BLM
Bayerische
Landeszentrale für
neue Medien

Sicher im Internet unterwegs

Tipps und Tricks zum Schutz der persönlichen Daten

Inhalts·verzeichnis

Vorwort

Jeden Tag gehen Menschen ins Internet.
Zum Beispiel mit ihrem Smartphone
oder mit ihrem Tablet.
Dabei denken viele **nicht** daran:
Im Internet hinterlässt man immer
eine Spur an Daten.
Egal ob wir in einen Chat schreiben
oder ein Foto posten.

Das heißt:
Mit jeder Aktion im Internet
geben wir Daten von uns weiter.
Unternehmen sammeln diese Daten.
Dann verkaufen die Unternehmen die Daten.
Oder sie benutzen die Daten
für persönliche Werbung.

Damit das **nicht** passiert, ist es wichtig:
Geben Sie nur wenig Daten im Internet an.
Aber wie kann man das machen?
Worauf muss man achten?
In diesem Heft steht mehr dazu.

Außerdem geben wir Ihnen Informationen und Tipps.
Damit können Sie Ihre Daten gut schützen.
Aber wir schreiben auch:
So können Sie das Internet gut nutzen.

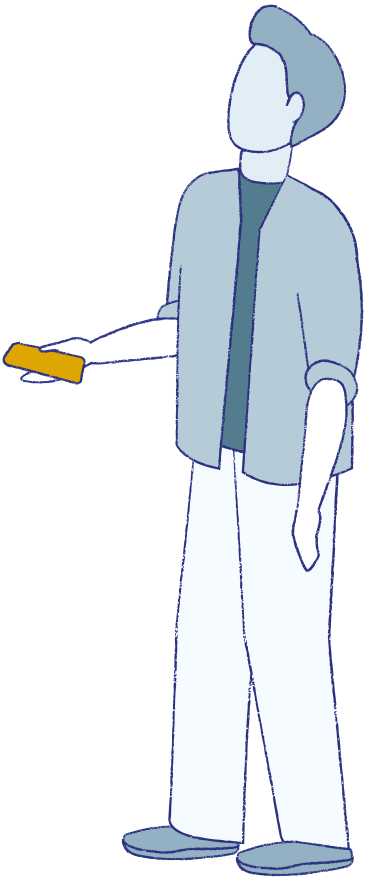
Nun wünschen wir Ihnen viel Spaß beim Lesen!

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


„Ich gebe möglichst wenig Daten von mir weiter.“

1. Persönliche Daten

Schutz von persönlichen Daten
Was meinen wir damit?



Beispiele für persönliche Daten:

- Name
- Alter, Geburts·datum
- Anschrift, Telefon·nummer
- E-Mail-Adresse
- Konto·nummer
- Fotos, Videos

Zeigen Sie fremden Menschen Fotos von sich selbst?
Oder geben Sie fremden Menschen Ihre Konto·nummer?
Wahrscheinlich **nicht**.
Aber genau das machen viele Menschen im Internet!
Dabei vergessen die Menschen:
Im Internet können sehr viele Menschen
meine Informationen und Daten lesen.
Oft auch unbekannte Menschen.

Die Weiter·gabe von persönlichen Daten im Internet
hat Vorteile.
Eine Internet·seite funktioniert dann besser.
Oder man kann dadurch zum Beispiel
Sachen bestellen.

Aber durch die Weiter·gabe von persönlichen Daten
gibt es auch Probleme.
Die merkt man nur **nicht** direkt.
Vielleicht bekommt man zum Beispiel
plötzlich ganz viel Werbung.
Zum Schutz unserer Daten gibt es Gesetze.
Aber jede Person kann auch selbst
etwas zum Schutz ihrer Daten tun.
In diesem Heft geben wir Ihnen dazu Informationen
und Tipps.

Wie gibt man persönliche Daten im Internet weiter?

Manche Daten gibt man mit Absicht weiter.
Beispiel:
Sie bestellen etwas im Internet.
Dazu müssen Sie auf der Internet·seite
persönliche Daten angeben.
Zum Beispiel Ihren Namen und Ihre Adresse.

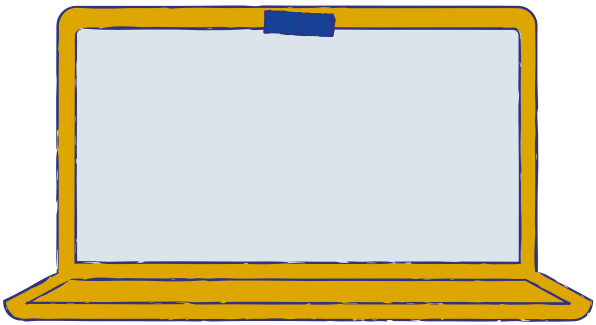
Aber gleichzeitig geben Sie andere Daten **nicht**
mit Absicht weiter.
Das heißt: Sie merken das gar **nicht**!
Zum Beispiel hat jeder Computer eine Nummer.
Die heißt IP-Adresse.
Das spricht man: Ei-Pi-Adresse.
Diese IP-Adresse wird automatisch verschickt.

