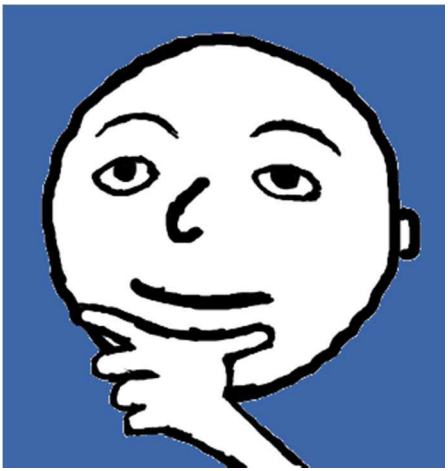
Tipps zum Schutz Ihrer Privatsphäre

in Leichter Sprache



„Wie bleibt Privates privat?“

Von

IntegrationLE

Vorwort

Wir versuchen, Ihnen das Wichtigste zum Schutz Ihrer Privatsphäre einfach zu erklären.
Wir schreiben in „Leichter Sprache“ und erklären schwere Wörter.
Leichte Sprache ist ein besonderes Deutsch mit besonderen Regeln.
Leichte Sprache können fast alle verstehen.
Das ist wichtig, vor allem bei einem so schweren Thema wie der Privatsphäre.

Viel-Leser müssen sich erst an Leichte Sprache gewöhnen.
Mehr zur Leichten Sprache finden Sie unter https://www.leichte-sprache.org/ .

Wir haben versucht, alles richtig zu schreiben.
Wir können trotzdem keine Gewähr (*Garantie*) übernehmen (*geben*), dass alles richtig ist.
Wir schließen auch eine Haftung aus (*übernehmen keine Verantwortung für Probleme*).

Vielleicht sind auch manche Internet-Adressen jetzt anders, weil es neue Adressen gibt - seit dem Schreiben von unseren Informationen.

Deshalb ist wichtig: **Informieren Sie sich auch immer selbst**, zum Beispiel beim BSI (Bundesamt für Sicherheit in der IT-Technik) www.bsi.bund.de .

Aktuelle Informationen in Leichter Sprache finden Sie auch auf unserem Blog www.it-sicherheit-ganz-leicht.de .

Wir wünschen Ihnen sicheres Arbeiten mit Ihren Geräten.

Inken Hagestedt *Stephanie Freundner-Hagestedt*

Ihre Privatsphäre

- Privatsphäre ist das, was **privat** ist und privat bleiben soll. Zum Beispiel:
  - wie Sie aussehen,
  - wen Sie lieben,
  - wer Ihre Freunde sind,
  - welche Krankheiten Sie haben,
  - wie viel Geld Sie haben,
  - was Sie einkaufen und wo Sie einkaufen,
  - was Sie essen,
  - was Sie gerne machen,
  - wo Sie jetzt sind und wo Sie waren.
- Sie wollen **selber entscheiden**, wem Sie diese privaten Sachen erzählen?
  Sie wollen nicht, dass jeder diese privaten Sachen über Sie weiß?
  Dann ist es wichtig, dass Sie Ihre **Privatsphäre schützen**.
- Warum?
  Über eine Person private Sachen zu wissen, ist ein großes **Geschäft**.
  Damit verdienen viele Firmen sehr **viel Geld**.
  Diese Firmen sammeln Informationen über Sie und verkaufen diese Informationen an andere Firmen.
- Sie sagen: Ich bin nicht interessant für eine Firma.
  Wir sagen: Doch, **auch Sie** sind sehr **interessant** für Firmen.

- Jede Firma muss Geld verdienen.
  Wenn eine Firma gute Informationen über ihre Kunden (*Käufer*) hat, dann kann Sie mehr Geld verdienen.
  - Firmen zeigen Ihnen **Werbung** auf Ihrem Smartphone oder Computer.
    Diese Werbung passt genau zu Ihnen.
    Denn die Firmen weiß, was Sie interessiert.
    Dann kaufen Sie vielleicht mehr, als Sie wollen.
  - Die Firmen schicken Ihnen Werbe-**Newsletter** von Sachen, die Sie interessieren.
  - Die Firmen wissen, dass Sie viel Geld haben:
    Sie bekommen viel Werbung für teure Sachen.
    Oder: Sie müssen einen **höheren Preis** für eine Sache bezahlen, die Sie bestellen.
  - Die Firmen wissen, dass Sie nur wenig Geld haben:
    Sie können nur bestellen, wenn Sie die Sachen **vor der Lieferung bezahlen**.
    Oder: Sie können gar **nichts bestellen** oder **keine Reise buchen**.
    Oder: Sie können **keine Raten-Zahlung** machen.
  - Restaurants und Geschäfte schicken Ihnen Werbung, weil Sie wissen, **wo Sie** gerade (*jetzt*) **sind**.
  - Sie **bewerben** sich auf eine Stelle:
    Sie **bekommen** die **Stelle nicht**, weil Sie eine Krankheit haben.
    Oder: Weil peinlich Fotos von Ihnen im Internet sind.
    Oder: Weil Sie eine bestimmte Person lieben.
    Oder: Weil Sie Kontakte mit Personen haben, über die die Firmen unangenehme (*schlechte*) Sachen wissen.
  - Ihre Anschrift oder E-Mail-Adresse werden von Kriminellen gekauft:
    Sie bekommen **peinliche Post**, **falsche Rechnungen** oder **Phishing-Mails**.

