie wirklich notwendige Apps. Überprüfen Sie regelmäßig Ihre Apps und deinstallieren Sie diejenigen, die Sie nicht oder kaum verwenden.

Elternhaus und Schule

In Elternhaus und Schule gelten die genannten Schutz- und Vorsichtsmaßnahmen zum Selbstdatenschutz nicht nur für „einen selbst", sondern Eltern sowie Lehrkräfte müssen auch auf ihre jungen „Schutzbefohlenen" achten. Kinder und Jugendliche kennen sich zwar häufig intuitiv mit Geräteanwendungen aus, aber es fehlt ihnen teilweise am Verständnis für den Schutz ihrer Daten. Sie sollten daher im Umgang mit Techniken und Geräten angeleitet und hinsichtlich Maßnahmen zum Selbstdatenschutz geschult werden. Wo dies an Grenzen stößt, können zumindest auch technische Zugangsbeschränkungen, Vereinbarungen oder Verbote sinnvoll sein.

TIPPS

- Sie können den Zugang zum Internet zeitweise ganz ausschalten – vor allem nachts.
- Wenn Sie nicht immer den Stecker des Internet-Routers ziehen möchten, können Sie beispielsweise mit einer Zeitschaltuhr arbeiten. Bestimmte Internet-Router verfügen über die Möglichkeit, eine **Nachtschaltung** zu aktivieren (z. B. FritzBox). Natürlich sind Sie selbst dann ebenfalls „offline".

- Sie können aber auch unterscheiden zwischen LAN-Verbindung (aktive Kabelverbindung für Ihren Computer) und WLAN (kabellos, nach Bedarf ein- oder ausgeschaltet).

Auch wenn es für Sie überflüssig klingt: Machen Sie Ihre Kinder darauf aufmerksam, dass die eigenen Passwörter wirklich geheim bleiben müssen. Es ist kein Freundschaftsbeweis, Passwörter weiterzugeben.

TIPPS

- Für Geräte sollten Sie bis zu einem Alter von ca. 12 Jahren **gemeinsame Nutzungszeiten** vereinbaren, in denen Sie Ihre Kinder unterstützen und begleiten. Hier können Sie gemeinsam einen „Mediennutzungsvertrag" schließen (mehr hierzu → siehe QR-Code und Link nächste Seite)
- Vereinbaren Sie **Nutzungspausen** oder behalten Sie insbesondere nachts die internetfähigen Geräte ein, wenn Sie der Meinung sind, dass Ihre Kinder leichtfertig agieren.

- Weisen Sie Ihre Kinder deutlich darauf hin: Bei Downloads und Anmeldungen im Internet sollten Sie grundsätzlich vorher informiert werden.
- Installieren Sie technische Schutzmaßnahmen wie Kinder- und Jugendschutzprogramme sowie Apps, z. B. „fragFINN", „JusProg" oder „Surfgarten". Zudem gibt es auch vorinstallierte anbieterseitige Schutzsysteme, die aber keiner neutralen Qualitätsüberprüfung unterliegen.

In der Schule ist zu unterscheiden:

Die Verwendung von eigenen Geräten der Schülerinnen und Schüler

Laut Gesetz müssen Mobilfunkgeräte und andere digitale Speichermedien im Bereich von Schulen in Bayern ausgeschaltet werden, wenn sie nicht im Unterricht verwendet werden. Bei Zuwiderhandlung können die Geräte einbehalten werden, Lehrkräfte können aber auch Ausnahmen zur Nutzung gestatten (vgl. Art. 56 Abs. 5 BayEUG).

Die Nutzung von Schultechnik und Geräten im Unterricht

Im Idealfall werden die Geräte und Software von einem Administrator der Schule gepflegt und auf dem aktuellsten Sicherheitsstand gehalten. Schulungen zu Sicherheitseinstellungen erscheinen sinnvoll. WLAN ist an Schulen umstritten, da die Gefahr des unkontrollierten Zugangs besteht und damit des Missbrauchs, z. B. durch illegale Downloads.

TIPPS

Für die Nutzung des Internets im Unterricht gilt:

- Holen Sie die schriftliche Zustimmung der Eltern (und ab 14 Jahren auch der Schülerinnen und Schüler) ein und klären Sie die Vorgehensweise mit der jeweiligen Schule ab.
- Lassen Sie die Verwendung von „Nicknames" (Pseudonymen) statt Klarnamen zu. Dies gilt auch wenn Sie mit anmeldepflichtigen Anwendungen im Internet arbeiten (externe E-Mail-Adressen, Cloud-Dienste*).

Weitere TIPPS → siehe Seite 36/37

Weitere Informationen unter:

Internet-ABC – Mediennutzungsvertrag

Internet-ABC – Internet im Unterricht

BLM – Infobroschüre Apps

2. Kommunikation im Internet

Einfach nur Gespräche führen mit dem Telefon – das war einmal. Heute besitzen fast alle ein Smartphone und selbst einfache Modelle sind Multifunktionsgeräte mit einer Vielzahl an Informations-, Unterhaltungs- und Kommunikationsmöglichkeiten: Telefonate sind über die normale Gesprächsfunktion oder über Internet-Telefonie mithilfe von Apps möglich (z. B. Skype, Jitsi oder in Messengern wie WhatsApp, Threema und Signal). Mit einigen dieser Apps kann man sich zusätzlich per Video sehen und Konferenzschaltungen mit mehr als zwei Personen einrichten (zu den eigentlichen Meeting-Tools → siehe ab Seite 34).

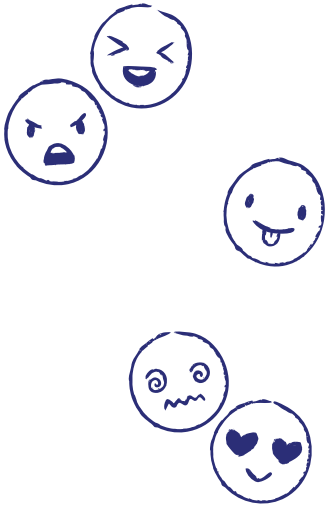
Messenger-Dienste

Textnachrichten können mit Messenger-Apps oder per E-Mail versendet werden, zunehmend seltener geschieht dies per SMS. Über **Messenger-Dienste** (z. B. WhatsApp oder die als datensicherer eingestuften Alternativen Threema und Signal) können neben Textnachrichten auch Sprachdateien, Fotos und Videos versendet und Gruppenchats eingerichtet werden. Threema hat den großen Vorteil, dass die Nutzung auch ohne Telefonnummer und Telefonbuchabgleich möglich ist, allerdings ist die App bei der Einrichtung kostenpflichtig, kann dann

aber unbefristet kostenfrei genutzt werden. Manche Anbieter verzichten auf eine vollständige Ende-zu-Ende-Verschlüsselung für all diese Funktionen; sie bewirkt, dass Daten generell nicht mitgelesen werden können. Einige Messenger-Dienste bedienen sich Ihrer persönlichen Kontaktliste, um die App zu installieren – diese Daten können beim Anbieter gespeichert werden. So gehören WhatsApp und der Facebook-Messenger zum Meta-Konzern (vormals Facebook), der diese Daten mit vielen weiteren Informationen, z. B. auch aus dem sozialen Netzwerk Facebook, verknüpfen kann. Nebenbei entsteht so ein umfangreiches Bild über die Gewohnheiten und Vorlieben der Nutzenden.

TIPPS

- Überlegen Sie sich, ob Sie eine Messenger-App wirklich benötigen. Informieren Sie sich über mögliche Alternativen zu WhatsApp, die mit vollständiger Ende-zu-Ende-Verschlüsselung (z. B. Threema, Signal) arbeiten. Versuchen Sie Ihre Kontakte davon zu überzeugen, mit Ihnen den Messenger zu wechseln.
- Denken Sie daran, dass übermittelte Fotos oder Videos auf dem Gerät des Empfängers abgelegt werden. Dieser kann sie ohne Ihr Wissen speichern oder weiterleiten.
- Einige Messenger bieten eine automatische Löschung von Nachrichten oder Fotos nach einer gewissen Zeit oder die Funktionen nur einmalig anzeigbarer Medien an („Verschwindende Nachrichten", z. B. Snapchat). Aber auch hier sind Screenshots möglich.
- Wenn Sie unsicher sind, um welche Person es sich bei Ihrem Gegenüber handelt, können Sie diese blockieren bzw. „stummschalten".
- Zeigen Sie Beleidigungen, sexuelle Belästigungen oder Erpressungsversuche bei der Polizei an. Fertigen Sie hierzu Screenshots („Bildschirmfotos") zur Beweissicherung an.



Die Entwicklungen bei Messengern sind schnelllebig – aktuelle Apps finden Sie hier:

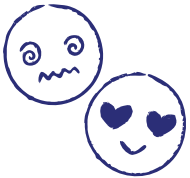
Handysektor – App-Tests

Verbraucherzentrale – Messenger im Überblick

TIPPS

- Überprüfen Sie immer die Privatsphäre-Einstellungen (z. B. Synchronisation, Online-Status, Konto löschen).
- Überlegen Sie genau, wer Ihre persönlichen Informationen, das Profilbild und den Online-Status sehen darf. Wählen Sie zwischen „Niemand", „Meine Kontakte außer...", „Meine Kontakte" bzw. „alle".

