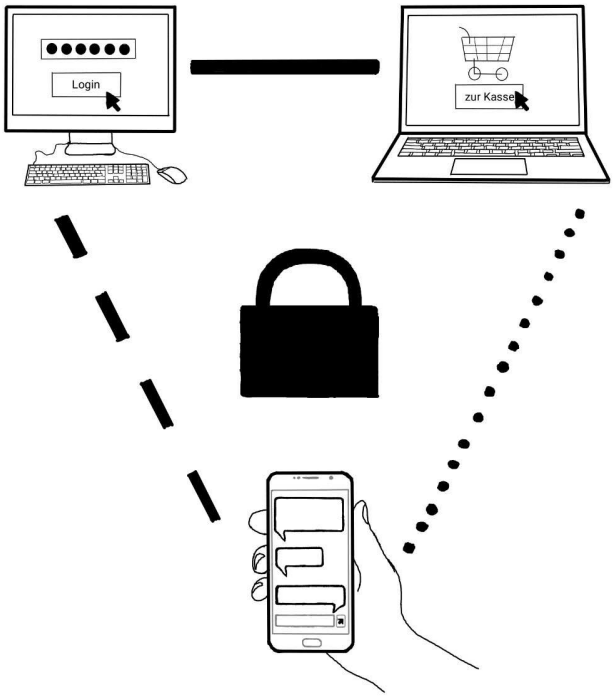
Mehr Sicherheit für Smartphone, Tablet und PC

Einfache Erklärungen und Tipps
in Leichter Sprache



Von

IntegrationLE

Vorwort

Wir versuchen, Ihnen das Wichtigste für die Sicherheit Ihrer elektronischen Geräte 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 Sicherheit.

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 Drucken von unseren Informationen.

Deshalb ist es 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*

Wichtige Informationen

- Sie haben **elektronische Geräte**? Zum Beispiel:
  - ein Smartphone
  - ein Tablet
  - einen Laptop
  - oder einen PC
- Sie können viele interessante Sachen mit diesen Geräten machen. Zum Beispiel:
  - **chatten** (*Nachrichten verschicken und bekommen; telefonieren*),
  - **mailen**,
  - nach **Informationen** suchen,
  - **Online-Banking** machen (*Geld überweisen und Ihr Konto bei der Bank ansehen*),
  - **bestellen**,
  - offizielle Sachen regeln wie die Steuererklärung, **Formulare** ausfüllen oder **Anträge** stellen (*machen*),
  - **Musik hören**, **Filme sehen**, **spielen**.
- Für diese Sachen brauchen Sie das **Internet**.
- Achtung: Sie müssen Ihre Geräte **schützen**. Sonst können andere Personen über das Internet auf Ihre Geräte zugreifen (*etwas auf Ihren Geräten machen*).

- Warum? - Diese Personen wollen zum Beispiel:
  - Ihre Passwörter wissen, um **auf Ihre Rechnung einzukaufen**.
  - Ihre Zugangsdaten für das Online-Banking wissen, um **Geld von Ihrem Konto abzubuchen** (*wegnehmen*).
  - Alles auf Ihren Geräten verschlüsseln (*verändern, dass Sie es nicht mehr öffnen und lesen können*) und Sie **erpressen** (*Sie sollen Geld bezahlen, damit Sie alles wieder lesen können*).

- Viel über Sie wissen, um dieses **Wissen** an Firmen zu **verkaufen** oder Sie zu **mobben** (*Schlechtes über Sie schreiben und sagen*).
- Ihre persönlichen Daten wissen, um mit Ihrer **Identität** Straftaten zu begehen (*kriminelle Sachen zu machen*).
- Ihre Geräte benutzen, um andere Geräte anzugreifen (*eindringen und steuern*).

➢ Fachleute haben dafür besondere Wörter:

- **Phishing**: Stehlen von Zugangsdaten und anderen Informationen.
- **Doxing**: Sammeln und veröffentlichen von Daten anderer Personen im Internet.
- **Hacken**: Suchen von Lücken in der Sicherheit von Computer-Programmen oder Apps.
  Und: über diese Lücken fremde Geräte steuern.
  Oder: schädliche Programme auf den Geräten installieren (*speichern*), zum Beispiel Viren, Würmer und Trojaner.
  - **Viren** sind Programme, die sich auf Geräten selbstständig **vermehren**.
    Viren versuchen, sich auf andere Geräte zu **verbreiten**.
    Viren schaden oder **zerstören** (*kaputt machen*) andere Programme und manchmal auch die Hardware (*Geräte und Zubehör, das man anfassen kann*).
  - **Würmer** sind Programme, die sich selbstständig **vermehren** und auf andere Geräte **verbreiten**.
    Ihre Geräte werden durch Würmer **sehr langsam** oder arbeiten gar nicht mehr richtig.
    Würmer schaden anderen Programmen und der Hardware nicht.
  - **Trojaner** sind Programme, die **spionieren** (*sehen, was Sie machen*) und diese Informationen an den Spion senden.

- Sie können **selber** viel tun, um Ihre Geräte,
  Ihre persönlichen Daten und Ihre Konten zu **schützen**.
  Dann machen Sie den Zugriff auf Ihre Daten und
  Ihre Geräte schwer.
- Aber: Einen Schutz gegen alles gibt es nicht.
  Und: Sie müssen immer selber **aktiv sein und bleiben**.

- In dieser Broschüre (*Heft*) können Sie **Tipps zu** diesen Themen lesen:
  - sicherer und privater **chatten** (ab Seite 8),
  - sicherer und privater in **Social Media** (*Sozialen Medien*) (ab Seite 12),
  - sicherer **mailen** (ab Seite 19),
  - sichere **Verbindung** von Ihren Geräten **mit** dem **Internet** (ab Seite 27),
  - sicherer und privater im **Internet** (ab Seite 31)**:**
    - **Browser** (ab Seite 31),
    - **Firewall** und **Virenscanner** (ab Seite 37),
    - sicherer **surfen** (*Internetseiten ansehen*) (ab Seite 40),
    - sicheres **Online-Banking** (ab Seite 42),
  - sichere **Passwörter** (ab Seite 43):
    - **Passwort-Manager** (ab Seite 46),
    - **Zwei-Faktor-Authentifizierung** (ab Seite 48),
    - **Sicherheitsabfragen** (ab Seite 49),
  - gutes **Backup** (*Sicherungskopie*) (ab Seite 50),
  - sichere **Software** (*Programme*) (ab Seite 53),
  - für die **erste Hilfe**, wenn etwas passiert ist (ab Seite 58),
  - zum Verstehen von **Fachbegriffen** (*Fachwörtern*) (ab Seite 62).

- Sie denken vielleicht: Im **Internet** ist vieles **kostenlos**?
- Das ist **nicht** ganz **richtig**.
  Sie bezahlen oft kein Geld.
  Aber: Sie **bezahlen mit Informationen** über sich selber.

- Die Internet-Firmen benutzen diese Informationen oder verkaufen sie an andere Firmen.
- Warum? - Die Firmen schicken Ihnen **Werbung**, die genau zu Ihnen passt.
  Und dann kaufen Sie vielleicht mehr, als sie wollen und brauchen.
- Was können Sie tun? Überlegen Sie:

  - **Brauche ich** dieses Programm oder diese App (*Programm*) wirklich?
    Möchte ich diese Internetseite wirklich nutzen?
  - **Welche Informationen** will dieses Programm, diese App oder diese Internetseite über mich haben?
    Möchte ich wirklich mit diesen Informationen dafür bezahlen?