Man kann sagen:
Wir hinter·lassen so etwas wie eine Spur im Internet.

Das kann Probleme machen
oder gefährlich sein.
Denn manche Unternehmen sammeln diese Daten.
Und verkaufen oder benutzen sie.

TIPPS

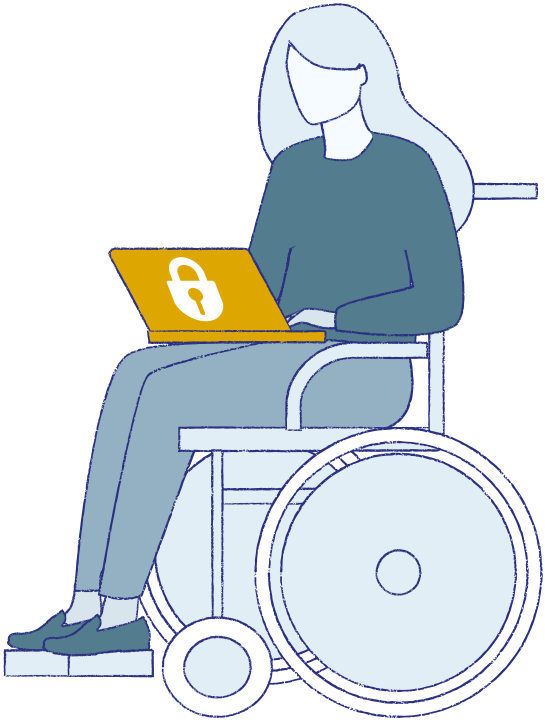
- Geben Sie immer möglichst **wenig** Daten an!
- Kleben Sie bei Bedarf Ihre Kamera mit einem Post-it oder Sticker ab.