Bsp.: WhatsApp, über → drei Punkte am oberen Rand (bzw. bei iPhone in der unteren Leiste) → **Einstellungen** → **Datenschutz** → **Zuletzt online** → Option **Niemand** auswählen



E-Mails

Auch bei E-Mails gelten das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis, welche durch das Grundgesetz geschützt sind. Doch in der Praxis sind E-Mails gegen das „Mitlesen" durch Unbefugte nur sehr schwer zu schützen.

TIPPS

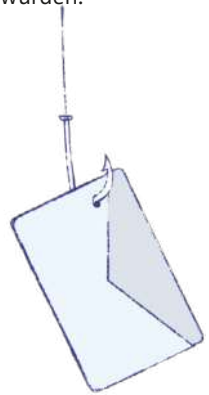
- **Senden Sie wichtige E-Mails auf einem verschlüsselten Übertragungsweg.** Selbst bei einer verschlüsselten Datenleitung können Sicherheitslücken am Gerät z. B. beim Senden und Empfangen bestehen. Bei der Nutzung eines eigenen E-Mail-Programms (z. B. Outlook, Thunderbird) auf Ihrem Gerät sollten Sie bei den Server-Einstellungen eine verschlüsselte Verbindung (Verschlüsselungsprotokolle veraltet: SSL/verbessert: TLS) und eine Authentifizierung mit Passwort auswählen.
- Freemail-Anbieter im Internet (z. B. Gmail, GMX, Yahoo, Web.de) verwenden verschlüsselte Datenleitungen, analysieren aber ihre E-Mail-Inhalte für Werbeeinblendungen und das Ausfiltern von Spam.

Auch der Inhalt der E-Mail sollte verschlüsselt werden. Hierfür ist eine Reihe von Schritten notwendig. Eine Anleitung finden Sie beispielsweise unter:

BSI – E-Mails verschlüsseln

Vorsicht auch beim E-Mail-Empfang: Über E-Mails werden nicht nur lästige Werbeinhalte, sondern auch gefährliche Schadprogramme verbreitet. Schädliche Viren- und betrügerische **Phishing-Mails** zum „Abfischen" persönlicher (Bank-)Daten werden immer professioneller. Die Zeiten, in denen man sie an schlecht gefälschten Firmenlogos und vielen Rechtschreibfehlern eindeutig erkennen konnte, sind vorbei. Testen Sie, ob Ihre Daten schon ausspioniert wurden:

hpi – Identity Leak Checker



TIPPS

- Öffnen Sie keine **Anhänge** oder **Links** in E-Mails von Unbekannten.
- Passen Sie aber auch auf, wenn Sie merkwürdige E-Mails von Bekannten erhalten – immer häufiger werden eigentlich vertrauenswürdige Identitäten bei Täuschungsversuchen missbraucht (Mail-Spoofing).
- Deaktivieren Sie ggf. die **HTML-Ansicht** in Ihrem E-Mail-Programm. Damit werden auch die in einer E-Mail eingebetteten Inhalte, die gefährlich sind, deaktiviert.
- Versenden Sie keine persönlichen Daten und erst recht niemals Bankdaten, selbst wenn Sie dazu aufgefordert werden, weil dies angeblich „Ihrer Sicherheit" dient.
- Legen Sie sich neben einer seriösen **E-Mail-Adresse** (für Arbeits- und Geschäftsleben) auch mindestens eine anonymisierte E-Mail-Adresse unter einem Pseudonym zu. Damit können Sie z. B. Newsletter abonnieren oder eine Anmeldung bei einem Angebot im Internet ausprobieren, ohne dass Ihre seriöse E-Mail-Adresse weiterverkauft und mit Spam überschüttet wird.

Kinder und Jugendliche nutzen Messenger-Apps, insbesondere WhatsApp, Snapchat, Threema oder Signal, um miteinander in Kontakt zu bleiben. Sprechen Sie mit Ihren Schützlingen sowohl über Risiken (z. B. Datenmissbrauch, Mobbing, falsche Freunde) als auch über Chancen der Internet-Kommunikation (z. B. Zusammenhalt, Austausch und Vernetzung, Information, Spaß). Viele Kinder und Jugendliche sind zwar kompetent in der Handhabung von Geräten und Apps, aber oftmals unvorsichtig, wenn es um ihre eigene Sicherheit geht. Bedenken Sie: Falls Ihren Schutzbefohlenen etwas misslingt, schaffen Schuldzuweisungen und Verbote kein Vertrauen.

TIPPS

- Bieten Sie Ihre Unterstützung an. Achten Sie dabei auf die Privatsphäre Ihrer Schützlinge. Je nach Alter nehmen Sie Downloads und Anmeldungen bei Apps nach Möglichkeit zusammen mit Ihren Kindern vor.
- Überprüfen Sie die Privatsphäre-Einstellungen gemeinsam und deaktivieren Sie automatische Downloads.
- Machen Sie Ihre Kinder darauf aufmerksam: Nachname, Adresse, Geburtsdatum und Telefonnummern sowie (intime) Fotos und Videos werden nicht an Unbekannte weitergegeben.
- Besprechen und erproben Sie die Möglichkeit einer anonymen Anmeldung bei einem Internet-Angebot.
- Wichtig ist es, das Angebot auf privat zu stellen, damit nicht alle Bilder öffentlich werden.

Die Nutzung von **WhatsApp** ist nach den Nutzungsbedingungen erst ab 16 Jahren erlaubt, mit Zustimmung der Eltern aber auch schon ab 13 Jahren möglich (Grund sind die Vorschriften der DSGVO zur Datenverarbeitung). Ähnliches gilt für Snapchat. Hier ist die Nutzung ohne elterliche Einwilligung nach Angaben des Anbieters erst ab 18 Jahren erlaubt. Neugierde, Gruppendruck und die geringere Verbreitung anderer Messenger-Apps treiben Kinder und jüngere Jugendliche zu beiden Messenger-Diensten. Ein Verbot der Installation auf dem Gerät wäre möglich, ist aber mit einer dauerhaften Kontrolle verbunden und daher kaum durchführbar.

TIPPS

Weisen Sie auf die kritischen Punkte bei der Nutzung von **WhatsApp** hin:

- Übertragung der Kontaktdaten
- Onlinestatus bei Anmeldung öffentlich voreingestellt
- Mobbing-Gefahr
- Kettenbriefe
- Erreichbarkeitsdruck
- Zugriffsberechtigungen der App auf Daten, die für die Funktionsfähigkeit der App nicht erforderlich sind

Zeigen Sie Ihren Kindern, deren Freundeskreis und auch den Lehrkräften Alternativen auf und besprechen Sie Handlungsoptionen. Der Wechsel zu einer App wie **Threema** oder **Signal** gelingt nur, wenn viele mitmachen.

Weitere Informationen unter:

Handysektor – WhatsApp

klicksafe – WhatsApp-Alternativen

Medienkompetenz sollte bereits in der Schule vermittelt werden, um anschließend in Ausbildung und im Beruf überlegt über das Internet kommunizieren zu können. Digitale Kommunikationswege können im schulischen Kontext geübt werden. Einsatzmöglichkeiten sind – in Ergänzung zur mündlichen Verständigung im Unterricht – beispielsweise der schriftliche Austausch über Termine und Inhalte (Wissen, Lernmaterialien, Aufgaben). Dies kann z. B. per Gruppenchat, E-Mail, über eine Kommunikationsplattform (wie mebis) oder einen Messenger-Dienst – gerade auch im Krankheitsfall – geschehen.

TIPP

Die gängigsten Anwendungen bzw. Apps sind selten auch die datenschutzfreundlichsten. Gehen Sie mit gutem Beispiel voran und versuchen Sie, zu Hause sowie für Unterricht und Klassenkommunikation alternative Angebote zu nutzen oder anzuregen. Möglicherweise ist dies mit (meist geringen Einmal-)Kosten verbunden.

TIPPS

- **Telefon- und Videokonferenzen**
  Visavid, Jitsi, BigBlueButton, Nextcloud Talk statt Skype, Zoom und Teams
- **Messenger**
  Threema, Signal statt WhatsApp, Snapchat
- **E-Mail**
  Schuleigenes Web-Hosting mit eigenen E-Mail-Adressen statt Freemail-Angebote
- **Gesamtlösungen**
  Plattformen wie mebis, BigBlueButton und Moodle mit individuell einstellbaren Kommunikationsmöglichkeiten
- **Altersgrenzen**
  Bei allen Angeboten auf die Altersgrenzen für die Nutzung achten und die Zustimmung der Eltern einholen.

Weitere Informationen unter:

BLM – Materialien

mobilsicher – Messenger-Apps im Sicherheits-Check

3. Selbstdarstellung auf Social-Media-Plattformen

Die Übergänge zu Messengern sind zwar fließend, aber Social-Media-Plattformen zeichnen sich deutlicher durch die Möglichkeiten der Selbstdarstellung mit Texten, Fotos und Videos in einem eigenen Profil aus. Ebenso wichtig sind die Vernetzung und der Austausch mit anderen Nutzerinnen und Nutzern. Beliebte Social-Media-Plattformen sind **Instagram, YouTube, TikTok und Facebook.** Auch **Twitter**, eigentlich ein Mikroblogging-Dienst für kurze Textnachrichten, wird hier oft hinzugezählt. Einige Netzwerke wie z. B. LinkedIn und XING sind auf berufliche Kontakte spezialisiert.