Tipps zum Schutz Ihrer Privatsphäre

- Sie können viel tun, wenn Sie Ihr Smartphone, Ihr Tablet und Ihren PC vorsichtig benutzen.
  Und wenn Sie genau überlegen, was Sie tun.
  Wie das geht, steht in unserer Broschüre „**IT-Sicherheit – ganz leicht**“.
  Eine Zusammenfassung **wichtiger Tipps für Ihre elektronischen Geräte** finden Sie auch ab der Seite 10.
  Sie finden die Broschüre auf unserer Internetseite
  www.it-sicherheit-ganz-leicht.de
- Aber: Sie können Ihre Privatsphäre auch noch anders schützen.
  Wie? Das erklären wir Ihnen hier in unseren **Tipps für den Alltag**.

Tipps für den Alltag

- Überlegen Sie, ob Sie Einkäufe, Dienste und anderes **bewerten** oder **liken**.
  Dabei geben Sie Firmen viele Informationen über sich.
- Überlegen Sie, an welchen **Preisausschreiben** (*Gewinnspiel*) Sie teilnehmen.
  Dabei zeigen Sie Ihre Interessen und was Sie gerne haben möchten.
  Und Sie geben Ihre Anschrift oder Ihre E-Mail-Adresse an Firmen.

Tipp

- Antworten Sie nicht auf **Spam-Mails** (*unerwünschte E-Mails*).
  - Dann bekommen Sie noch mehr Spam-Mails.
    Warum? Weil der Absender der Spam-Mail dann weiß, dass bei Ihrer Adresse die E-Mails ankommen und gelesen werden.
  - Benutzen Sie einen Spam-Filter (*Programm zum Erkennen von Spam-Mails*).
    Schauen Sie ab und zu, ob interessante E-Mails in den Spam-Filter einsortiert wurden.
    Danach löschen Sie die Spam-Mails.
- Geben Sie nur bei wichtigen Sachen Ihre **Anschrift** und Ihre **E-Mail-Adresse** an.
- Wenn Sie etwas bestellen oder auf einer Internetseite sind: Sehen Sie nach, ob Ihnen automatisch ein **Newsletter** (*Informations-E-Mail*) geschickt wird.
  - Nur wenn Sie interessiert sind, sollten Sie einen Newsletter bestellen.
  - Melden Sie Newsletter ab, wenn Sie daran nicht interessiert sind.
    Dann wird auch Ihre E-Mail-Adresse gelöscht.
- Wenn Sie **Werbung** und **Kataloge** mit der Post bekommen:
  - Schreiben Sie eine E-Mail an den Absender, dass Sie das nicht wollen.
  - Widersprechen (*verbieten*) Sie auch der Weitergabe Ihrer Daten (*Informationen*) an Dritte (*andere Personen*).
    Dann darf der Absender Ihre Adresse und andere Informationen nicht mehr verkaufen.

- Die „**Deutsche Post Direkt GmbH**“ analysiert (*untersucht*), welche Briefe Sie bekommen.
  - Die „Deutsche Post Direkt“ gehört zur „Deutschen Post AG“.
  - Sie „vermietet“ die Adressen. Das ist legal (*erlaubt*).
  - Das geht zum Beispiel so: Sie haben eine Computer-Zeitung abonniert (*bestellt*).
    Diese Zeitung bekommen Sie jeden Monat.
    Plötzlich bekommen Sie auch Werbebriefe und Kataloge von Computer-Firmen.
    Die „Deutsche Post Direkt“ hat von den Computerfirmen den Auftrag bekommen, Briefe und Kataloge an Computer-Interessierte zu schicken.
  - Wenn Sie das nicht möchten, können Sie bei der „Deutschen Post Direkt“ widersprechen.
    Die E-Mail-Adresse ist: online-services@postdirekt.de

- Überlegen Sie, ob eine **Kundenkarte** von einem Geschäft oder eine **Bonuskarte** gut für Sie ist.