- Sie denken vielleicht:
  Niemand interessiert sich für mich und **meine Daten**.
- Das **stimmt nicht**.
  Viele Firmen wollen die Daten von möglichst vielen Personen haben.
  Sie verdienen damit sehr viel Geld.
  Auch **Ihre Daten** sind **interessant**.

- Sie denken vielleicht:
  So **viele** Menschen **benutzen** dieses Programm.
  Oder: So viele Menschen machen das genauso wie ich.
  Dann muss es gut sein und ist nicht gefährlich.
- Das **stimmt nicht**.
  Auch **viele** Menschen können **gleiche Fehler** machen.

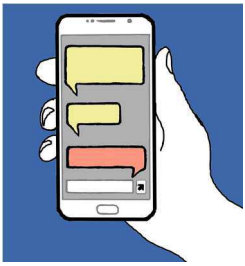
- Was können Sie tun?
  Informieren Sie sich.
  Werden und bleiben Sie **aktiv** und **schützen** Sie sich.
  Dann sind Sie **sicherer**.

- Sie denken vielleicht:
  Ich kann doch alles mit meinen Geräten machen, was ich will.
  Und jetzt soll ich diese ganze Broschüre lesen?
- Wir sagen: ja!
  Sie fragen vielleicht: warum?
- Wir fragen Sie:
  Lassen Sie alle Fenster und Türen von Ihrer Wohnung offen, wenn Sie weggehen? – Nein?
  Warum lassen Sie dann Betrügern und Hackern eine große Chance, Ihnen zu schaden?
- Leider müssen Sie viel wissen, um sich zu schützen.
  Aber: Es lohnt sich. Denn Sie werden sicherer.
  Und: **Sie müssen sich selber schützen!**
  Das kann niemand anderes für Sie tun.
  Auch die Polizei kann Ihnen dabei nicht helfen.

- Nehmen Sie sich Zeit für Ihre eigene Sicherheit und Privatsphäre.
- Lesen Sie diese Broschüre **Schritt für Schritt**.
  Überlegen Sie:
  - Was ist wichtig für mich?
  - Was möchte ich ändern oder **sicherer machen**?

- Wir sagen: Sie schaffen das!
  Wir mussten das auch alles erst lernen.
- Aktuelle Informationen in Leichter Sprache finden Sie auf unserem Blog (*besondere Form einer Internetseite*)
  www.it-sicherheit-ganz-leicht.de .

Erklärungen und Tipps



Instant-Messenger:

- Instant-Messenger werden auch kurz **Messenger** genannt.
- Messenger sind Dienste für eine schnelle **Kommunikation** (*Austausch von Nachrichten*).
- Messenger gehören zu den Social Media (Sozialen Medien).
- **Social Media** sind die digitalen (*elektronische*)Techniken, über die Nutzer (*jemand, der etwas benutzt*) kommunizieren und Informationen austauschen können.
- Messenger sind zum Beispiel „WhatsApp“, „Skype“, „Signal“, „Google Hangout“, „iMassage“, „Telegram“ und der „Facebook-Messenger“.
- Die Nutzer von Messengern werden mithilfe von einem speziellen Computerprogramm über das Internet miteinander verbunden.
  Solche Computerprogramme nennt man **Client** (*Messenger-Programm*).
- Nutzer von Messengern
  - kommunizieren über Textnachrichten,
  - verschicken Anhänge,
  - verschicken Sprachnachrichten, Bilder und Video-Nachrichten,
  - telefonieren,
  - chatten (*Nachrichten austauschen*) in Gruppen.

- Die meisten Messenger sind kostenlos.
  Sie bezahlen also kein Geld dafür.
- Aber: Für die meisten Messenger bezahlen Sie mit **Informationen über sich**.

- Deshalb: Informieren Sie sich in den **Nutzungsbedingungen** (*Regeln für das Benutzen*) von den Anbietern, welche Informationen die verschiedenen Dienste von Ihnen speichern.

- **Überlegen** Sie genau, welchen Messenger Sie nehmen.

- Der Messenger, den viele von Ihren Freunden benutzen, muss nicht der richtige für Sie sein oder ist Ihnen vielleicht nicht sicher genug.
- **Informieren** Sie sich und überlegen Sie, welcher Messenger für Sie am besten passt.
- Vielleicht können Sie auch Ihre Freunde überzeugen (*mit guten Gründen dazu bringen*), zu Ihrem Messenger zu wechseln.
- Informationen über Messenger finden Sie beim BSI.
- So finden Sie Informationen:
  Geben (*schreiben*) Sie in Ihre Suchmaschine (*zum Beispiel „Google“ oder „Startpage“*) die Stichworte „BSI“ und „Messenger“ ein.

- Laden (*auf Ihr Gerät übertragen*) Sie den Client für den ausgewählten Messenger immer nur aus dem **App-Store** von Ihrem Smartphone oder von der **Original-Internetseite** vom Anbieter herunter.
  Das ist am sichersten.

- So finden Sie die Original-Seite:
  Geben Sie den Name des Clients in Ihre Suchmaschine ein.

- Sehen Sie sofort in die **Einstellungen**.
  Deaktivieren Sie alles, was Sie können. – Warum?
  So geben Sie dem Anbieter am wenigsten Information über sich.
  Damit schützen Sie Ihre Privatsphäre.

- Die Einstellungen finden Sie im Menü vom Client.
  Das Menü ist die Liste von Funktionen.
  Oft wird das Menü mit drei Strichen übereinander angezeigt oder mit Punkten nebeneinander

---

- Laden Sie immer **sofort alle Updates** und **Upgrades** für Ihren Messenger herunter.
  Das sind Verbesserungen von einem Programm.
  Mehr dazu finden Sie ab Seite 54.
- Jeder Anbieter hat ein Interesse daran, dass sein Betriebssystem sicher ist.
  Deshalb verbessert der Anbieter die Sicherheit ständig durch **Sicherheits-Updates**.
  Laden Sie deshalb immer alle Sicherheits-Updates sofort herunter.

- Achtung:
  Sie bekommen eine Nachricht, dass ein **neues Gerät** auf Sie **angemeldet** wurde.

- Was können Sie tun, wenn Sie kein neues Gerät angemeldet haben?
  - **Wenden** (*Kontakt aufnehmen*) Sie sich **sofort** an den **Anbieter** von Ihrem Messenger.
  - Sonst kann eine andere Person Ihre gesamte Kommunikation über diesen Messenger mitlesen.

- Denken Sie daran:
  Alles, was Sie über einen Messenger kommunizieren, **kann öffentlich** (*viele anderen Personen bekannt*) **werden**.

Tipp

- Bitte schreiben und sprechen Sie nur über Sachen, die **nicht** sehr **privat** sind.
- Nehmen Sie ein gutes **Bild** für Ihr Profil (*Angaben über sich*).
  Es sollte **nicht peinlich** (*unangenehm*) sein.
  Bei vielen Messengern kann es auch ein anderes Bild als ein Foto von Ihrem Gesicht sein.

- Denken Sie auch daran:
  Jeder kann Ihre Handy-Nummer lesen und Sie anrufen.

- Überlegen Sie genau, welche **Kontaktanfragen** Sie annehmen.

- Solche Kontaktanfragen können auch kommen
  - von Kriminellen,
  - von Personen, die Sie mobben (*schlecht über Sie sprechen oder schreiben*) wollen,
  - von Computern, die viele Informationen über Sie sammeln oder Sie falsch informieren wollen.