Finanzierung

Die Social-Media-Anbieter stellen ihre Angebote kostenfrei zur Verfügung. Um dies finanzieren zu können, verkaufen sie die Nutzerdaten (Anmeldedaten sowie Nutzungsgewohnheiten – Tracking*) an Werbetreibende. Die (offensichtliche oder versteckte) Werbung auf Social-Media-Plattformen kann in mehreren Formen auftreten:

- durch Anzeigen, die sich je nach Privatsphäre-Einstellung am Nutzungsverhalten orientieren,
- durch bezahlte Beiträge z. B. von Unternehmen (diese müssen als Werbung gekennzeichnet sein, sind es aber nicht immer) und
- durch Produktplatzierungen oder ausführliche Produktpräsentationen in den Profilen sog. Influencerinnen und Influencer*.

Weitere Informationen unter:

Die Medienanstalten – Werbekennzeichnung

Anmeldemöglichkeiten

Für die aktive Teilnahme bei den Netzwerken – und manchmal sogar auch nur für das Anschauen von Inhalten – ist eine Anmeldung erforderlich. Dann können Sie eigene Beiträge verfassen bzw. posten, andere, die Ihnen gefallen, per Klick auf einen Button „liken" oder ganzen Profilen folgen und damit Ihr Netzwerk vergrößern – denn das ist eines der Ziele von Social-Media-Plattformen.

• Vielleicht muss Ihr Profil gar nicht öffentlich sichtbar sein, sondern nur für ausgewählte Freunde und Bekannte? Meistens kann man einen Account auf „privat" stellen (beachten Sie auch die TIPPs unter „Elternhaus und Schule").

TIPPS

• Sie wollen nur einmal in eine Social-Media-Plattform „hereinschauen" und selbst nicht gefunden werden oder aktiv teilnehmen? Dann testen Sie die Teilnahme, indem Sie sich mit einer anonymisierten E-Mail-Adresse unter einem Pseudonym anmelden. Dies schützt Sie teilweise auch vor einer Weiterverwertung Ihrer persönlichen Daten.

• Auch wenn Sie unter einem Pseudonym aktiv sind, können Sie aufgrund der Metadaten zumindest von den Netzwerkanbietern trotzdem identifiziert werden (z. B. IP-Adresse*, Ort, Zeit, Verlinkungen, Interaktionen wie Likes, Hashtags etc.).

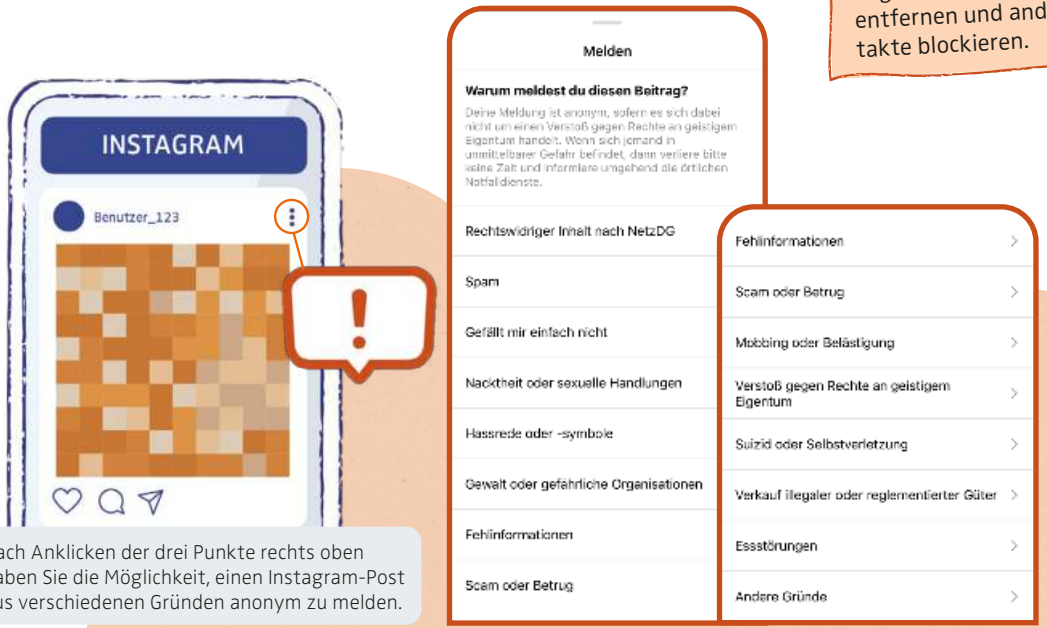
Sie wollen sich für eine Stelle oder einen Ausbildungsplatz bewerben? Denken Sie daran: Viele Arbeitgeber recherchieren Informationen über neue Mitarbeiterinnen und Mitarbeiter auch in den Profilen im Internet. Entscheiden Sie selbst, welchen Eindruck Sie hinterlassen wollen!

Problematische Inhalte

Anonymisierte Anmeldungen haben Vor- und Nachteile: Sie werden von Nutzerinnen und Nutzern nicht nur zum Schutz vor Datensammlung genutzt, sondern auch zum Schutz vor persönlichen Beleidigungen, **Hate Speech** (Hassrede, Hetze) oder Mobbing. Einige Personen, die Fake News (absichtliche Falschinformationen), Hate Speech oder sexuelle Belästigungen verbreiten, verwenden Pseudonyme, aber auch, um sich einer möglichen Strafverfolgung zu entziehen.

TIPPS

- Zeigen Sie entsprechende Taten bei der Polizei an, denn Täter können meistens trotzdem ermittelt werden.
- Nutzen Sie die Möglichkeit, unangemessene Beiträge bei den Anbietern zu melden. Diese Möglichkeit finden Sie oft etwas versteckt unter den drei Punkten am oberen Rand.
- Sie können auch Beiträge, die bei Ihnen angezeigt werden, aus Ihrer Timeline entfernen und andere Profile oder Kontakte blockieren.



Nach Anklicken der drei Punkte rechts oben haben Sie die Möglichkeit, einen Instagram-Post aus verschiedenen Gründen anonym zu melden.

Elternhaus und Schule

Social-Media-Plattformen bieten viele Möglichkeiten, selbst aktiv zu werden. Mit Postings bzw. Fotos und Videos auf **Instagram, TikTok** und **YouTube** geben die Userinnen und User oft sehr viel Persönliches von sich preis. Vor allem junge Menschen agieren im **„Mitmachnetz“** unbefangen: Es geht ihnen um Spaß und Unterhaltung, Vernetzung und kreativen Selbstausdruck; weniger um Vorsicht und Zurückhaltung, auch was persönliche Daten betrifft.

Viele der bei jungen Menschen besonders populären Dienste gehören zu den großen amerikanischen Technologieunternehmen, die somit immer mehr Daten von Internetnutzenden auswerten, z. B. Meta Platforms Inc. (WhatsApp, Instagram, Facebook) sowie Google LLC (YouTube ist eine Tochtergesellschaft). Aber auch TikTok ist wegen seiner Herkunft aus China mit großer Vorsicht zu betrachten – Selbstdatenschutz ist also gefragt. Zwar wissen die meisten, dass ihre Daten die Basis der Finanzierung solcher Angebote sind. Doch was genau gespeichert, übermittelt und analysiert wird, bleibt in den umfangreichen Datenschutzrichtlinien und Allgemeinen Geschäftsbedingungen nebulös.

Oft fühlen sich Kinder und Jugendliche hinsichtlich des Schutzes ihrer Daten in den Netzwerken sicher und offenbaren hier nicht nur von sich, sondern auch von anderen zu viel.

TIPPS

- Achten Sie darauf, dass Ihre Schützlinge in Texten, Bildern oder Videos nicht zu viel Persönliches von sich und anderen in die Social-Media-Angebote einstellen. Wie das Internet allgemein, „vergessen“ auch diese Netzwerke nichts.
- Noch unerfahrene Heranwachsende müssen dafür sensibilisiert werden, dass sie Daten, Fotos oder Videos von und mit anderen (z. B. ihren Freunden, Lehrkräften und Eltern) nicht ohne deren Erlaubnis posten dürfen. Dies folgt aus dem Recht am eigenen Bild.

Weitere Informationen unter:

BLM – Recht am eigenen Bild

Umgekehrt sollten sich Heranwachsende bewusst machen, dass ihre auf privaten Profilen eingestellten eigenen Daten und Bilder von anderen mit einem Screenshot dauerhaft gespeichert und missbräuchlich – ohne Einholung einer entsprechenden Erlaubnis – öffentlich gemacht werden können (auch vermeintlich kurzlebige Fotos z. B. auf Snapchat). Wählen Sie für Profilinformationen und Beiträge restriktive Privatsphäre-Einstellungen.