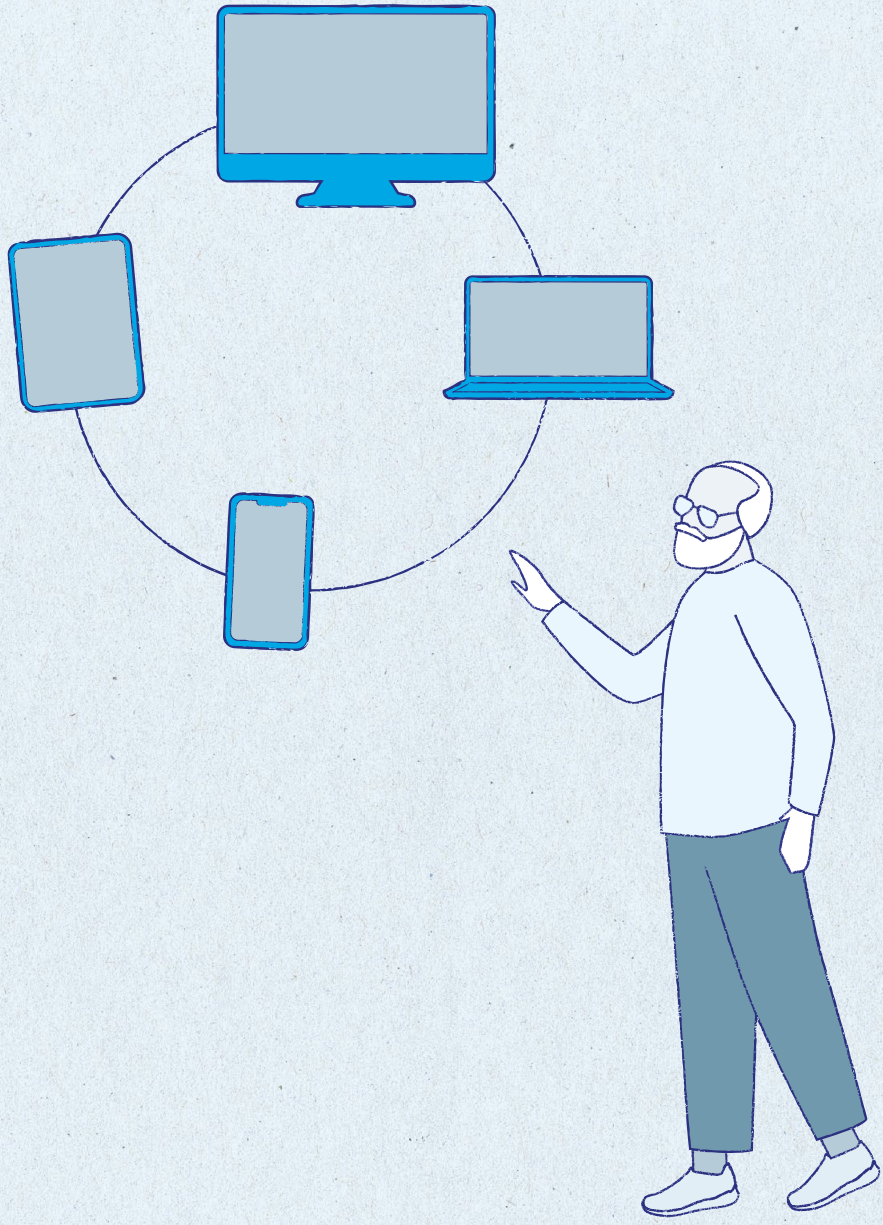


Oft fragen Internet·seiten zu viele Daten ab.
Das können Sie manch·mal erkennen:
Es gibt Pflicht·felder.
Da müssen Sie etwas eintragen.
Diese Felder haben meist einen Stern: *

Die anderen Felder haben **keinen** Stern.
Das sind freiwillige Angaben.
Da müssen Sie **nichts** eintragen.

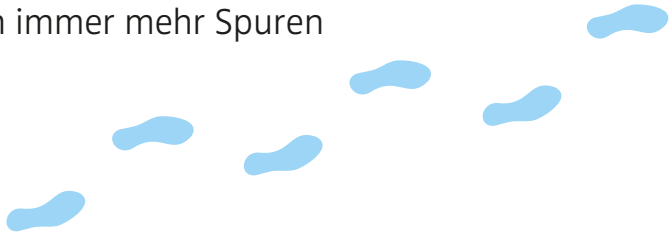
Deshalb denken Sie am besten an den Spruch:
„Meine Daten gehören mir!“





2. Technik und Geräte

Wir nutzen das Smartphone oder das Tablet
oft und überall.
Wir machen damit viele unterschiedliche Dinge.
Immer wieder kaufen wir neue Geräte.
Mit jedem neuen Gerät kann man mehr Dinge tun.
Aber:
Wir hinter·lassen auch immer mehr Spuren
im Internet.
Ohne es zu merken.



Denn oft sind die Einstellungen
der neuen Geräte so:
Das Gerät gibt zu viele Daten weiter.
Aber Sie können die Einstellungen ändern.
Dann gibt das Gerät weniger Daten weiter.

TIPP

Sie haben ein neues Gerät?
Zum Beispiel ein neues Smartphone?
Oder Sie benutzen eine neue App?
Dann prüfen Sie die Einstellungen zum Daten·schutz.

Zugangs·sperren

Andere Menschen können Ihr Gerät benutzen.
Wenn Sie zum Beispiel gerade **nicht**
am Computer sind.
Oder wenn jemand Ihr Smartphone gestohlen hat.
Diese Menschen können Ihre Daten bekommen.
Richten Sie deshalb eine Zugangs·sperre ein.
Damit die Menschen Ihre Daten **nicht** bekommen.

Beispiele für Zugangs·sperren:

Muster 

PIN-Nummer 

Pass·wort 

Finger·abdruck 

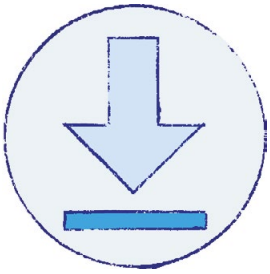
Gesichts-Scan:
Das ist das Erkennen
vom eigenen Gesicht
durch die Kamera.