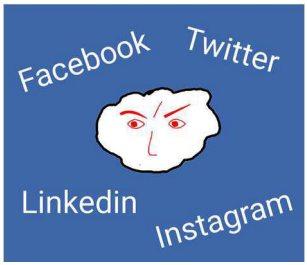
- Laden (*im Messenger speichern und zeigen*) Sie keine Fotos oder Texte hoch, die Sie **nicht selber** gemacht haben.
  Das ist **ungesetzlich** (*gegen Gesetze*).
- Wenn Sie Fotos gemacht haben, auf denen auch **andere Personen** zu sehen sind:
  Fragen Sie immer erst, ob diese Personen mit dem Hochladen von Fotos **einverstanden** sind.
  Sonst dürfen Sie diese Fotos nicht hochladen.

- **Teilen** (*etwas auch an andere schicken*) Sie **keine Fotos von anderen Nutzern** und leiten (*schicken*) Sie solche Fotos nicht weiter.
  Das kann große Probleme geben.
- Schreiben und teilen Sie **keine** Texte mit **bösen** oder **sexuellen Aussagen** (*Inhalt*) oder leiten Sie keine solchen Texte weiter.
  Das kann große Probleme geben.

- Achtung: Überlegen Sie genau, bevor Sie **Anhänge** öffnen.
  Darin kann **Schad-Software** (*schädliche Programme*) sein.
- Achtung: Überlegen Sie genau, bevor Sie auf einen **Link klicken** (*eine genannte Internetadresse öffnen*).
  Der Link kann Sie zu einer Internetseite führen, die Ihnen **Schad-Software** auf Ihr Gerät lädt.

- Schreiben Sie **keine negativen Sachen über Ihre Arbeit**, Ihren Chef oder Ihre Kollegen.
  Was Sie geschrieben haben, könnte Ihr Chef irgendwann finden und lesen.
  Das kann ein Grund für eine **Kündigung** sein.

Facebook, Instagram, Twitter und andere Social Media



- Es gibt viele verschiedene **Social Media** (Soziale Medien, Soziale Netzwerke).
- Die bekanntesten sind zurzeit (*jetzt*) „**Facebook**“, „**Instagram**“ und „**Twitter**“.

- Das Social Media, das von vielen Ihrer Freunde benutzt wird, muss nicht das richtige für Sie sein oder Ihnen sicher genug sein.
- **Informieren** Sie sich und überlegen Sie, welches Social Media für Sie am besten passt.
  Mehr Informationen finden Sie beim BSI.
  Geben (*schreiben*) Sie in Ihre Suchmaschine die Stichworte „BSI“ und „Soziale Netzwerke“ ein.

- Die Nutzung von den meisten Social Media ist kostenlos.
  Sie bezahlen also kein Geld dafür.
  Aber: Sie **bezahlen mit Informationen** über sich.

- Lesen Sie die **Nutzungsbedingungen** (*Regeln vom Anbieter für das Benutzen*).
  Dann sehen Sie, welche Informationen von Ihnen gespeichert werden.

- Oft gehen auch die **Rechte** von Ihren Bildern und von Ihren Texten an das Social Media.
  Das heißt: Ihre Bilder und Ihre Texte gehören dem Social Media und nicht mehr Ihnen.
  Das Social Media kann Ihre Bilder und Ihre Texte verkaufen.

- Laden (*auf ihr Gerät übertragen*) Sie nur **Apps** für das gewünschte Social Media aus dem **App-Store** passend für Ihr Gerät herunter.

- Oder: Registrieren (*eintragen*) Sie sich und melden Sie sich nur direkt auf der **Original-Internetseite** vom gewählten Social Media an.
- Gehen Sie sofort in die **Einstellungen**.
  Die Einstellungen finden Sie im Menü.
  Das Menü ist die Liste von Funktionen.
  Oft wird das Menü mit drei Strichen übereinander angezeigt oder mit Punkten nebeneinander.

- **Deaktivieren** Sie alles, was Sie können. – Warum?
  So geben Sie am wenigsten Information über sich an den Anbieter.
  Damit schützen Sie Ihre Privatsphäre.
- Benutzen Sie für die **Registrierung** die **Zwei-Faktor-Authentifizierung** möglichst auf 2 verschiedenen Geräten.
  Mehr zur Zwei-Faktor-Authentifizierung finden Sie ab Seite 48.
- Laden Sie immer sofort **alle Updates** und **Upgrades** herunter.
  Das sind Verbesserungen von einem Programm.
  Mehr dazu finden Sie auf der Seite 54.

- Wenn Sie die Nachricht bekommen, dass Sie ein **neues Gerät angemeldet** haben:
  Reagieren Sie **sofort**, wenn Sie kein neues Gerät angemeldet haben.
  Kontaktieren Sie Ihren **Anbieter**.
  Sonst kann vielleicht eine andere Person alles mitlesen.

- Denken Sie daran:
  In Social Media aktiv zu sein, kostet Sie **Zeit**.
  Sie brauchen und sollten nicht immer gleich antworten.
- Online in Social Media dürfen Sie nur **in Ihrer Freizeit** sein.
  Am Arbeitsplatz ist das Benutzen von privaten Smartphones oft nur in den Pausen erlaubt.
  In der Schule ist das Benutzen von Smartphones oft ganz verboten.

- Achtung: Sie dürfen nur **Fotos** von Personen machen und hochladen (*dort speichern und zeigen*),
  wenn diese Personen gesagt haben,
  dass sie damit **einverstanden** sind.

- **Überlegen** Sie genau, welche **Freundschafts-Anfragen** Sie annehmen.
  Am besten nehmen Sie nur Anfragen von Personen an, die Sie schon kennen.

- Achtung: Freundschafts-Anfragen können gefährlich sein:
  - Freundschafts-Anfragen können auch von **Kriminellen** kommen. – Warum?
    Die Kriminellen wollen Kontakt mit Ihnen haben, um Straftaten (*etwas gegen die Gesetze*) zu begehen (*machen*).
  - Freundschafts-Anfragen können auch **von Computern** kommen. – Warum?
    Die Computer-Programme wollen Ihre **Meinung** mit bestimmten Informationen **manipulieren** (*beeinflussen, lenken*).
    Solche Computer-Programme reagieren automatisch auf Fragen und bestimmte Stichworte.
    Solche Computer-Programme nennen Fachleuten **Bot**.
    Über solche Computer werden manchmal sogar Wahlen manipuliert.

- Denken Sie daran:
  Sie können auch **Personen** wieder aus Ihrer Gruppe **entfernen** (*wegnehmen*).

- **Merkwürdige** (*passt nicht zu Ihnen und zur Situation*) **Nachrichten** sollten Sie nicht beantworten und teilen (*an andere Personen weiterschicken*).

- **Merkwürdige Fotos** sollten Sie nicht kommentieren (*etwas dazu schreiben*) und teilen.

- In Social Media bleibt fast **nichts privat**.
- **Überlegen** Sie genau, was Sie in Ihr **Profil** (*Angaben über sich*) schreiben und andere Personen lesen können.

- Sie müssen wissen:
  Alles, was Sie hochladen kann über andere Nutzer vielen Personen **bekannt** werden, auch Ihrem Chef und Ihren Kollegen.
- Deshalb: **Laden Sie keine peinlichen Texte und Fotos hoch**.
  Denn: Viele Firmen prüfen, was sie von Bewerbern auf eine Stelle in Social Media finden.

- Laden Sie keine Fotos oder Texte hoch, die Sie **nicht selber** gemacht haben.
  Das ist **ungesetzlich** (*gegen Gesetze*).