Weitere Informationen unter:

Klicksafe –
Apps für Kinder

Handysektor –
App-Tests

Eine besondere Bedeutung haben Videoplattformen für junge Menschen: **YouTube** und **YouTube Shorts** nutzen die meisten täglich, um sich Videos, Clips oder zeitversetzt Fernsehinhalte anzusehen.

Angemeldet im persönlichen Konto werden die mit Cookies nachverfolgten Spuren mit den Daten der anderen Google-Dienste zusammengeführt. Diejenigen, die hier oder auch bei anderen sehr beliebten Apps wie **TikTok** und **Snapchat** selbst Videos hochladen, sollten bewusst entscheiden, ob sie diese öffentlich und damit für alle sichtbar einstellen.

Erläutern Sie die Vor- und Nachteile von personalisierter und **anonymisierter Nutzung**. Wenn Sie oder Ihre Kinder bei **YouTube** weitgehend anonym Videos sehen wollen, melden Sie sich nicht an und nutzen Sie die beschriebenen Browser-Einstellungen und -Erweiterungen, um Cookies zu unterbinden.

TIPPS

Beim **Einstellen von Videos**, für das eine Anmeldung beim Anbieter notwendig ist, ist auf Folgendes zu achten:

- keine persönlichen Informationen veröffentlichen (Name, Adresse, Telefonnummer etc.)
- Minderjährige nicht sexualitätsbezogen darstellen
- keine Dritten ohne deren Erlaubnis abbilden

Wichtig ist, dass keine urheberrechtlich geschützten Songs, Musikvideos oder Filmaufnahmen verwendet werden.

Weitere Informationen unter:

BLM –
Urheberrecht

TIPP

Weisen Sie auf die Veröffentlichungsoptionen beim Hochladen von Videos auf YouTube hin. Eingestellte Videos (standardmäßig: „öffentlich") können auch noch rückwirkend nach einer Veröffentlichung „privat" gestellt werden.

Unter **Video-Manager** → Option **Bearbeiten** wählen → **Öffentlich** anklicken → **Privat** auswählen.

Auch bei anderen Apps (z. B. TikTok) kann das Profil jederzeit auf „privat" gestellt werden.

Bei TikTok kann unten rechts auf das Profilbild geklickt werden → auf die drei Punkte/Striche oben rechts → **Datenschutz** → **privates Konto** einstellen

Der „Leitfaden für Beschäftigte der Staatsverwaltung zum Umgang mit Sozialen Medien" sensibilisiert Lehrkräfte für die Besonderheiten von Social-Media-Angeboten und empfiehlt bei der privaten Kommunikation mit Schülern und Eltern ein verantwortungsvolles Handeln.

Aus Gründen des Selbstdatenschutzes und aus rechtlichen Gründen ist die Nutzung von **WhatsApp** und **Facebook** im schulischen Kontext eigentlich tabu. Lehrkräfte sollten WhatsApp- und Facebook-Gruppen nicht für schulische Zwecke nutzen. Wer Stundenpläne, Arbeitsblätter, Noten etc. nur (noch) hier bekannt gibt, zwingt (einzelne) Schülerinnen oder Schüler zu ihrer Nutzung und kann unter Umständen eine Vermischung schulischer und privater Informationen nicht vermeiden.

Weitere Informationen unter:

mebis – Infoportal

BLM – Materialien

4. Unterhaltung über Streamingdienste

Filme, Fernsehsendungen oder Internetvideos üben eine starke Faszination aus. Diese Bewegtbilder nehmen nicht nur über den Konsum von Videoschnipseln in den Social-Media-Angeboten, sondern gerade auch durch die Nutzung von Streamingangeboten einen zentralen Stellenwert in der alltäglichen Unterhaltung ein.

Wie Computer, Smartphones und Tablets sind auch Fernsehgeräte inzwischen als „Smart-TV" für die Nutzung von Online-Angeboten häufig mit dem Internet verbunden.

Kostenpflichtige Streamingangebote bieten Filme oder Serien ohne Werbeunterbrechung. Einige der Angebote können direkt über einen Internetbrowser angewählt werden, für andere sind spezielle Apps erforderlich.

Anmeldung und Nutzung

Bei der Nutzung aller Angebote werden Daten gesammelt. Dies geschieht einmal durch Ihre Anmeldung, was bei Bezahlangeboten natürlich unumgänglich ist, zum anderen aber auch durch Ihr Nutzungsverhalten. Verwenden Sie auch hier ein sicheres Passwort, damit nicht Fremde auf Ihren Account zugreifen.

Hinter besonders günstigen (Video-)Angeboten, die oft ganz ähnliche Namen wie bekannte Plattformen verwenden (z. B. „...stream", „i-..." oder „...flix"), stecken oft betrügerische Absichten: Verbraucherzentralen und die Polizei warnen vor unseriösen Abo-Fallen und Drohungen durch Inkassobüros.

Viele Anbieter ermöglichen Ihnen einen kostenfreien Probemonat, damit Sie das Angebot kennenlernen können. Vorsicht: Vergessen Sie nicht, rechtzeitig zu kündigen, sonst werden Sie automatisch zu einem zahlenden Abonnenten. Denn Ihre Bankverbindung müssen Sie meistens auch schon für den Probezeitraum bei Ihrer Anmeldung hinterlegen (oder sie ist schon hinterlegt, z. B. bei Amazon). Allerdings sind die Kündigungsfristen inzwischen kundenfreundlicher. Eine Abmeldung aus einem Abonnement ist oft schon nach einem Monat möglich.

TIPPS

- Mit einer **Abo-Kündigung** sollten Sie auch die Aufforderung verbinden, Ihre Daten (Adress-, Zahlungs- und Nutzungsdaten) vollständig löschen zu lassen.
- Daten zu Ihrem Nutzungsverhalten und Ihren Geräten werden durch die Verwendung von **Cookies** gesammelt – auch an Ihrem Smart-TV. Diese können Sie löschen. „Kostenlose" Anbieter richten die Werbeclips oder -anzeigen, die Sie zu sehen bekommen, meist nach Ihrem Nutzungsverhalten aus.

TIPP

- Ihre Rückmeldungen, z. B. durch Bewertungen von Videos („Gefällt mir"-Button), sind ebenfalls Informationen, die von den Anbietern gesammelt und dafür genutzt werden, Ihnen Video-Vorschläge zu machen.

Es gibt kostenfreie und kostenpflichtige Streamingdienste, die sich über einen Internetbrowser oder spezielle Apps auf allen genannten Gerätetypen nutzen lassen.

Kostenfreie Angebote

- Besonders bekannt sind etwa die Mediatheken von ARD und ZDF (mit allen zugehörigen Regional- und Spartenprogrammen).
- Manche privaten Fernsehsender bieten eine Auswahl ihrer Sendungen ebenfalls kostenfrei über das Internet an.
- Einige Internet-Plattformen wie YouTube und Vimeo ermöglichen auch Interaktionen, z. B. das Hochladen von Videos in eigene Profile (→ siehe Kapitel 3).

Kostenpflichtige Angebote

• Es gibt Streamingportale, die Bestandteil eines größeren Unternehmens sind (z. B. Amazon Prime Video, Apple TV, Disney+).

• Andere etablierte Portale sind eigenständig (z. B. Netflix).

• Kostenpflichtige Angebote können meist nur per Abonnement dauerhaft genutzt werden. Dafür werden Filme und Serien ohne Werbeunterbrechung angeboten.

• Je nach Abo-Modell und Kosten können Sie das Angebot dann nur auf einem Gerät oder zeitgleich auf mehreren Geräten (möglicherweise nur aus einem Haushalt) nutzen.

• Manchmal gibt es aber auch die Möglichkeit, für einzelne Filme bzw. Videos zu bezahlen („Pay-per-View").

• Für Musik gibt es ebenfalls Streamingangebote (z. B. Spotify, Apple Music). Diese ähneln hinsichtlich ihrer Nutzung und hinsichtlich ihrer Angebotsvarianten der Gestaltung von Video-Plattformen.

TIPPS

Für die Änderung der eigenen Nutzungseinstellungen gibt es zwei Bereiche:

• Die **App-Einstellungen** beziehen sich eher auf das jeweilige Gerät, hier können Sie Benachrichtigungen zulassen oder abstellen, die Download-Videoqualität bestimmen und Cookie-Einstellungen ändern.

• In den **Konto-Einstellungen** können Sie nicht nur Ihre Abo-Mitgliedsdaten anpassen, sondern auch viele andere relevante Änderungen vornehmen, z. B. genutzte Geräte und Ihre Streamingaktivität überblicken (dies hilft zu erkennen, ob Fremde auf Ihr Abo zugreifen).

• Meist können Sie hier auch alle über Sie gespeicherten Nutzungsdaten beim Angebot in Datenform anfordern.

TIPPS

Ein Blick in die Einstellungen lohnt sich:

- Neben den Voreinstellungen für Sprache und Untertitel können Sie auch das automatische Abspielen des nächsten Videos (Autoplay) abstellen.
- Netflix und Amazon Prime ermöglichen es, für alle Nutzerinnen und Nutzer einer Familie individuelle Accounts einzurichten. Für Kinder bis 12 Jahre kann ein spezielles Kinderprofil mit eingeschränktem Nutzungsangebot eingerichtet werden
- Bei Spotify kann man Inhalte, die als unangemessen gekennzeichnet sind, deaktivieren, auch für einzelne Abomitglieder, bspw. Kinder bei einem Family Abo.