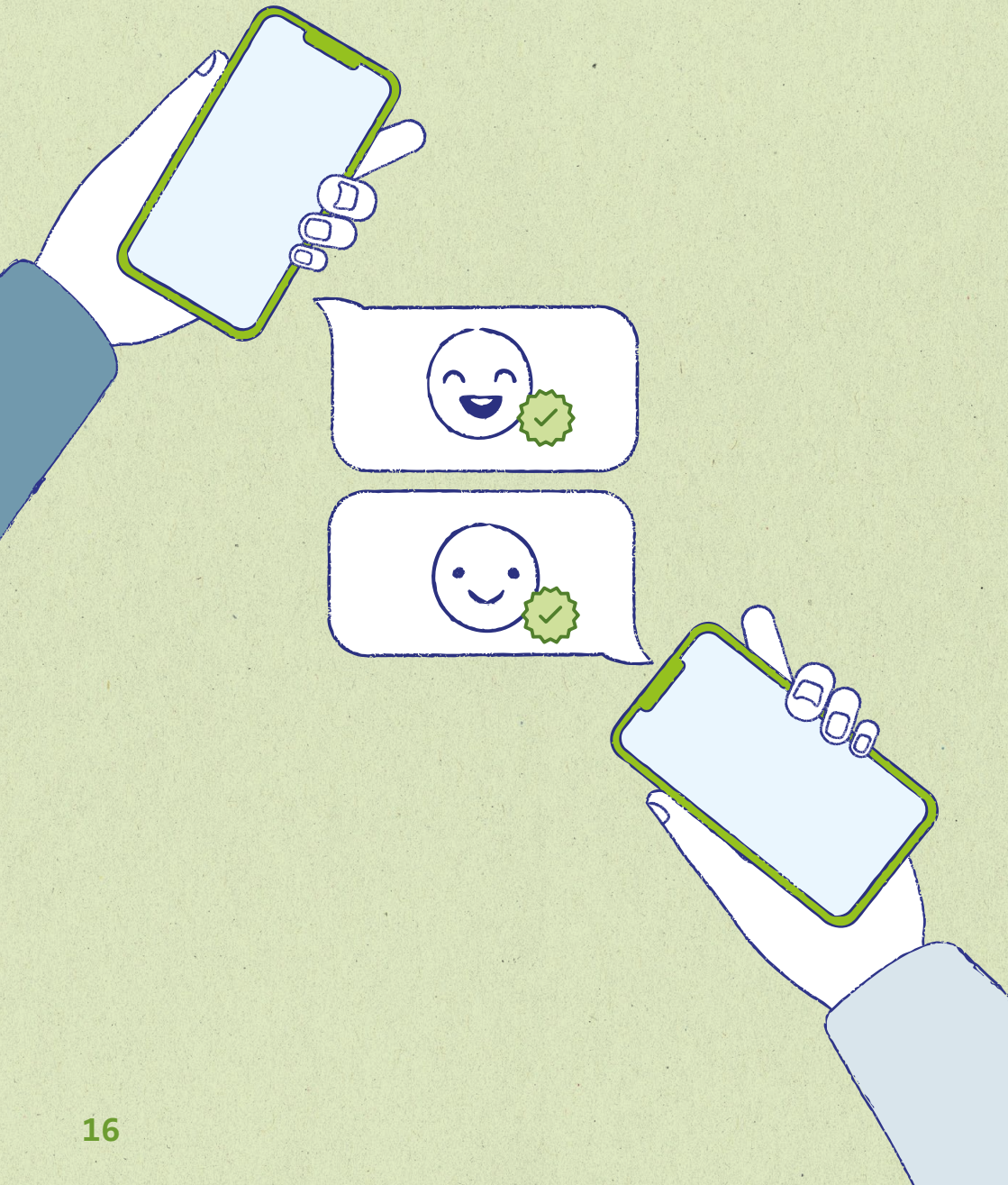

Installation von Apps

Manche Apps sind kosten·los.
Das heißt:
Die Apps kosten **kein** Geld.
Aber:
Die Anbieter dieser Apps sammeln Ihre Daten.
Dann verkaufen die Anbieter Ihre Daten.
Oder sie benutzen die Daten
für persönliche Werbung.
So verdienen die Anbieter Geld mit Ihren Daten.
Deshalb ist die App eigentlich **nicht** kosten·los:
Sie bezahlen die App mit Ihren Daten.

TIPPS

- Laden Sie möglichst wenig Apps herunter.
- Laden Sie Apps nur aus bekannten App-Stores.
  Zum Beispiel aus dem von Google oder Apple.





3. Unterhaltungen im Internet

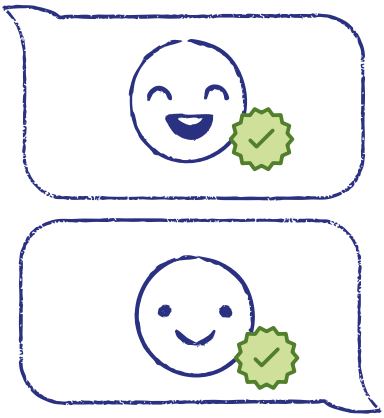
Früher hatte fast jeder Mensch ein Telefon.
Damit hat man telefoniert.

Heute hat fast jeder Mensch ein Smartphone.
Damit kann man viele verschiedene Dinge tun.
Man kann damit auch telefonieren.
Entweder so wie mit einem Telefon.
Dann hat man das Smartphone am Ohr
und spricht mit einer anderen Person.
Oder man telefoniert mit einer App.
Zum Beispiel mit Skype oder Jitsi.
Dann kann man die andere Person sehen
und mit ihr sprechen.