- **Teilen** (*etwas auch an andere schicken*) Sie **keine Fotos** von anderen und leiten (*schicken*) Sie keine solchen Fotos weiter.
  Das kann große Probleme geben.
- Schreiben und teilen Sie **keine** Texte mit **bösen** oder **sexuellen Aussagen** (*Inhalt*) oder leiten Sie keine solchen Texte weiter.
  Das kann große Probleme geben.

- Achtung:
  Überlegen Sie genau, bevor Sie **Anhänge** öffnen.
  Darin kann **Schad-Software** sein.

- Achtung:
  Überlegen Sie genau, bevor Sie auf einen **Link klicken** (*in eine Nachricht geschriebene Internetadresse öffnen*).
  Der Link kann Sie zu einer Internetseite führen, die Ihnen **Schad-Software** auf Ihr Gerät lädt.

- **Glauben** Sie **nicht alles**, was Sie in Social Media lesen.

- **Informieren** Sie sich auch immer über andere Quellen, zum Beispiel Fernsehen, Nachrichten-Seiten im Internet oder Zeitungen.
- Bilden Sie sich **selber** Ihre **Meinung**. – Warum?
  Über Social Media werden oft falsche Nachrichten an viele Nutzer geschickt.
  Solche falschen Nachrichten nennt man **Fake-news**.

- Mit Fake-news wollen bestimmte Personen Ihre Meinung **manipulieren**, zum Beispiel vor wichtigen Wahlen.
- Oft bekommen Sie auch vom Anbieter mehr **Nachrichten**, die gut **zu Ihnen passen**.
  Andere Nachrichten bekommen Sie nicht so oft oder gar nicht.
- Warum?
  Sie sollen möglichst viel Zeit in dem Social Media bleiben.
  Deshalb schickt der Anbieter Ihnen möglichst viele Informationen, die Sie gerne lesen.

- Es kann sein, dass **Kriminelle** mit Ihnen **Kontakt** haben.
- Sie denken, es sind gute Freunde.
  Aber alles ist **falsch**, was diese Kriminellen Ihnen **schreiben**.

- **Besondere Vorsicht** ist wichtig,

  - wenn jemand will, dass Sie ihm ein **Nackt-Foto** von sich schicken,
  - wenn jemand sich mit Ihnen **treffen** will,
  - wenn jemand sie um **Geld** bittet,
  - wenn jemand Ihnen etwas geben will, das Sie für ihn **aufbewahren** (*für eine Zeit lang bei Ihnen sein*) sollen,
  - wenn jemand möchte, dass er Ihnen **Geld** schickt und Sie es auf an anderes Konto **weiterschicken** sollen.
  - wenn jemand möchte, dass Sie irgendetwas anderes für ihn **heimlich** (*niemand anderes soll es wissen*) tun sollen.

- **Überlegen** Sie immer genau:

  - Für welchen Freund würde ich so etwas wirklich tun?
  - Kenne ich diese Person nur über Social Media oder auch im realen (*in der richtigen Welt*) Leben?

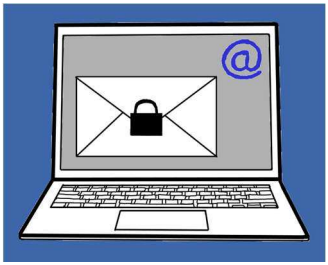
- Wenn Sie unsicher sind, **sprechen** Sie mit Freunden oder Ihrer Familie darüber.

- Gehen Sie **nicht alleine** zu einem **Treffen** mit einer Person, die Sie nur über Social Media oder Messenger kennen.

  Treffen Sie sich an einem Ort, wo **auch andere Menschen** sind, zum Beispiel in einem Café oder einem Restaurant.
  Gehen Sie **erst** mit zu jemandem **in** seine **Wohnung**, wenn Sie ihn mehrere Male getroffen und ihn wirklich **gut kennengelernt** haben.

- Wenn Sie **vorsichtig** sind, genau überlegen und mit vertrauten Personen darüber sprechen, haben **Kriminelle wenige Chancen** bei Ihnen.

Sicherer Mailen:



- Eine **E-Mail** ist eine Nachricht, die elektronisch über das Internet übertragen (*transportiert*) wird.
- Sie haben einen **Anbieter** (*Firma*), bei dem Sie sich mit persönlichen Daten registrieren (*eintragen*).
- Anbieter nennt man auch **Provider**.
  Bekannte **Anbieter** sind zum Beispiel „web.de“, „gmx.de“, „gmail.com“, „yahoo.de“.
- Sie haben eine **E-Mail-Adresse** für sich gewählt.
- Sie müssen ein Passwort angeben (*nennen*), um Ihren E-Mail-Account (*Konto*) anzusehen.
- Wichtig: Nehmen Sie ein **gutes Passwort**.
  Mehr Informationen zu guten Passwörtern lesen Sie ab Seite 44.

- Bei den meisten Anbietern können Sie **kostenlos** ein E-Mail-Konto einrichten.
- Aber: Meistens bekommen Sie dafür **Werbung** von Ihrem Anbieter.
  Diese Werbung können Sie nicht abmelden.
- Wenn Sie keine Werbung haben wollen, müssen Sie einen kostenpflichtigen Anbieter nehmen, zum Beispiel „posteo.de“, „mail.de“.

- Sie können Ihre E-Mails **verwalten**, mailen und senden über
  - die **Internetseite** von Ihrem Anbieter
  - oder über ein **E-Mail-Programm** wie zum Beispiel „Outlook“, „Thunderbird“, „myMail“, „K9“.
- Welche **Vorteile** hat ein E-Mail-Programm?
  - Ihre E-Mails sind **lokal** auf Ihrem Gerät gespeichert.
  - Sie können **offline** (*ohne Verbindung zum Internet*) E-Mails schreiben und die E-Mails wegschicken, wenn Sie wieder online (*Verbindung zum Internet haben*) sind.
  - Ihr E-Mail-**Adressbuch** ist lokal auf Ihrem Gerät gespeichert.
    Ihr Provider kennt das Adressbuch nicht.
    Das schützt Ihre **Privatsphäre** und die von Ihren Kontakten.
  - Ein E-Mail-Programm ist **sicherer**. – Warum?
    Es ist ein spezielles Programm mit wenigen Funktionen.
    Deshalb ist das Risiko von Sicherheitslücken geringer als bei der Benutzung von einem Internet-Browser (*Programm zum Aufrufen von Internetseiten*).

- Laden (*übertragen*) Sie E-Mail-Programme nur über die Internetseite **vom Original-Anbieter** auf Ihre Geräte.
  Wie Sie diese Internetseiten finden, steht auf der Seite 54.
- Gehen Sie sofort in die **Einstellungen** vom E-Mail-Programm.
  Machen Sie die Einstellungen so, wie Sie es brauchen.
  Wir sagen Ihnen auf den nächsten Seiten, was wichtig ist.
  Die Einstellungen finden Sie im Menü (*Liste von Funktionen*) von Ihrem E-Mail-Programm.
  Oft wird das Menü mit drei Strichen übereinander angezeigt oder mit Punkten nebeneinander.

- Viele **Angriffe** (*Versuche einzudringen*) auf Ihre Privatsphäre und auf Ihre Geräte gehen über E-Mails.

- Blockieren (*verbieten*) Sie in den Einstellungen das Nachladen von externen Bildern und blockieren Sie die HTML-Darstellung (*Zeigen von Bildern in E-Mails*).

- Warum? – Sonst können Rückmeldungen über Ihren Umgang (*wie Sie etwas machen*) mit der E-Mail an den Absender zurückgehen, ohne dass Sie das wissen.
- Oder: es kann auch Schad-Software auf Ihre Geräte übertragen werden.