Früher wurde vor einem eigenen Fernseher im Kinderzimmer gewarnt – heute eher vor dem unkontrollierten Zugang ins Internet, auch zu Streamingportalen.
Der Vorteil der zeitunabhängigen Nutzung sinnvoller Inhalte wird mit Blick auf Kinder (und jüngere Jugendliche) für viele Eltern sowie Pädagoginnen und Pädagogen schnell zum Nachteil: Es finden sich insbesondere viele Videos, bei denen es Probleme mit der Altersfreigabe bzw. dem Jugendschutz geben kann. Hinzu kommen eine ausufernde Nutzungsdauer und den Schlafrhythmus störende Uhrzeiten. Übrigens: Auch Erwachsene sind anfällig für „Binge-Watching", dem Schauen eines stundenlangen Serienmarathons. Denken Sie also daran, dass Ihr Verhalten eine Vorbildfunktion für Ihre Kinder hat!

Schutzeinstellungen, die von den Eltern eingesetzt werden, können einerseits helfen, die Nutzung ungeeigneter Inhalte zu verhindern. Andererseits können sie auch genutzt werden, um das Konsumverhalten der Kinder auf geeignete Inhalte zu lenken und diese mit ihnen zu besprechen. Auf jeden Fall sollten Nutzungszeiten immer mit den Minderjährigen abgesprochen werden.

Grundsätzlich gilt: Die Schutzmöglichkeiten bei der Nutzung der einzelnen Streamingangebote weichen stark voneinander ab. Das Mindestalter ist meistens 18 Jahre (oder ab 16 Jahren mit Zustimmung der Eltern).

TIPPS

- Sie können unter **Profile bearbeiten** (oder „verwalten", „hinzufügen") für Ihre Kinder ein eigenes Profil im Kinderbereich anlegen.
- Für ältere Kinder und jüngere Jugendliche kann ein eigenes Profil mit eingeschränkter **Altersfreigabe** eingerichtet werden.
- Da alle Profile mit einer **PIN** geschützt sind, haben Ihre Kinder dann keinen Zugriff auf ungeeignete Inhalte. Voraussetzung: Sie geben Ihren Kindern nicht die Profil-Passwörter.

TIPP

Nur Sie können die Profile und die zugehörigen Sicherheitseinstellungen verwalten. Dies sind z. B. allgemeine Altersfreigaben und/oder die Sperrung bestimmter Titel, Deaktivierung von Vorschau und Autoplay-Funktion, ggf. Kaufbeschränkungen.

(Weitere TIPPs → siehe Seite 30/31)

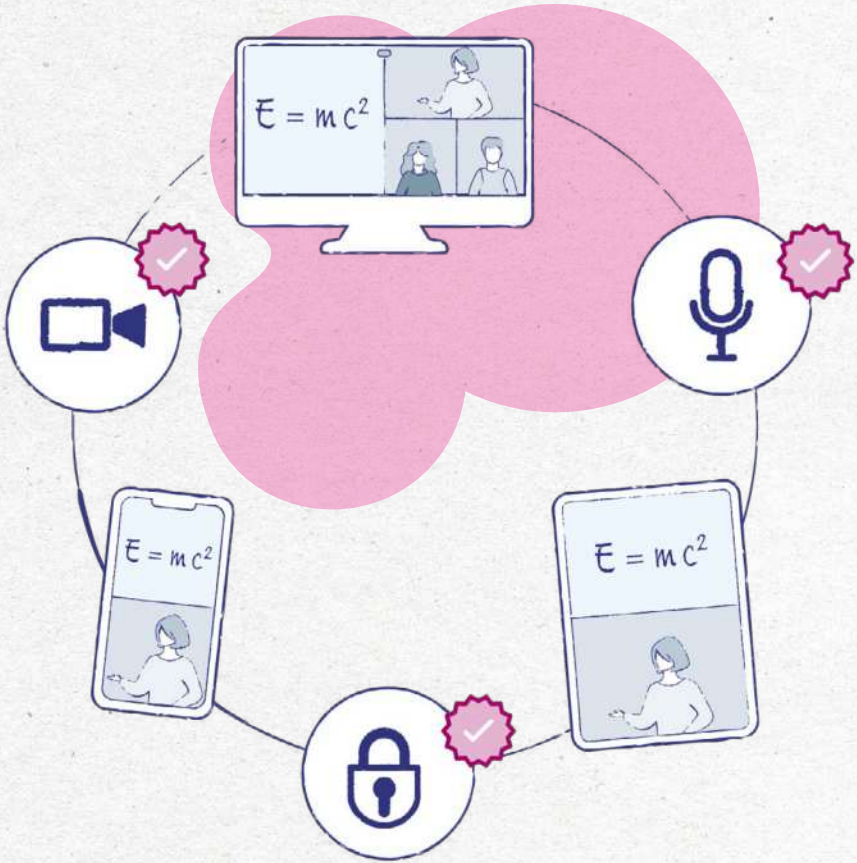
Weitere Informationen unter:

klicksafe – Streamingdienste

FLIMMO – Elternratgeber für TV, Streaming & YouTube

Zumeist gibt es orientierende Hinweise zum Inhalt des Films oder der Serie und einen Trailer – Sie können sich zumindest diesen gemeinsam mit Ihrem Kind ansehen oder die ganze Zeit gemeinsam schauen. Beachten Sie auch: Die Altersangaben der Streaming-Anbieter variieren nicht nur untereinander, sondern weichen auch von den Altersfreigaben der Freiwilligen Selbstkontrolle der Filmwirtschaft (FSK) ab. Beides sind keine pädagogischen Altersempfehlungen. FSK-Freigaben besagen, dass die Inhalte des Angebotes für Kinder unter dieser Altersstufe entwicklungsbeeinträchtigend sein können.

5. Meeting- und Lernplattformen



Bei großen Unternehmen und Bildungseinrichtungen werden **Videokonferenzsysteme** und **Arbeitsplattformen** schon länger genutzt. Seit der Covid-Pandemie gehören Meeting-Tools und Lernplattformen im Rahmen von **Homeoffice** und Homeschooling zum Alltag vieler Menschen. Digitale Tools für die Online-Zusammenarbeit („Collaboration-Tools") ermöglichen, dass sich Personen örtlich und zeitlich unabhängig voneinander schriftlich und sprachlich miteinander austauschen können.

Hinweise zur Nutzung

Voraussetzungen für die Nutzung derartiger Tools sind entsprechend ausgestattete Geräte mit Mikrofon und Kamera sowie einer möglichst leistungsfähigen Internetverbindung. Bei der Nutzung derartiger Meeting-Tools können Sie prüfen, ob diese ihren Sitz in der EU bzw. im europäischen Wirtschaftsraum haben und dort ihre Daten verarbeiten. Gängige Tools wie Google Meet, Microsoft Teams, Skype und Zoom verarbeiten ihre Daten zumeist nicht in der EU. Alternativen sind Visavid, Jitsi, BigBlueButton und Nextcloud Talk.

Sicherheitsvorkehrungen

Es ist wichtig, den Zugang Unbefugter zu Videokonferenzen und Arbeitsplattformen sowie den Zugriff auf Inhalte und Daten der Teilnehmenden zu verhindern (→ siehe auch Kapitel 1).

TIPPS

- **Wählen einer verschlüsselten Verbindung:** Schauen Sie, ob diese bei Ihren Browsern inklusive ist.
- **Zugang zum Meeting nur mit Passwort:** Das Passwort erhalten nur vorab angemeldete Teilnehmende.
- **Anmeldung über einen Gastzugang oder einen eigenen Zugang mit pseudonymisiertem Benutzernamen:** Bei einer Anmeldung mit einem bestehenden Konto (z. B. von Google oder Facebook) gibt man mehr Daten von sich preis.

TIPPS

- Denken Sie an eine angemessene Umgebung, wenn Sie per Video sichtbar sind (**Schutz der häuslichen Privatsphäre**): Virtuelles Hintergrundbild digital einfügen oder „Unschärfe"-Funktion nutzen.
- Das Mitschneiden und Weitergeben von Videokonferenzen (Gespräche und Texte) ist mit Desktop-Apps leicht möglich: Seien Sie in Ihren Verhaltensweisen und Äußerungen in Videokonferenzen – auch im Begleitchat – so vorsichtig und höflich wie im „analogen" Leben.

Elternhaus und Schule

Wenn Kinder und Jugendliche von zu Hause am Online-Unterricht teilnehmen (**Homeschooling**), sollten sie ihren eigenen, ruhigen Arbeitsbereich haben. Eltern sollten zumindest am Anfang bei der Anmeldung und bei (technischen) Problemen mit Meeting- und Lernplattformen zur Verfügung stehen.

TIPPS

Für Eltern

• Zeigen Sie Ihren Kindern, wie Sie die Mikrofon- und Kamerafunktion (de)aktivieren bzw. die Kamera mit einem Post-it abkleben können.

• Weisen Sie Ihre Kinder darauf hin: Die Kamera sollte nur im geschützten Klassenverband eingeschaltet sein.