  Bonuskarten sind zum Beispiel „Payback-Karte“ oder „Deutschlandcard“.
  Oft bekommen Sie Rabatt (*geringerer Preis*), wenn Sie diese Karten zeigen.
  Aber: Alle Informationen über Ihre Einkäufe werden gespeichert und analysiert.

- Überlegen Sie sich, wann Sie bar **bezahlen** und wann mit EC-Karte oder Kreditkarte.
  Wenn Sie alles mit **Karte** bezahlen, geben Sie viele Informationen an Ihre Bank.

- Schalten Sie **GPS** an Ihrem Smartphone aus, wenn Sie es nicht brauchen.

Tipp

  Verbieten Sie die Standortabfrage (*Frage nach dem Ort*) an Ihrem PC.

- Kleben Sie die **Kamera** von Ihrem PC ab, wenn Sie die Kamera nicht brauchen, zum Beispiel mit einem Pflaster für empfindliche Haut.
  Dann bleibt die Kamera sauber und Sie können sie sofort benutzen, wenn Sie wollen.
  Aber: Kein Hacker (*Angreifer*) kann Sie über Ihre Kamera beobachten.

Tipp

- **Suchen** Sie ab und zu **nach Ihren Namen** mit Ihrer Suchmaschine (*Programm zur Suche im Internet*).
  Dann wissen Sie, was andere Personen über Sie im Internet finden können.
  Wenn Sie falsche Angaben oder falsche Fotos über sich finden, können Sie die Löschung von der Internetseite oder von dem Dienst verlangen (*fordern*).

- Überlegen Sie genau, welche **smarten** (*intelligente*) **Geräte** Sie benutzen wollen.
  Smarte Geräte schicken viele Informationen von Ihnen an Firmen.
  Informieren Sie sich über die Sicherheitseinstellungen.

- Benutzen Sie einen **Sprach-Assistenten** (zum Beispiel Alexa, Siri, Cortana, Google Assistant)?
  - Schalten Sie das **Mikrofon** mit dem Schalter **aus**, wenn es möglich ist und Sie den Assistenten jetzt nicht brauchen.
  - Oder nehmen Sie den Assistenten **vom Strom** (*den Stecker aus der Steckdose ziehen*).
  - Ändern Sie den **Weckruf** (*Wort zum Aktivieren vom Gerät*), wenn Sie oder jemand in Ihrer Familie einen Namen hat, der so ähnlich wie der Weckruf ist.
  - Nennen Sie keine **Passwörter** (*Kennwörter*) oder andere Zugangsdaten (*Anmeldewörter*) für Konten, solange der Assistent aktiv werden kann.

Tipp

- **Widersprechen** Sie der „Verwendung von Aufnahmen für die Weiterentwicklung des Dienstes“.
  Oft geht dies unter der Überschrift „Bei der Entwicklung von neuen Funktionen mithelfen“ oder einer ähnlichen Überschrift bei der Firma vom Sprachassistenten.
- Sie können gemachte Aufnahmen von sich auch löschen lassen.

➢ Benutzen Sie ein **Smart-TV** (*Fernseher, der ins Internet gehen kann*)?

- **Schalten** Sie den Fernseher ganz **aus**, wenn Sie ihn jetzt nicht benutzen.
  Am besten geht das Ausschalten über eine schaltbare Steckdose (*Steckdose mit Schalter*).
  Wenn der Fernseher auf Stand-by ist, kann er noch arbeiten und ins Internet gehen.
- Kleben Sie die **Kamera** ab, wenn Sie sie jetzt nicht brauchen, zum Beispiel mit einem Pflaster für empfindliche Haut.
  Dann bleibt die Kamera sauber und Sie können sie sofort wieder benutzen, wenn Sie sie brauchen.
- Überlegen Sie, ob Ihr Fernseher immer **Zugang zum Internet** haben darf.
  Dann kann er auch immer Informationen über Sie an die Firma schicken.
  Zum Beispiel über das, was Sie sich über den Fernseher ansehen.
  Oder auch das, was die Kamera und das Mikrofon über Sie aufnehmen.
- Über ein **WLAN** (*Verbindung von Geräten über Funk*) können Sie dem Fernseher den Zugang zum Internet immer nur dann freischalten (*einschalten*), wenn Sie das wollen.
  Das ist unbequem, aber sicherer.