- Abhängig von Ihrem E-Mail-Provider finden Sie neue Mails oft in diesen Ordnern:
  - im **Posteingang**
  - unter Freunde und Bekannte
  - in Spam (*unerwünschte Mail*) oder in Junk (*Müll-Mail*)

- Im Ordner **Freunde und Bekannte** werden von Ihrem Provider oder Ihrem E-Mail-Programm meistens die E-Mails einsortiert, von denen die Absender-Adressen bekannt sind.
- In der Ordnern **Spam** oder **Junk** werden häufig die E-Mails einsortiert, von denen die Absender-Adressen nicht bekannt sind.
  Spam-Mails und Junk-Mails sind meistens Werbe-Mails oder Phishing-Mails (mehr dazu finden Sie ab Seite 23).
- In welchen Ordner die ankommenden E-Mails sortiert werden, wird durch ein besonderes Programm entschieden. Dieses Programm nennt man **Spam-Filter**.
  Manche Spam-Filter sind gut, manche sind schlecht.
  Deshalb kann man sich nicht auf die Spam-Filter verlassen.

- Sie können selber die **Einstellungen** vom Spam-Filter auf der Internetseite von Ihrem E-Mail-Provider oder in den Einstellungen von Ihrem E-Mail-Programm **ändern**.
  So können Sie selber mit entscheiden, in welche Ordner die ankommenden E-Mails einsortiert werden.
- **Kontrollieren** Sie auch immer wieder den **Spam-Ordner**.
  Oft finden sich im Spam-Ordner interessante und wichtige E-Mails, manchmal auch noch E-Mails von bekannten Absendern.

- Sie bekommen viele **E-Mails**, die Sie gar **nicht** haben **wollen**, zum Beispiel:
  - Werbe-Mails von Ihrem E-Mail-Provider,
  - Newsletter (*Informations-Mail*) von Firmen, bei denen Sie bestellt haben,
  - Werbe-Mails von Firmen, von denen Sie noch nie gehört haben,
  - Phishing-Mails (*Mail für einen Versuch, zu betrügen*)
- Nicht alle diese E-Mails werden in den Spam-Ordner oder Ihren Junk-Ordner einsortiert.
  Nicht alle diese E-Mails sind gefährlich.
- Wenn Sie das Nachladen von Bildern und die HTML-Darstellung abgeschaltet haben, können Sie fast alle E-Mails gefahrlos öffnen und lesen.
- Sie müssen aber **selber genau** hinschauen und **überlegen**, was Sie dann weiter mit Ihren E-Mails tun.

- **Werbe-Mails von** Ihrem **E-Mail-Provider** können Sie meistens nicht abmelden.

- Schauen Sie sich alle E-Mails von Ihrem E-Mail-Provider an.
- Wenn darin nichts zu einer Änderung von Ihrem Vertrag mit dem Provider steht, können Sie die E-Mail löschen.

- **Newsletter** informieren Sie über Produkte von Firmen oder Aktivitäten von Organisationen, mit denen Sie meistens schon einmal Kontakt hatten.

- Wenn Sie etwas auf einer Internetseite **bestellen**, können Sie **ankreuzen**, ob Sie den Newsletter bekommen wollen oder nicht.
- Jeden Newsletter können Sie zu jeder Zeit **abmelden**.
  In jedem Newsletter muss stehen, wie das geht.
  Meistens steht es sehr klein geschrieben kurz vor dem Ende vom Newsletter.
- Melden Sie alle Newsletter ab, die Sie nicht interessieren.

Tipp

- Sie bekommen wahrscheinlich auch **Werbe-E-Mails** von Firmen, zu denen Sie noch keinen Kontakt hatten.

- E-Mail-Adressen werden gerne von Firmen verkauft und gekauft.
  Das dürfen die Firmen, wenn sie keine anderen Daten als die E-Mail-Adressen weitergeben.
- Löschen Sie solche Werbe-E-Mails.
  Wenn es Newsletter sind, melden sie diese ab.

Tipp

- Wahrscheinlich bekommen Sie auch **Phishing-Mails**.

- Mit Phishing-Mails versuchen **Kriminelle**
  - Ihre Passwörter, Ihre **Zugangsdaten** für das Online-Banking oder andere wichtige Konten zu bekommen,
  - von Ihnen über **falsche Rechnungen** Geld zu bekommen,
  - ein **Foto von** Ihrem **Ausweis** zu bekommen, um Ihre Identität für kriminelle Aktivitäten zu benutzen.

- **Phishing-Mails** kommen oft von **unbekannten Absendern**.
- Achtung: **Auch von bekannten Absendern** können Sie Phishing-Mails bekommen, wenn Hacker (*Angreifer*) E-Mail-Konten von Ihren Freunden, Ihren Bekannten oder Ihrer Familie gehackt (*steuern können*) haben.

- Deshalb ist es wichtig: Bitte sind Sie immer **vorsichtig**, vor allem bei E-Mails mit merkwürdigem (*passt nicht zu Ihnen und Ihrer Situation*) Inhalt.
- **Phishing-Mails** können **unterschiedlich** aussehen.
  Zurzeit (*jetzt*) gibt es bestimmte Typen von Phishing-Mails.
  Phishing-Mails, die aussehen wie
  - E-Mails von offiziellen Stellen (*Ämtern, Banken…*),
  - E-Mails von Anwälten,
  - besonders interessante Nachrichten.

  Es wird immer wieder neue Typen geben.

- Denken Sie daran:
  Die Phishing-Mails können **wie offizielle E-Mails** von Banken,
  Paypal, Amazon, Telefon-Anbietern und anderen Firmen aussehen.
- In solchen E-Mails steht:
  Sie sollen Ihre Zugangsdaten an den Absender von der E-Mail zurückschicken oder anrufen.
- **Nennen Sie nie in einer E-Mail oder am Telefon Ihre Zugangsdaten!**
- Keine zuverlässige Bank, keine zuverlässige Firma, kein zuverlässiger Anbieter wird Sie nach Ihren Zugangsdaten fragen.

- **Kontrollieren Sie nie Ihre Konten, indem Sie auf einen Link in einer E-Mail klicken** (*in der Mail geschriebene Internetadresse öffnen*)**.**
  Kontrollieren Sie Ihre Konten, indem Sie sich über die Internetseite der Bank oder der Firma einloggen (*anmelden*).

- Phishing-Mails sehen zum Beispiel aus **wie E-Mails von Anwälten** oder Firmen und fordern Sie auf, sofort eine **Rechnung** zu bezahlen.
  Die Rechnung ist im Anhang.

- Oft steht in dieser E-Mail auch etwas über eine **Mahnung** (*Erinnerung an eine unbezahlte Rechnung*) für eine unbezahlte Rechnung.
- **Öffnen Sie nicht den Anhang**!
  In solchen Anhängen ist häufig Schad-Software (*Programme, die Ihren Geräten schaden*).

- Der Text der E-Mail soll Ihnen Angst machen, damit Sie den Anhang schnell öffnen.
- **Bezahlen Sie nicht! – Überlegen** Sie:
  - Habe ich alle Rechnungen bezahlt?
  - Habe ich eine Rechnung über diesen Betrag oder von dieser Firma bekommen?
  - Habe ich etwas bei dieser Firma bestellt oder gekauf?
  - Habe ich eine Mahnung mit der Post bekommen? Mahnungen werden meistens mit der Post geschickt.