Man kann aber auch auf andere Art
Gespräche führen.
Über Messenger-Dienste.
Das spricht man so aus: Messendscher-Dienste.
Zum Beispiel WhatsApp, Threema oder Signal.
Threema ist ein englisches Wort.
Am Anfang steht das englische Wort
für die Zahl 3: three.
Man spricht das ganze Wort so aus: Three-ma.

Messenger-Dienste

Auf Deutsch heißt das: Nachrichten-Dienste.
Gemeint sind Apps mit denen man Nachrichten verschicken kann.



Zum Beispiel WhatsApp, Threema oder Signal.

Verschicken kann man

- Texte
- Sprach·nachrichten
- Fotos
- und Videos

Bei den Nachrichten-Diensten muss man persönliche Daten angeben.

Das sind Probleme bei Nachrichten-Diensten:

- Manche Nachrichten-Dienste nutzen viele persönliche Daten.
- Manchmal ist der Schutz der Nachrichten schlecht. Dann können auch Fremde die Nachrichten lesen.

TIPP

- Signal oder Threema zum Beispiel schützen Daten gut.
- Überlegen Sie:
  Soll ich zusammen mit meinen Freundinnen und Freunden vielleicht Signal oder Threema nutzen?

Fotos und Videos verschicken

Vielleicht verschicken Sie Fotos oder Videos.

Überlegen Sie:

Welches Foto oder Video verschicke ich?

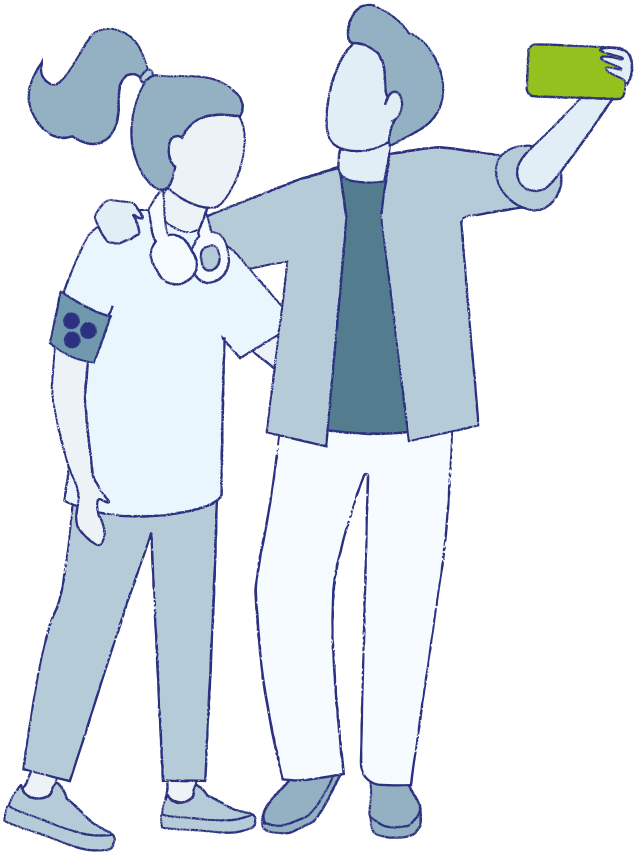
Wer erhält Ihr Foto oder Video?

Die Person kann Ihr Foto oder Video speichern oder weiter·leiten.

Das heißt:

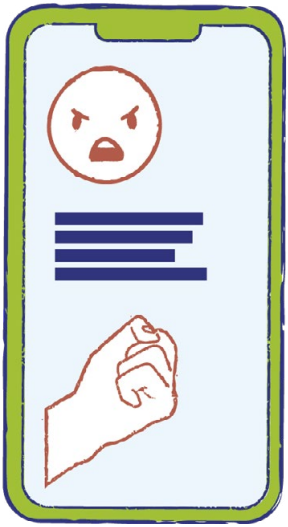
Viele Personen können Ihr Foto oder Video bekommen.

Sie haben **keine** Kontrolle darüber!



Vielleicht meldet sich bei Ihnen eine Person.
Aber Sie möchten **keinen** Kontakt zu der Person.
Dann können Sie die Person blockieren.

Vielleicht machen Sie schlechte Erfahrungen.
Beispiel:
Jemand beleidigt Sie oder jemand belästigt Sie.
Dann machen Sie ein Bildschirm·foto
von dem Text oder Bild.
Gehen Sie dann zur Polizei
und stellen Sie eine Straf·anzeige.