TIPP

• Denken Sie an eine angemessene Umgebung, wenn Sie oder Ihre Kinder per Video sichtbar sind. Erklären Sie den Einsatz eines virtuellen Hintergrundbildes oder der „Unschärfe"-Funktion (**Schutz der häuslichen Privatsphäre**).

Schulen verwenden meist vom Kultusministerium zugelassene Plattformen und Anwendungen. Bei Fragen können sich Lehrkräfte an die Datenschutzbeauftragten und Systemadministratoren ihrer Schule wenden. Trotzdem sollten sie auch selber einige Dinge beachten. In der alltäglichen Praxis sollten Lehrkräfte die Schülerinnen und Schüler in die Nutzung einweisen und auf Fragen eingehen können.

TIPPS

Für Schulen/Lehrkräfte

• Holen Sie eine **schriftliche Einverständniserklärung** der Eltern für die Nutzung von Online-Tools ein (laut Art. 8 DSGVO bis 16 Jahre).

• Vermeiden Sie Störungen durch Dritte und verwenden Sie nur Angebote mit **verschlüsselten Datenleitungen** sowie persönlicher Anmeldung und Passwortschutz.

• Informieren Sie sich im Vorfeld, wie Sie in einem Tool störende Teilnehmer stummschalten oder aus dem Meeting ausschließen können.

• Behandeln Sie alle persönlichen Daten und Zugangsdaten vertraulich.

• Erläutern Sie neben dem notwendigen Handlungswissen auch mögliche Gefahren.

• Erstellen und veröffentlichen Sie klare Regeln, deren Verstoß auch Konsequenzen hat.

Seien Sie kreativ und entwickeln Sie Ihr eigenes Plakat für den Online-Unterricht:

Bei klicksafe kann man sich ein Regel-Plakat kostenlos downloaden:

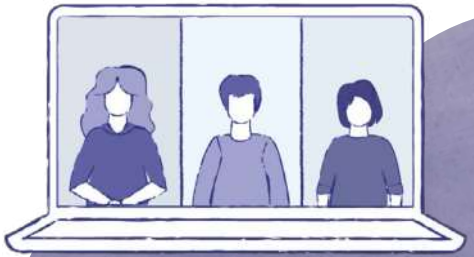
klicksafe – Regeln-Videochat

Arbeiten Sie – auch in Ihrem Kollegium – nach Möglichkeit in einem „gesicherten Internet" mit individuell einstellbaren Kommunikationsmöglichkeiten (z. B. mit den landeseigenen schulischen Lernplattformen **mebis** und **Moodle**). Die eingesetzten Plattformen müssen konform zur DSGVO und dem BayEUG sein. Daher ist der Einsatz von außereuropäischen Anbietern (z. B. von Microsoft, Google, Dropbox, Skype) meist nicht möglich. Das Bayerische Staatsministerium für Unterricht und Kultus empfiehlt für alle Schularten und Schulaufsichtsbehörden die zentrale bayernweite Videokonferenzsoftware Visavid.

Zur Verbreitung schulischer Informationen und Materialien können Schulen bzw. Lehrkräfte ebenfalls Lernplattformen wie mebis und Moodle nutzen. Aber beachten Sie die Urheberrechte, falls Sie Materialien Dritter bei den Plattformen einstellen wollen. Erklären Sie auch Ihren Schutzbefohlenen den Umgang mit dem Urheberrecht (→ siehe Seite 26 und 43).

Informationen zum Videokonferenz-Tool Visavid:

ByCS – Videokonferenzsystem



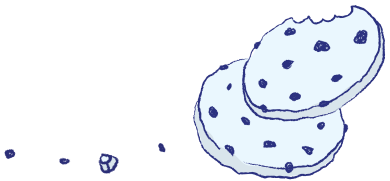
6. Online unterwegs

Je häufiger wir das Internet in unserem Alltag nutzen, desto mehr lässt sich über uns erfahren. Bei jedem Aufruf einer Internetseite geben wir Persönliches von uns preis. Besonders gern wird unser Surf-, Such- und Kaufverhalten erfasst. Hierbei lassen sich die Datenspuren zu einem umfassenden Profil von uns verdichten.

Doch wie behalte ich im Internet ein Mindestmaß an Kontrolle über meine Daten? Kann ich überhaupt verhindern, dass ich ausspioniert werde? Auch hierfür gibt es nicht das eine Erfolgskonzept. Schon mit der Auswahl von Browser und Suchmaschine, geänderten Einstellungen der genutzten Angebote, Apps und Dienste sowie der zusätzlichen Hilfe bestimmter Tools lässt sich ein Abgreifen unserer Daten durch Dritte zumindest begrenzen.

IP-Adresse

Bereits die IP-Adresse verrät einiges über uns. Sie wird bei jeder Seiten- oder Suchanfrage übermittelt, damit die Server im Netz wissen, wohin sie das angefragte Angebot schicken sollen. Sie gehört zu den personenbezogenen Daten und ermöglicht – vergleichbar einer Telefonnummer – die Zuordnung zu einem bestimmten Gerät (bzw. einer Person). Sie gibt auch Auskunft darüber, von wo aus man sich für das Angebot interessiert, welcher **Provider** (Dienste- oder Inhalte-Anbieter) genutzt wird und welche technischen Infrastrukturen (DSL, WLAN etc.), die für die Nutzung des Internets erforderlich sind, verwendet werden.



TIPPS

• Rufen Sie die Internetseite eines Lokalisierungstools auf (z. B. www.utrace.de), um sich anzeigen zu lassen, welcher Region und welchem Provider Ihre aktuelle IP-Adresse zugeordnet ist.

• Mit bestimmten Maßnahmen können Sie sich hinter einer anderen IP-Adresse „verstecken" und weitgehend anonym im Netz surfen, alle Varianten können aber die Internetgeschwindigkeit verringern:

- Umleitung des gesamten Datenverkehrs über einen Proxyserver (der allerdings ebenfalls Daten speichern kann).

- Einrichtung eines VPN (Virtuellen Privaten Netzwerks) für den gesamten Datenverkehr, hier werden Ihre Daten auch verschlüsselt, ggf. fallen Kosten beim Anbieter an.

- Nur für das Surfen im Internet: Browser mit integrierter VPN-Funktion (z. B. Opera) verwenden oder VPN-Erweiterung installieren.

- Der Einsatz des Tor-Browsers bzw. das Tor-Netzwerk haben ein negatives Image, da diese auch von Kriminellen genutzt werden. Der Tor-Browser bzw. das Tor-Netzwerk stellen aber grundsätzlich eine Möglichkeit dar, anonym im Netz zu agieren.

Auch der Browser übermittlet Informationen. Auslesbar ist hier nicht nur, ob man gerade mit Google Chrome, Firefox, Edge, Opera oder Safari etc. surft, sondern auch die Version, die gewählte Bildschirm- und Spracheinstellung sowie die zuvor besuchte Webseite.

TIPP

Mit regelmäßigen Updates erhöhen Sie nicht nur die Geschwindigkeit Ihres Browsers, sondern schließen auch Sicherheitslücken. Sie können sich bei Zendas die aktuell von Ihrem Browser übermittelten Daten anzeigen lassen:

Zendas – Browserdaten

Cookies

Auf vielen Webseiten kommen standardmäßig **Cookies** und **Zählpixel** (unsichtbare Grafiken) zum Einsatz. Ihnen lässt sich entnehmen, was sich die Nutzenden auf welcher Webseite wie lange anschauen, was sie wie oft anklicken und ob sie erstmalig die Seite nutzen. Bei Inhalten eingesetzt, die über viele Webseiten gestreut werden (z. B. Werbung), machen Cookies und Zählpixel Ihren Weg durch das Internet für andere nachvollziehbar.

Rasant verbreitet haben sich auch **Super-Cookies**. Sie nisten sich an Speicherorten ein, die nicht vom Cookie-Manager des Browsers verwaltet werden, und sind daher kaum zu löschen. Diese Cookies erfassen nahezu unbegrenzt die Aktivitäten der Nutzerinnen und Nutzer, um von bestimmten Anbietern ausgelesen und ausgewertet zu werden. Einzelne Browser versuchen, dies technisch zu unterbinden (z. B. Firefox).

Beim Aufrufen einer Webseite werden Sie häufig gefragt, ob und wenn ja, welche Cookies Sie akzeptieren.

TIPPS

- Lehnen Sie Cookies ab oder stimmen Sie nur der Erhebung von funktionalen Cookies zu.
- Achten Sie darauf, dass teilweise durch eine manipulative Aufbereitung des Cookie-Fensters (großer, farbig hervorgehobener Button versus kleinem, unauffälligem oder verstecktem Button) der User oder die Userin zum Akzeptieren aller Cookies verleitet werden soll.
- Mit der Anpassung der Einstellungen Ihres Browsers können Sie die Speicherung einfacher Text-**Cookies** regulieren und z. B. automatisch löschen lassen.

Weitere Informationen unter:

Verbraucherzentrale Bayern – Manipulative Cookie-Banner erkennen

Surfen im **Privat- oder Inkognito-Modus** verhindert das Speichern von Cookies, Chronik, Suchanfragen und temporären Dateien. Beachten Sie: Dies hat keine anonymisierende Wirkung nach außen. Der Modus verhindert lediglich, dass bestimmte Daten auf Ihrem Gerät gespeichert werden. Andere Personen, die Ihr Gerät nutzen, können so Ihr Surfverhalten nicht nachvollziehen.