- **Phishing-Mails** können zum Beispiel aussehen wie
  - Werbung für ein ganz **billiges Angebot**,
  - eine Nachricht, dass Sie etwas **gewonnen haben**,
  - ein ganz preiswertes Angebot für einen **Kredit** (*Geld leihen*),
  - eine aktuelle (*neue*) Nachricht über etwas ganz **Interessantes** oder **Tolles**.

- In diesen E-Mails stehen Link-Adressen (*Verbindungen zu Internetseiten*).
- **Klicken Sie nie schnell auf Link-Adressen in E-Mails!**
  
  Oft wird eine zuverlässige Link-Adresse angezeigt.
  Aber: Der Link geht zu einer anderen Internetseite.
  Von dieser Seite aus, wird Ihnen vielleicht Schad-Software auf Ihre Geräte geladen (*übertragen*).
- Der Text soll Sie nur dazu bringen, auf den Link zu klicken.
- **Überlegen** Sie immer erst, ob diese E-Mail von einer zuverlässigen Firma oder einem zuverlässigen Absender kommt.
- Das ist besser:
  Suchen Sie im Internet nach der Firma und sehen Sie sich die Internetseite über Ihren Browser an.

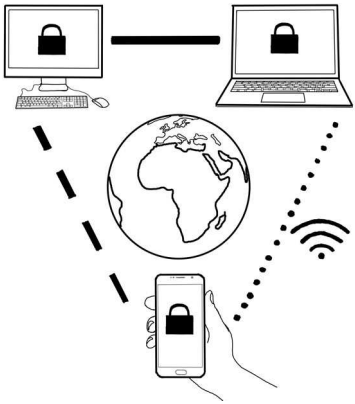
- Das macht Sie **sicherer**:
  - Bitte **nicht** schnell auf **Links** in E-Mails **klicken**.
  - Bitte **nicht** schnell **Anhänge öffnen**.
  - Bitte **immer** erst **überlegen** und **prüfen**, ob der Absender zuverlässig ist.
  - Wenn Sie unsicher sind, ob Ihr **E-Mail-Konto gehackt** wurde, **ändern** Sie Ihr **Passwort**.
    Dann ist Ihr E-Mail-Konto wieder sicher.
    Nicht vergessen:
    Wenn Sie ein E-Mail-Programm benutzen, müssen sie dort auch das neue Passwort eingeben.
  - Denken Sie daran:
    Auch **von bekannten Absendern** können **Phishing-Mails** kommen, wenn die E-Mail-Konten von diesen Personen gehackt wurden.

Tipp

- Gut zu wissen:
  - Die meiste Schad-Software kommt auf Geräte, weil die Benutzer selber nicht aufgepasst und Fehler gemacht haben.
  - Wenn Sie **vorsichtig** sind, **passiert** Ihnen das **nicht** oder nur sehr selten.

- Laden Sie immer sofort alle **Updates** und **Upgrades** von Ihrem E-Mail-Programm herunter.
  Das sind Verbesserungen von einem Programm.
  Nur dann sind sie am sichersten.
  Mehr dazu finden Sie ab Seite 54.

Sicher ins Internet gehen:



- Das **Internet** wird oft auch **Netz** genannt.
- Das Internet ist die **weltweite Verbindung** von elektronischen Geräten.
- Sie brauchen einen Zugang (*Weg*) ins Internet, wenn Sie Ihr Gerät mit dem Internet verbinden wollen.

- Meistens haben Sie mehrere Geräte.
  Diese bilden zusammen ein kleines Netzwerk.
  Das nennt man **LAN** (Lokales Netzwerk), manchmal sagt man auch **Heimnetzwerk**.

- Um Ihr LAN mit dem Internet zu verbinden, brauchen Sie ein besonderes Gerät: einen **Router**.
- Die Fachleute sagen auch: Der Router **koppelt** (*verbindet*) Ihr Heimnetzwerk mit dem Internet.

- Es gibt zwei Möglichkeiten, Ihre **Geräte mit** dem **Router** zu **verbinden**:
  - Sie benutzen ein Kabel zwischen Router und Ihrem Gerät. Dieses Kabel nennt man **LAN-Kabel**.
  - Sie benutzen WLAN. **WLAN** ist eine Funk-Verbindung (*Übertragung ohne Kabel*) zwischen dem Router und Ihrem Gerät.

- Hat eine Person **Zugriff** (*kann steuern*) **auf ein Gerät** in Ihrem Heimnetzwerk, hat sie meistens auch **Zugriff auf alle Geräte**, die mit Ihrem Heimnetzwerk verbunden sind.
- **Sichern** Sie Ihren **Zugang** ins Internet:
  - Machen Sie Ihren Router sicherer.
  - Sichern Sie Ihr WLAN ab. Es gibt Gesetze, dass Sie das machen müssen.

- Gehen Sie in die **Einstellungen** von Ihrem Router und bearbeiten Sie die Punkte, die wir auf den nächsten Seiten für Sie aufgeschrieben haben.
  Die Einstellungen finden Sie im Menü von Ihrem Router.
  Das Menü ist die Liste von Funktionen.
  Oft hat der Router eine Internetseite, die Sie mit dem Browser ansehen können.
  Dort finden Sie die Einstellungen.

- **Ändern** Sie das **Passwort** von Ihrem Router, wenn es noch das Passwort vom Hersteller (*Firma, die etwas gemacht hat*) ist.
- Warum? – Sonst (*wenn Sie das nicht machen*) kann jeder, der die Passwörter der Firmen kennt, auf Ihren Router und auf Ihre Geräte zugreifen (*eindringen*).
- Nehmen Sie ein **gutes Passwort**.
  Mehr zu guten Passwörtern finden Sie ab Seite 44.
- **Deaktivieren** Sie **WPS**.
  WPS ist eine Funktion, um aus Geräten ein Netzwerk zu bilden.
  Sie ist nicht sicher.
- **Deaktivieren** Sie **UPNP**.
  Über UPNP kann eine andere Person von außen über Ihren Router auf Ihr Netzwerk zugreifen.
- Sie müssen Ihr **WLAN verschlüsseln** (*so verändern, dass es niemand anderes lesen kann*).
  Dazu wählen Sie eine aktuelle Verschlüsselung.
  Das ist zurzeit (*jetzt*) **WPA2**. – Bald wird es **WPA3** geben.
  Dann benutzen Sie bitte diese neue Verschlüsselung.

- Warum? – Sonst können Personen in Ihrer Nachbarschaft oder auf der Straße über Ihr unverschlüsseltes WLAN und Ihren Internetzugang ins Internet gehen.
- Diese Personen können sogar kriminelle oder terroristische Aktivitäten über Ihr WLAN organisieren.
  Das kann Ihnen große Probleme bereiten (*machen*).
  Deshalb müssen Sie verschlüsseln.
  Das steht in unseren Gesetzen.
- Sichern Sie auch den Zugriff aus dem **Heimnetzwerk** auf Ihren Router durch ein gutes **Passwort**.

- Spielen (*übertragen*) Sie immer **sofort alle Updates** von Ihrer Router-Software auf Ihrem Router.
  Das sind Verbesserungen von einem Programm.
  Nur dann ist er so **sicher**, wie es geht.
  Mehr dazu finden Sie auf der Seite 54.