Profil·bild

Bei Messenger-Diensten können Sie
ein Profil·bild einfügen.
Vielleicht ein Foto von sich selbst?
Am besten überlegen Sie vorher:
Das soll von mir zu sehen sein.
Oder Sie nehmen **kein** Foto von sich selbst.
Sondern ein anderes Bild.
Zum Beispiel von einer Blume.

Sie müssen bei Messenger-Diensten
auch persönliche Informationen angeben.
Überlegen Sie:

- Welche Informationen gebe ich an?
- Wer darf diese Informationen lesen?

Das können Sie selbst einstellen.

E-Mails

Eine E-Mail schicken ist so ähnlich
wie einen Brief schicken.
Aber: Einen Brief kleben Sie zu.

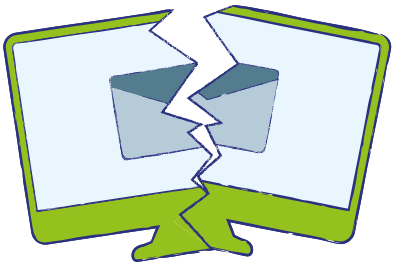
Dann kommt er in den Brief·kasten.
Und wird verschickt.
Keiner kann ihn auf dem Weg lesen.

Eine E-Mail schreiben Sie.
Dann machen Sie einen Klick.
Und verschicken die E-Mail.
Manchmal können andere diese E-Mail mit·lesen.

TIPP

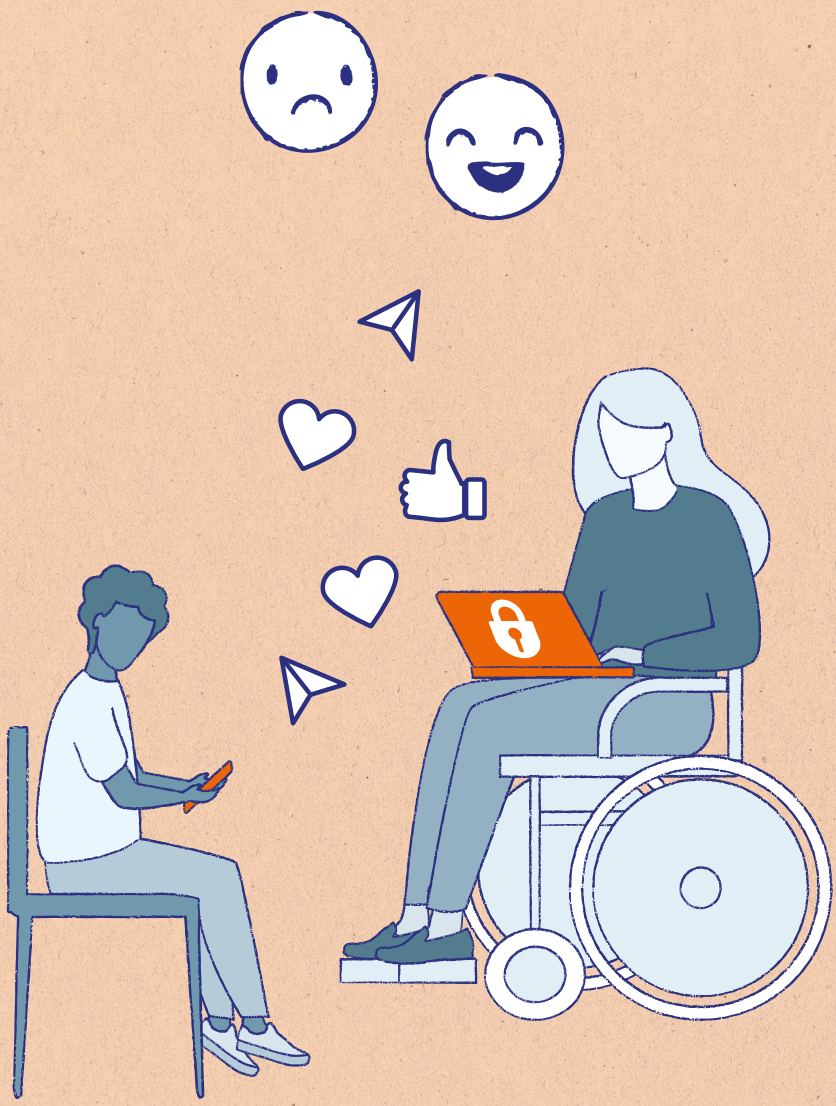
Verschicken Sie nur verschlüsselte E-Mails.
Dann kann niemand Ihre E-Mails lesen.
Wie geht das?
Fragen Sie dazu eine Fach·person für Computer.