TIPPS

- Sie können ein Inkognitofenster entweder über die drei Punkte oben am Rand oder eine Tastenkombination öffnen: Drücken Sie Strg + Shift + n (Windows) oder Cmd + Shift + n (Apple). Je nach Browser unterscheidet sich die Bezeichnung: z. B: „InPrivat“ (Microsoft Edge), „Incognito“ (DuckDuckGo; Google Chrome), Privates Fenster (Firefox).
- Um das unerwünschte Nachverfolgen durch „Tracker“ beim Surfen im Internet zu verhindern, können grafischen Zählpixel mit kostenlosen Browser-Erweiterungen (Add-ons) wie bspw. „Ghostery“ angezeigt und deaktiviert werden.

Sie können ein Inkognitofenster über eine Tastenkombination Strg + Shift + n (Windows) bzw. Cmd + Shift + n (Apple) öffnen.

Suchmaschinen

Umfangreiche Datenspuren hinterlassen wir auch bei der Nutzung von **Suchmaschinen**. Je mehr Dienste ein Anbieter unter seinem Dach hat, desto mehr kann er über uns herausfinden. Der Global Player Google LLC verfügt über weitere populäre Dienste, z. B. YouTube, Gmail, Google Drive, Google Maps. Durch die Verknüpfung der hier erfassten Daten mit Suchanfragen weiß Google sehr viel über uns – egal von welchem Endgerät (PC, Smartphone, Tablet etc.) wir die Dienste nutzen: Google kennt unser Kommunikationsverhalten, unsere Medienvorlieben und persönlichen Interessen.

TIPPS

- Achten Sie auch bei der Websuche auf Ihre Privatsphäre. Sie können verschiedene datensparsamere Suchmaschinen nutzen, z. B. **DuckDuckGo** und **Qwant**. Mit der Nutzung von **Startpage** erhalten Sie anonymisierte Google-Ergebnisse.
- Wenn Sie bei Google-Diensten angemeldet sind und einen Eindruck vom Netzwerk Ihrer Daten bekommen möchten, schauen Sie sich das Dashboard an (Anmeldung unter myaccount.google.com/dashboard).

Mithilfe von **Cloud-Diensten** überall, jederzeit und unabhängig vom Endgerät auf seine Daten zugreifen zu können, ist sehr praktisch. Doch wie sicher sind **Google Drive, Dropbox, iCloud** & Co.? Wie kann ich verhindern, dass der Anbieter des Online-Speichers meine hinterlegten Daten einsehen kann oder die privaten Dokumente, Bilder, Videos etc. nach einem Hacker-Angriff im Netz landen?

Wer den Sicherheitsstandards der Cloud-Anbieter nicht vollends vertraut, verschlüsselt seine Daten selbst. Schnell erstellt sind passwortgeschützte Dateien-Archive mit freier Software wie 7-Zip (Windows/Linux) und iZip (OS X).

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz hat dazu ein PDF erstellt:

RLP – Verschlüsselung

Neben Apps sind Browser auf allen Geräten das zentrale Hilfsmittel, um Internetseiten aufzurufen. Auch auf den Geräten, die Kinder und jüngere Jugendliche nutzen, sollte daher auf aktuelle und datensparsame Anwendungen geachtet werden. Die gängigen Browser verfügen in der Regel nicht über eine besondere „Kindersicherung".
Stellen Sie im Browser eine Startseite ein, die für Ihre Kinder geeignet ist. Wählen Sie beispielsweise die Kindersuchmaschinen Blinde Kuh oder fragFinn aus.

Sie können zudem auf den Startseiten gängiger Suchmaschinen in den „Sucheinstellungen" Suchfilter (z. B. „Familienfilter") gegen das Anzeigen „anstößiger Suchergebnisse" aktivieren.

Für Schulen gilt, dass die Nutzung eines Online-Speichers als „Schul-Cloud" nur im Rahmen einer zugelassenen Lernplattform infrage kommt (→ siehe Seite 36/37).

Blinde Kuh –
Suchmaschine für Kinder

fragFINN –
Suchmaschine für Kinder

Weitere Informationen und Tipps finden Sie in unseren anderen Broschüren:

Tipps zum sicheren Passwort
Diese Publikation zum Selbstdatenschutz gibt Antworten auf die Frage, wie sich sichere Passwörter einfach gestalten und leicht merken lassen, gleich ob es um Online-Banking, den Einkauf im Netz, das Mailen oder die Smartphone-Nutzung geht.

Urheberrecht
In dieser Broschüre werden Mediennutzerinnen und -nutzern praxisorientierte und alltagstaugliche Tipps im Umgang mit dem Urheberrecht aufgezeigt. Schwerpunktthemen sind „Legale Nutzung", „Texte, Fotos und Grafiken", „Musik, Hörbücher, Filme und Videos", „Soziale Netzwerke und Messenger-Apps" sowie „Folgen von Verstößen".

Recht am eigenen Bild
Aufnahmen erstellen, Fotos hochladen und Videos teilen – was ist bei der täglichen Nutzung von Kommunikations-Apps und Social-Media-Angeboten zu beachten? Diese Broschüre bietet Mediennutzerinnen und -nutzern, im Speziellen Eltern, Erziehenden und Lehrkräften, praxisorientierte und alltagstaugliche Tipps im Umgang mit dem Recht am eigenen Bild. Auch in Leichter Sprache verfügbar.

Alle Broschüren finden Sie hier:

BLM –
Materialien

Weitere nützliche Internetseiten:

- www.blm.de
- www.stiftung-medienpaedagogik-bayern.de
- www.klicksafe.de
- www.mobilsicher.de
- www.handysektor.de

Glossar – das Wichtigste in Kürze

Add-on
Kurzform vom Englischen „to add" (dt: etwas hinzufügen). Ein Add-on fügt neue Funktionen zu einer bestehenden Hard- oder Software hinzu. Beispielsweise kann ein Add-on eine Browser-Erweiterung sein.

Bluetooth
Funkstandard für Datenübertragung zwischen Geräten im Nahbereich (bis 10 Meter). Die austauschenden Geräte müssen vom jeweiligen Besitzer „gekoppelt" werden.

Browser
Programme, die notwendig sind, damit Internetseiten mit den verschiedenen Endgeräten (PC, Laptop, Smartphone, Tablet etc.) aufgerufen und angezeigt werden können. Die aktuell am häufigsten genutzten Browser sind mit zusammen fast 90 Prozent Marktanteil: Firefox, Google Chrome, Safari und Edge.

Cloud(-Dienste)
Externer Speicherort für Dateien (Dokumente, Bilder, Videos etc.) und Dateienarchive. Diese werden auf einem Rechner abgelegt, auf den mittels des Internets (oder mittels eines anderen Computernetzwerks) zugegriffen werden kann. So kann man unabhängig vom aktuell genutzten Endgerät auf alle seine in der Cloud abgelegten Daten zugreifen.

Cookies
Kleine Dateien, die beim Besuch einer Webseite auf dem Rechner gespeichert werden, damit zum Beispiel persönliche Einstellungen nicht verloren gehen. Im Gegensatz zu Session-Cookies, die mit dem Schließen des Browsers automatisch gelöscht werden, gibt es auch Cookies, die die Informationen unter Ihrer ID dauerhaft speichern: Unabhängig vom Browser können sich bei Nutzung von Multimediaeinbindungen (z. B. Videos) auf Webseiten auch Super-Cookies in zentralen Ordnern des Computers einnisten und von dort aus die Aktivitäten der Nutzenden ausspähen. Diese Cookies haben nicht nur eine längere Verweildauer, sondern können auch größere Datenmengen erfassen.

Datenschutz-Grundverordnung (DSGVO)
Die Europäische Datenschutz-Grundverordnung vereinheitlicht das europäische Datenschutzrecht und damit auch die Wettbewerbsbedingungen. Ein besonderer Schwerpunkt liegt auf dem Schutz personenbezogener Daten durch genaue Vorgaben für ihre Verarbeitung (z. B. verpflichtende Einwilligung, Recht auf Auskunft und Löschung).

Firewall
Eine Firewall (dt. Schutzwall) ist ein Sicherungssystem zwischen Internet und eigenem Netzwerk bzw. Geräten: Unerwünschte Zugriffe werden blockiert und nur erwünschte Verbindungen zugelassen. Die Blockaderegeln können vom Nutzenden vorgegeben werden.

GPS
GPS steht für Global Positioning System und beschreibt die weltweit funktionierende Bestimmung der eigenen Position mit Hilfe von Satelliten.

Influencerinnen und Influencer
Diese sind vorwiegend in Social-Media-Kanälen wie YouTube, Instagram, TikTok und Facebook präsent. Oft haben sie besondere Kompetenzen bzw. erlangen mit ihren Videos sogar Expertenstatus für bestimmte Inhalte oder ihre Tätigkeit (z. B. Tipps für Mode und Schminken, Sport und Fitness). Sie wirken authentisch und können als Idole mit Vorbildfunktion oder „Meinungsführer"

durch Produktplatzierungen oder ausführliche Produktpräsentationen insbesondere Kinder und Jugendliche beeinflussen.