- Geben Sie Gästen nur über Ihr Gast-WLAN Zugang zu Ihrem Netzwerk.
- Schalten Sie Ihr **Gast-WLAN** nur an, wenn es benutzt werden soll und danach wieder aus.
  Dann ist das Risiko einer Benutzung durch fremde Personen geringer.
- Nehmen Sie für das **Gast-WLAN** ein **eigenes Passwort**.
  Warum? – Wenn Geräte von Ihrem Gast gehackt wurden, hat ein Hacker (*Angreifer*) sonst auch auf Ihr WLAN Zugriff.
- **Überlegen** Sie bitte auch, wem Sie Zugang zu Ihrem Gast-WLAN geben.
  Ist Ihr Gast zuverlässig und haben Sie Vertrauen in ihn?

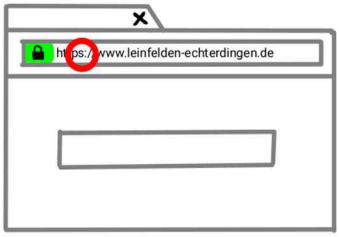
- **Öffentliches WLAN** ist **nicht** so **sicher** wie ihr WLAN zuhause.
  Für geübte Personen ist es ganz leicht,
  - alle Ihre Aktivitäten im Internet zu lesen und zu sehen
  - Ihre Passwörter und andere Zugangsdaten zu bekommen.
- **WLAN in Hotels** kann unsicher oder sicher sein.
- **Nutzen** Sie öffentliches WLAN und WLAN von Hotels:
  - nur für **unwichtige** Alltags-Kommunikation,
  - nur zum Ansehen von **verschlüsselten Internetseiten** (mehr dazu finden Sie auf der Seite 40),
  - **nicht für Online-Banking**,
  - **nicht für die Kommunikation von privaten Daten und Gesundheits-Daten.**

Tipp

Tipp

- Schalten Sie das **WLAN** an Ihren Geräten **aus**, wenn Sie mit Ihren Geräten **unterwegs** (*nicht zuhause*) sind.
- Schalten Sie es erst wieder an, wenn Sie wirklich mit WLAN ins Internet gehen wollen.
- Warum? – Wenn das WLAN eingeschaltet ist und Ihr Gerät kein WLAN hat, sucht es automatisch nach einem WLAN. Wenn es ein offenes (*nicht verschlüsselt*) WLAN findet, verbindet sich Ihr Gerät automatisch mit diesen offenen WLAN.
- Manche Hacker haben ein offenes WLAN.
  Sie warten auf ein Gerät, dass sich in ihr offenes WLAN einbucht (*eine Verbindung herstellt*).
  Dann suchen die Hacker mit speziellen Programmen nach Sicherheitslücken auf dem Gerät, um schädliche Programme aufzuspielen (*zu übertragen*).
- Ist ihr WLAN aus, kann so etwas nicht passieren.
  Und: Ihr Akku hält länger, weil das Gerät weniger Energie braucht.

Sicherer und privater im Internet



- Zum Surfen (*Seiten im Internet anzusehen*), brauchen Sie ein spezielles Programm.
  So ein Programm heißt **Web-Browser** oder kurz **Browser**.
- Es gibt verschiedene Browser, zum Beispiel „Mozilla Firefox“, „Safari”, „Google Chrome”, „Microsoft Edge”, „Opera”, auf älteren Geräten auch den „Internet Explorer“.

- Ein Browser stellt (*zeigt*) die Internetseiten auf Ihrem Gerät dar.
- **Internetseiten** nennt man auch **Webseiten** oder **Homepages**.

- Informieren Sie sich genau, welcher Browser zu Ihnen passt.
- Informationen zu Browsern finden Sie, wenn Sie in Ihre Suchmaschine (*Programm zur Suche im Internet*) die Frage eingeben (*schreiben*): „Welche Browser sind sicher“.

- **Browser** sind das bevorzugte (*am meisten genommen*) **Ziel von Hackern** (*Angreifer*).
- Hacker versuchen meist, **Sicherheitslücken** in Browsern zu finden, die sehr viele Nutzer haben.
- Denn: Haben die Hacker eine Sicherheitslücke gefunden, können sie sehr viele Nutzer angreifen (*eindringen und steuern*).
- Deshalb überlegen Sie:
  Ist es gut, einen viel benutzen Browser zu nehmen?

- **Laden** (*auf Ihr Gerät übertrag*) Sie Browser nur **von** den **Original-Internetseiten** der Anbieter herunter.
  Die Original-Seiten finden Sie mithilfe Ihrer Suchmaschine.

- Gehen Sie sofort in die **Einstellungen** des Browsers.
  Die Einstellungen finden Sie im Menü von Ihrem Browser.
  Das Menü ist die Liste von Funktionen.
  Oft wird das Menü mit drei Strichen übereinander angezeigt oder mit Punkten nebeneinander.
- **Wählen** Sie die Einstellungen so, wie es zu Ihnen passt.
- **Überprüfen** Sie alle **Berechtigungen** (*was jemand darf*).
- Nehmen Sie sich die Zeit, alle Einstellungen zu lesen und genau zu **überlegen**, was für Sie richtig ist.

- Wir können Ihnen nur Informationen und ein paar Tipps geben.
  Sie müssen selber entscheiden, was Sie brauchen und was Sie **deaktivieren** (*ausschalten*), um möglichst sicher und privat im Internet zu sein.

- Überlegen Sie genau, ob das **Mikrofon** und die **Kamera** von Programmen über Internetseiten eingeschaltet werden dürfen.

  Schad-Software schaltet manchmal das Mikrofon und die Kamera an.
  So können anderen Personen Sie über Ihre Geräte abhören (*alles hören*) und beobachten.

- Stellen Sie Ihren Browser so ein, dass **Zugangsdaten** und Passwörter für viel besuchte Internetseiten **nicht** automatisch **gespeichert** werden.

- Das ist für Sie unbequem, weil Sie jedes Mal Ihre Zugangsdaten und Passwörter neu eintippen müssen.
  Aber es ist **sicherer**.

- Überlegen Sie, ob der Browser Informationen über Ihren **Standort weitergeben** darf.

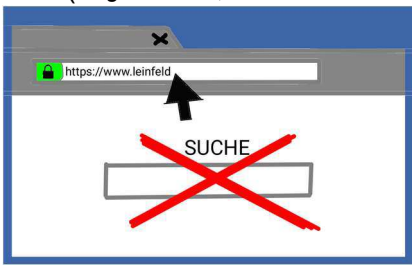
- Sie können die Weitergabe von Ihrem Standort auf dem Smartphone und auf Ihrem PC anders einstellen.
  Oft braucht man am PC keine Weitergabe vom Standort.
- Sie können meistens auch **einstellen**, dass Sie jedes Mal **gefragt** werden, ob bestimmte Informationen weitergegeben werden dürfen.
  Dann können Sie dies ablehnen oder zulassen, wie Sie es in der Situation wollen oder brauchen.

- Erlauben Sie Programmen **nur** den Zugriff auf den Dienst für **Barriere-Freiheit**, **wenn** Sie **eingeschränkt** (*behindert*) sind und diesen Dienst wirklich brauchen.

- Schalten Sie das **Blockieren** (*verbieten*) **von gefährlichen und betrügerischen Inhalten ein**.

- **Popup-Fenster** sind Fenster, die plötzlich auf Ihrem auftauchen (*gezeigt werden*).
- Oft zeigen die Popup-Fenster Werbung und Sie müssen die Fenster wegklicken (*schließen*), wenn Sie die Internetseite richtig ansehen wollen.
- Popup-Fenster können aber auch **Informationen** enthalten, die interessant für Sie sind.
- Stellen Sie Ihren Browser so ein, dass Sie jedes Mal gefragt werden und **entscheiden** können, ob Sie das Popup-Fenster schließen oder offen lassen.