- Sie können auch **über** Ihren **PC** ins Internet gehen und ihn mit einem HDMI-Kabel (*Kabel zum Übertragen von Bildern und Ton*) an den Fernseher anschließen.
  Dann arbeitet der Fernseher nur als großer Bildschirm und kann nicht selber ins Internet.

- Haben Sie andere **smarte Geräte**?
  - Informieren Sie sich über die Vorteile und über die Risiken.
  - Überlegen Sie sich genau, ob und wie Sie die Verbindung zum Internet frei geben.
- Denken Sie daran: Für vieles im Internet bezahlen Sie kein Geld.
  Aber: Sie **bezahlen mit Informationen** über sich.
  Die Fachleute nennen diese Informationen „Daten“.

Wichtige Tipps für Ihre elektronischen Geräte

- Überlegen Sie immer:
  Brauche ich diese App (*Programm*) oder diesen Dienst?
  Wie oft brauche ich diese App oder diesen Dienst wirklich?

- **Informieren** Sie sich, ob diese App oder dieser Dienst sicher ist.
  Geben Sie dafür den Namen von der App oder von dem Dienst in Ihre Suchmaschine ein und lesen Sie die Testberichte.

- Informieren Sie sich auch in den **Nutzungsbedingungen** von Apps, von Diensten und von Internet-Shops über die Verwendung (*Benutzung*) Ihrer Daten.
- **Blockieren** (*nein sagen*) Sie so viel wie möglich in den Apps und Diensten.

- Denken Sie daran, dass viele Apps und Dienste Ihre Adressliste, Ihre Fotos, gespeicherte **Daten von Ihrem Smartphone** kopieren und speichern.
  Auch Ihre GPS-Daten werden gespeichert.
  So wissen die Betreiber (*Firmen*) der Apps und Dienste, wo Sie oft sind, wo Sie jetzt sind und wo Sie wann waren.

- Schreiben Sie keine sehr **privaten Sachen** in E-Mails, Messengern (*Dienst für schnelle Kommunikation*) oder Social Media (*Soziale Medien*).

Tipp

- Posten (*im Internet öffentlich machen*) Sie **keine peinlichen Fotos** von sich und anderen.
- Schreiben Sie in Ihr **Profil** (*Angaben zu Ihrer Person*) so wenige Informationen wie möglich.
- Geben Sie bei Social Media an, dass Sie nicht von **Suchmaschinen** erkannt werden wollen.
- Melden Sie sich nicht über Social Media auf einer anderen Internetseite an.
  Rufen Sie andere **Internetseiten** immer direkt auf.
- Überprüfen Sie ab und zu die Einstellungen von Ihrem **Browser** (*Programm zum Surfen im Internet*) und anderen Diensten.
  Die Betreiber (*Firmen*) können Ihre Einstellungen ändern, ohne dass Sie das wissen.
- Bestellen Sie in **Internet-Shops** als „Gast“, wenn das möglich ist.
- **Loggen** (*abmelden*) Sie sich bei Messengern, Social Media, Diensten oder Internet-Shops **aus**, wenn Sie diese jetzt nicht benutzen.
- **Löschen** Sie Ihren **Account** (*Konto*) auf Internetseiten, Social Media und anderen Diensten, wenn Sie ihn nicht mehr brauchen.

- Benutzen Sie eine **Suchmaschine**, die Ihre Suche nicht verfolgt und speichert, zum Beispiel „Startpage“ oder „Duckduckgo“.
- Lassen Sie beim Ansehen von Internetseiten keine **Cookies** (*Daten von Anbietern, die von Internetseiten auf Ihr Gerät übertragen werden*) zu, wenn es möglich ist.
  Und: Stellen Sie Ihren Browser so ein, dass alle Cookies gelöscht werden, wenn Sie Ihren Browser schließen.
- Stellen Sie Ihren Browser so ein, dass er keine **Chronik** (*zeigt, welche Internetseiten Sie aufgerufen haben*) macht.
  Dann speichert der Browser nicht, welche Internetseiten Sie sich angesehen haben.
- Überlegen Sie, welche Daten und Fotos Sie in einer **Cloud** (*Speicherplatz im Internet*) speichern.
- Denken Sie daran:
  Benutzen Sie gute Passwörter und die Zwei-Faktor-Authentifizierung (*Einloggen in 2 Schritten*)**, wenn es möglich ist.**

- Mehr Informationen finden Sie in unseren Tipps „IT-Sicherheit ganz leicht“.
  Und auf unserer Internetseite www.it-sicherheit-ganz-leicht.de