IP-Adresse
Das Internetprotokoll (IP) legt fest, welche Daten zwischen Computern ausgetauscht werden. Für den Datenaustausch im Internet werden den verschiedenen Computern und Servern im Netz IP-Adressen zugewiesen, anhand derer der jeweilige Computer bzw. Server eindeutig identifizierbar ist. Die Adressen stellen sicher, dass die angefragten bzw. ausgegebenen Daten an das richtige Gerät geschickt werden.

NFC (Near Field Communication)
NFC bedeutet Nahfeldkommunikation und ist eine Funktechnik zur Datenübertragung auf kürzester Distanz (ca. 10 cm). Sie wird insbesondere bei Bezahlterminals eingesetzt.

Passwort-Manager
Diese Programme verwalten verschlüsselt die Benutzernamen und Passwörter von unterschiedlichen Accounts. Für den Gebrauch notwendig ist dann nur noch ein – unbedingt sehr gutes – Masterpasswort und ggf. der Einsatz Zwei-Faktor-Authentisierung (mittels Passwort und Bestätigung der Identität z. B. durch einen Fingerabdruck-Scan oder ein Einmalkennwort in einer anderen App auf einem anderen Gerät). Aus Sicherheitsgründen sind eigenständige Passwort-Manager gegenüber den browserintegrierten zu bevorzugen.

Phishing
Dies ist der englische Begriff für „password fishing" – das betrügerische „Abfischen" von Daten bzw. Passwörtern mithilfe von gefälschten E-Mails oder Internetseiten.

Router
Vermittlungsgerät für den Internet-Anschluss, der die Verbindung zu den eigenen Endgeräten herstellt und steuert.

Tracking
Tracking bezieht sich auf die Verfolgung und Aufzeichnung von Informationen über ein digitales Gerät. Es wird verwendet, um das Verhalten von Benutzern zu verstehen und zu analysieren, um personalisierte Angebote und Inhalte bereitzustellen oder um die Wirksamkeit von Werbekampagnen zu messen.

Verschlüsselung
Übersetzung von sinnvollen, lesbaren Daten in scheinbar sinnlose, unlesbare Daten, die nur „entschlüsseln" kann, wer über den passenden Schlüssel verfügt. Bei der Verschlüsselung im Internet gibt es zwei Varianten: Die Transportwegverschlüsselung oder die Leitungsverschlüsselung (auch: Punkt zu Punkt-Verschlüsselung) zwischen den Geräten. An den sendenden und empfangenden Geräten selbst besteht keine Sicherheit. Sicherer ist die **Ende-zu-Ende-Verschlüsselung**: Der Sender verschlüsselt und der Empfänger entschlüsselt jeweils die Daten in seinem E-Mail-Programm.

WLAN
WLAN, engl. Wireless Local Area Network, ist ein kabelloses, lokales Funknetzwerk für den Internetzugang.

WPA2-/WPA3-Standard
Bezeichnet eine besonders sichere Verschlüsselungstechnik für WLAN mit einem langen Passwort.

Ein ausführliches Glossar finden Sie unter:

BLM – Glossar
„Sicher online unterwegs"

Stichwortverzeichnis

Add-on *12, 40, 44*
Amazon (Prime Video) *29 ff.*
Apple (TV) *13, 30, 40*
Apps *5, 7 ff., 11, 13, 15 ff., 20 f., 26 ff., 35, 38, 42 f., 45*

Berechtigungen *11, 13, 21*
BigBlueButton *21, 34*
Big Data *6*
Bluetooth *9, 44*
Browser *7 f., 11 f. , 26, 28 f., 35, 38 ff., 42, 44*

Cloud(-Dienste) *15, 41 f., 44*
Cookies *7, 26, 29, 39 f.*

Datenschutz-Grundverordnung (DSGVO) *4 f., 20, 36 f., 44*
Disney+ *30*

E-Mail *5 f., 8, 12, 15 f., 18 f., 21, 23, 43, 45*

Facebook *17, 22, 25, 27, 35, 44*
Firewall *12*

GPS *5, 9, 11*

Homeoffice *34*
Homeschooling *34, 36*
https *11 f.*

Inkognito-Modus *40*
Influencer/-innen *22, 44*
Instagram *22, 24 f., 44*
IP-Adresse *23, 38 f., 44*

Jitsi *16, 21, 34, 37*

Kamera *8, 11, 34, 36*
kostenpflichtige Angebote *16, 28, 30*
Konto (Kunden-) *6, 18, 26 f., 30, 35*
Kreditkarte *5*

Lokalisierungstools *39*

mebis *21, 27, 37*
Mediathek *29*
Messenger *16 f., 20 ff., 43*
Mikrofon *11, 34, 36*
Moodle *21, 37*

Netflix *30 f.*
NFC (Near Field Communication) *9, 45*

Passwort(-Manager) *8 ff., 14, 18, 28, 32, 35 f., 41, 43, 45*
Phishing *12, 19, 45*
PIN *8, 32*
Provider *38 f.*

Recht am eigenen Bild *25, 43*
Router *9 f., 14, 44*

Signal (Messenger) *16 f., 20 f.*
SIM-Karte *8*
Skype *16, 21, 34, 37*
Snapchat *17, 20 f., 26*
Social Media *4 ff., 22 f., 25, 27 f., 43 f.*
Spam *6, 18 f.*

Spotify *30 f.*
Streaming *28 ff.*
Suchmaschinen *38, 41 f.*

Threema *16 f., 20 f.*
TikTok *22, 25 ff., 44*

Updates *12, 39*

Verschlüsselung *9, 11 f., 17 f., 41, 45*
Videokonferenz *34 f., 37*
Visavid *21, 34, 37*
VPN *39*

WhatsApp *16 ff., 20 f., 25, 27*
WLAN *9 f., 14 f., 38, 45*
WPA2-/WPA3-Standard *9 f., 45*

YouTube *22, 25 ff., 29, 33, 41, 44*

Zählpixel *39 f.*
Zugangsdaten *36*
Zugangssperren *7 f.*

Impressum

Herausgeberin
Bayerische Landeszentrale für neue Medien (BLM)

Verantwortlich
Kerstin Prange
(Bereichsleiterin Inhalte & Medienkompetenz, BLM)

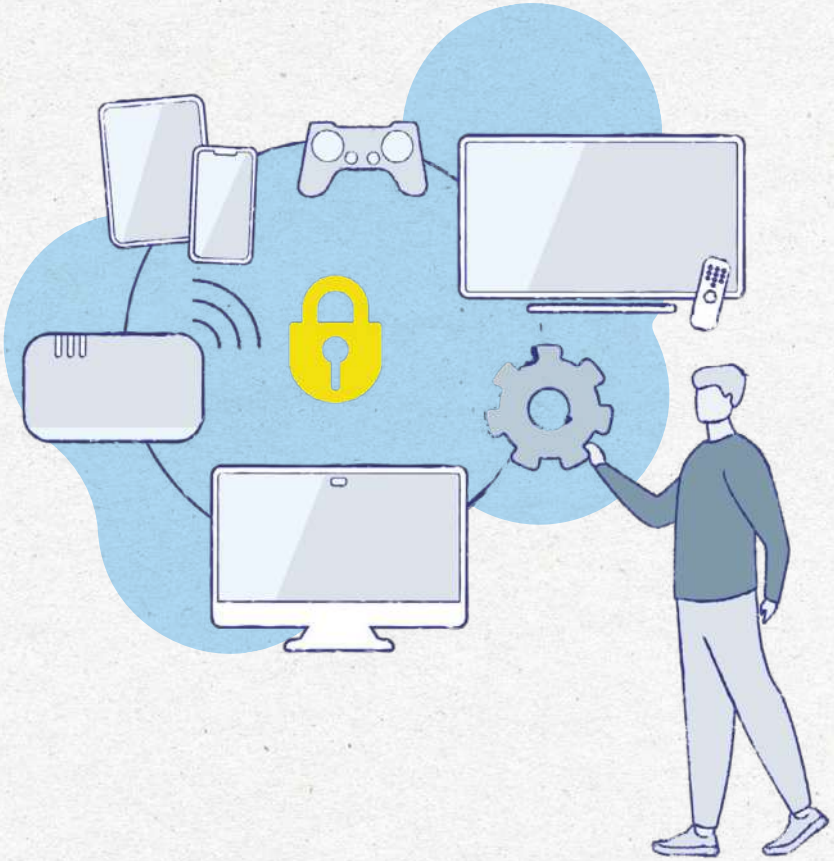
Redaktion (BLM)
Dr. Kristina Hopf
Elke Hesse

Autoren
Dr. Olaf Selg (AKJM, www.akjm.de)
Stefan Gehrke (bfnd, www.bfnd.de)

Layout/Illustration
Theresa Fischer

Druck
Senser Druck

München, 2023



Bayerische Landeszentrale für neue Medien | Rechtsfähige Anstalt des öffentlichen Rechts
Heinrich-Lübke-Straße 27 | 81737 München | Tel. +49 (0)89 63808-0 | info@blm.de | www.blm.de