Eine E-Mail bekommen ist so ähnlich
wie einen Brief bekommen.
Aber man muss beim Öffnen von einer
E-Mail vorsichtiger sein.
Denn manchmal bekommt man eine E-Mail
mit einem Computer·virus.
So ein Virus macht den Computer kaputt.



TIPP

Sie bekommen eine E-Mail.
Aber Sie kennen den Absender **nicht**.
Vielleicht hat die E-Mail einen Datei·anhang
oder einen Link.
Dann öffnen Sie den Datei·anhang **nicht**.
Klicken Sie den Link **nicht** an.
Denn vielleicht ist das ein Virus.



4. Social-Media-Angebote

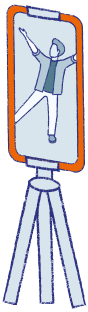
Das spricht man so aus:
Soschijel Midia Angebote.

Die meisten Menschen benutzen
diese Social-Media-Angebote:

- Instagram
- YouTube
- TikTok oder
- Facebook

In den Social-Media-Angeboten kann man sich
selbst darstellen.
Zum Beispiel mit

- Texten
- Fotos oder
- Videos



Man kann sich dort auch mit anderen Menschen aus·tauschen.
Die Angebote sind kosten·los.
Wobei das **nicht** ganz stimmt:
Wir bezahlen mit unseren persönlichen Daten.
Die Daten werden verkauft
und von anderen Unternehmen benutzt.
Wir bekommen dann viel Werbung gezeigt.

TIPPS

- Schreiben Sie nur wenige persönliche Daten in das Social-Media-Angebot.
- Stellen Sie Ihr Profil auf privat:
  Dann können nur Ihre Kontakte Ihr Profil sehen.
- Sie möchten ein Foto von einer anderen Person zeigen?
  Dann müssen Sie die andere Person vorher fragen.

TIPPS

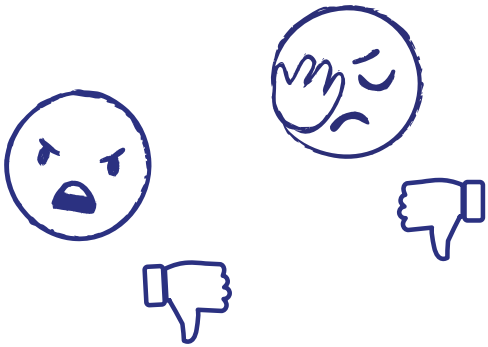
- Überlegen Sie bei Fotos von sich selbst:
  Was möchte ich von mir zeigen?
- Überlegen Sie bei Text und Kommentaren:
  Was schreibe ich?

Denn andere können Ihren Text lesen
und Ihre Fotos sehen.
Andere können Ihre Fotos und Texte
auch speichern.
Und an andere Kontakte weiterleiten.

Problematische Inhalte

Manchmal gibt es in Social-Media-Angeboten

- Beleidigungen
- Hass-Rede
- falsche Nachrichten oder
- sexuelle Belästigung



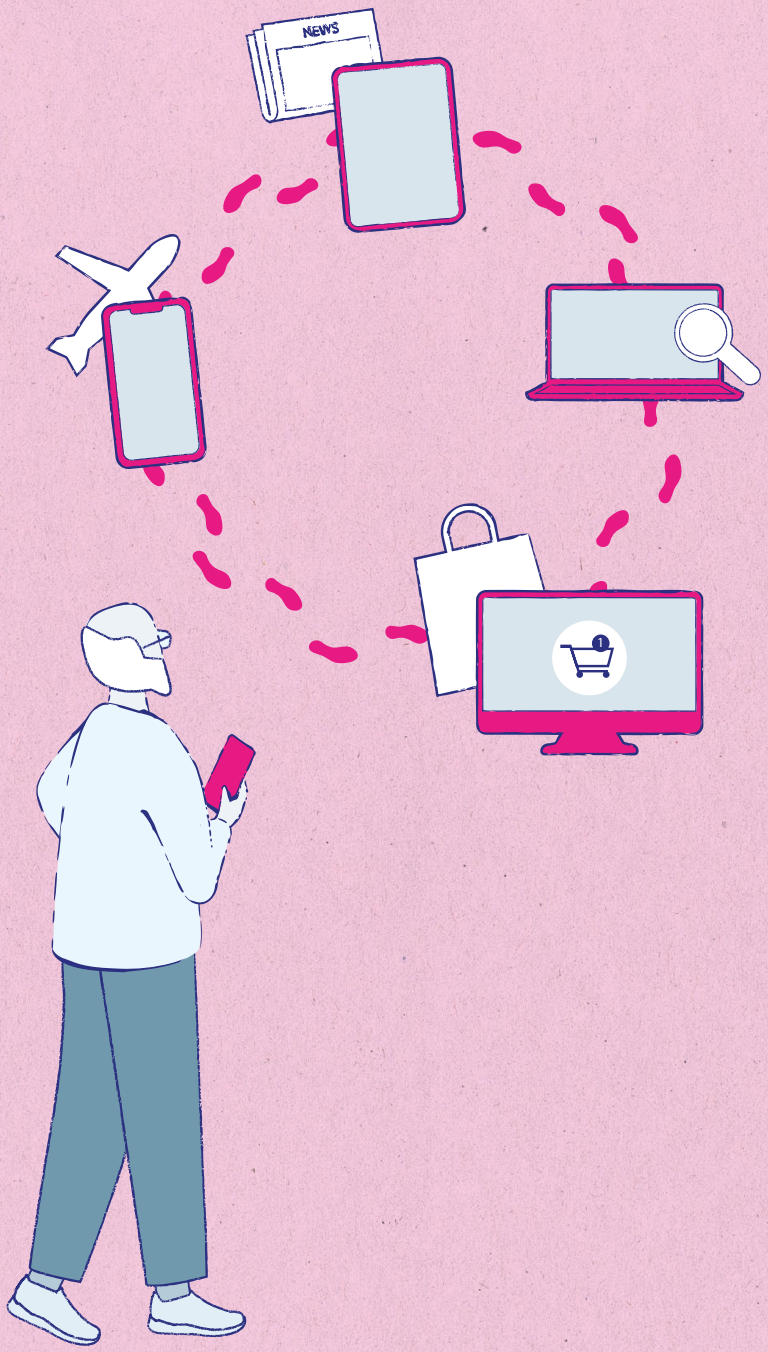
Vielleicht passiert Ihnen das auch.
Dann können Sie den Inhalt
beim Social-Media-Angebot melden.

TIPPS

Oft können Sie

- den Beitrag löschen und
- den Kontakt blockieren.

Sie können auch bei der Polizei eine Straf·anzeige stellen.


NEWS

5. Im Internet unterwegs

Cookies

Das spricht man so aus: Ku-kies.
Auf vielen Internet·seiten gibt es Cookies.
Das sind kleine Programme.
Die Programme speichern die Daten von Ihnen.
Man kann dann sehen:

- Diese Internet·seite haben Sie angeschaut.
- So lange waren Sie auf der Internet·seite.
- Das haben Sie auf der Internet·seite angeklickt.

Das heißt:
Mit Cookies kann man den Weg einer Person
durch das Internet sehen.

TIPP

Sie gehen auf eine Internet·seite.
Dann werden Sie nach Cookies gefragt.
Tun Sie das:

- **Lehnen Sie Cookies ab** oder
- **klicken Sie an: nur funktionale Cookies.**

Dann speichert die Internet·seite weniger Daten.

Weitere Informationen in Leichter Sprache:

Recht am eigenen Bild
Tipps in Leichter Sprache

Hier wird erklärt:
Darauf sollten Sie beim Fotografieren, Filmen und Posten von Bildern im Internet achten.

Das Heft können Sie bestellen: info@blm.de
oder online lesen.
Scannen Sie dazu den QR-Code:

Gefährliche Verschwörungs-Geschichten
Das können Sie dagegen tun

Hier wird erklärt:
Manche Menschen glauben an
Verschwörungs-Geschichten.
Aber es sind Lügen und sie sind gefährlich.
In dem Heft steht:
Das können Sie dagegen tun.

Das Heft können Sie bestellen: info@blm.de
oder online lesen.
Scannen Sie dazu den QR-Code:

Sicher online unterwegs
Tipps & Tricks zum Selbstdatenschutz

Das ist das Original-Heft.
Es ist in Schwerer Sprache geschrieben.

Das Heft können Sie bestellen: info@blm.de
oder online lesen.
Scannen Sie dazu den QR-Code:

Impressum

Herausgeberin
Bayerische Landeszentrale für neue Medien (BLM),
Heinrich-Lübke-Str. 27, 81737 München

Redaktion der BLM
Kerstin Prange (verantwortlich), Dr. Kristina Hopf,
Elke Hesse

Autoren der Ausgangsbroschüre
„Sicher online unterwegs –
Tipps & Tricks zum Selbstdatenschutz"
Dr. Olaf Selg, Stefan Gehrke

Übersetzung und Prüfung Leichte Sprache
AnWert e.V., Aachen

Layout/Illustration
Theresa Fischer

Druck
Senser Druck

eco zoom

natureOffice.com/DE-559-MLMERMA

Rohstoffe

Transporte

Produktion

g CO_2e

282

pro Produkt

CO_2e-Emissionen ausgeglichen

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