- Am besten stellen Sie Ihren Browser so ein, dass er eine **leere Seite** zeigt,
  - wenn Sie ihn öffnen
  - oder wenn Sie einen neuen Tab (*Registerkarte, neue leere Seite*) öffnen.
- Dann geben Sie automatisch die **Adresse** der von Ihnen gewünschten Internetseite **oben in** das **Adressfeld** von Ihrem Browser ein.



- Viele Nutzer haben Ihren Browser so eingestellt, dass sich sofort die Seite der Google-Suche öffnet.
  - Die Nutzer geben die Internet-Adressen von den Seiten, die sie ansehen wollen, in das große Suchfeld der Google-Suche ein.

- Dann verfolgt (*mitschreiben und speichern*) Google genau,
  - welche Internetseiten Sie aufrufen,
  - welche Unterseiten Sie wie lange ansehen
  - welche Bestellungen Sie aufgeben (*machen*).

  Wollen Sie das wirklich?

- **Suchmaschinen** sind Programme, die auf Internetseiten nach den Wörtern suchen, die Sie eingeben (*in das Suchfeld schreiben*).
  In ganz kurzer Zeit bekommen Sie die Seiten angezeigt, in denen diese Wörter vorkommen (*sind*).

- Überlegen Sie sich, welche Suchmaschine Sie benutzen wollen.

- Die meisten Nutzer nehmen Google.
  Gut zu wissen: **Google** verfolgt alle Ihre Aktivitäten im Internet und speichert diese **Informationen**, um Ihnen genau passende **Werbung** zu schicken.
  Google verkauft diese Informationen auch an andere Firmen.
  Ihre Suche mit Google bleibt nicht privat.

- Es gibt **andere Suchmaschinen**, die Ihre **Aktivitäten nicht verfolgen**.
  Bei diesen Suchmaschinen bleibt Ihre Suche **privat**.
- Solche Suchmaschinen sind zum Beispiel (*heißen*):
  - Metager,
  - Duckduckgo,
  - Startpage.

- Probieren Sie eine andere Suchmaschine.
  Vielleicht bekommen Sie auch mit so einer Suchmaschine gute Ergebnisse.
- Welche Suchmaschine Sie am häufigsten benutzen wollen, können Sie in Ihrem Browser einstellen.

- Wenn mehrere Personen ein Gerät benutzen oder eine andere Person Zugriff auf Ihre Geräte hat:
  Diese Personen können sehen, welche Internetseiten Sie angesehen haben.
  Es bleibt dann nicht privat, auf welchen Seiten Sie waren.

- **Überlegen** Sie:
  Wollen Sie das oder wollen Sie **privat surfen**?
  Das heißt:
  Niemand kann sehen, auf welchen Internetseiten Sie waren.

- Wenn Sie ganz privat surfen wollen, können Sie die Einstellungen von Ihrem Browser ändern.
  Suchen Sie in den Einstellungen nach Funktionen mit diesen Namen:
  - Schalten Sie die Funktion „**Do not track**“ (*nicht aufschreiben*) **ein**.
  - Schalten Sie den „**Schutz vor Aktivitätenverfolgung**“ **ein**.
  - Stellen Sie ein, dass alle **Cookies** (*lesen Sie bitte weiter*) beim Schließen vom Browser **gelöscht** werden.

Tipp

- **Cookies** sind Daten, die beim Ansehen von Internetseiten von den Anbietern der Internetseiten auf Ihre Geräte geladen (*übertragen*) werden.

- Cookies speichern **Informationen über Sie.**
  Das kann der Anbieter der Internetseite später lesen.
  Cookies bekommen Sie fast von jeder Internetseite.
  Oft können Sie die Internetseite nicht richtig ansehen und benutzen, wenn Sie den Cookies nicht zustimmen (*ja sagen*).
- Die Cookies werden jedes Mal **wieder aktiv**,
  wenn Sie die Internetseite wieder öffnen.

- Zum Schutz Ihrer **Privatsphäre** ist es besser, wenn die **Cookies** beim Schließen vom Browser **gelöscht** werden.

- Zum Schutz Ihrer Privatsphäre können Sie in Ihrem Browser auch noch diese Funktionen einstellen:
  - **privates Surfen** *(der Name der Internetseite, die Sie ansehen, wird nicht gespeichert)***,**
  - **löschen der Chronik** (*Geschichte; welche Internetseiten, Sie sich angesehen haben*).

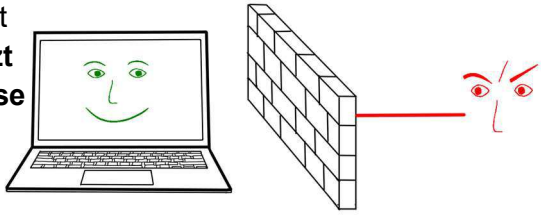
  Dann wird beim Schließen vom Browser gelöscht, welche Internetseiten Sie sich angesehen haben.

Tipp

- Sie möchten vielleicht bestimmte Seiten immer wieder ansehen und finden deshalb die Chronik praktisch.
- Dafür gibt es eine andere Lösung:
  Machen Sie **Lesezeichen** für Internetseiten, die Sie oft besuchen.
  Lesezeichen können Sie in jedem Browser machen.
  Informieren Sie sich, wie das bei Ihrem Browser geht.
  Diese Informationen finden Sie in den Hilfe-Seiten von Ihrem Browser.

Tipp

- Eine **Firewall** (*Brand-Schutz-Mauer*) ist Software und **schützt** Ihr **Netzwerk zuhause** und Ihre Geräte vor Zugriffen aus dem Internet.



- Eine Firewall arbeitet wie ein **Filter**, der nur gewünschte Daten von außen in Ihr Netzwerk und auf Ihre Geräte lässt.

- **Virenscanner** sind Software, die aktiv auf Ihren Geräten nach Bedrohungen (*Gefahren*) suchen.
- Solche Bedrohungen sind **Viren**, **Würmer** und **Trojaner**.
  Mehr dazu können Sie auf der Seite 4 lesen.
- Virenscanner können Viren, Würmer und Trojaner **erkennen**, **blockieren** und oft auch **unschädlich machen**.
- Virenscanner werden bei bestimmten Funktionen Ihrer Geräte automatisch aktiviert.
  Zum Beispiel wenn Sie etwas aus dem Internet herunterladen oder den Anhang von einer E-Mail speichern.
- Viele Betriebssysteme enthalten (*haben*) eine Firewall und Virenscanner.
  Mehr zu Betriebssystemen finden Sie auf der Seite 53.
- Jeder Anbieter hat ein Interesse daran, dass sein Betriebssystem sicher ist.
  Deshalb verbessert der Anbieter die Sicherheit ständig durch **Sicherheits-Updates**.
  Laden Sie deshalb immer alle Sicherheits-Updates sofort herunter.

- Brauchen Sie eine **zusätzliche Firewall** und **zusätzliche Virenscanner**?
- **Überlegen** Sie:

  - Was mache ich mit meinen Geräten?
  - Sind auf meinen Geräten Daten, die besonders geschützt werden müssen?
- Gut zu wissen:

  - Nicht jeder Virenscanner macht Ihre Geräte sicherer.
  - Virenscanner können auch selber Sicherheitslücken oder sogar Viren enthalten.

- Manche Virenscanner blockieren auch das Herunterladen von unschädlicher Software, manchmal sogar von Sicherheits-Updates.
- **Informieren** Sie sich genau, bevor Sie Virenscanner auf Ihren Geräten installieren (*einrichten, überspielen*).
- Informationen finden Sie, wenn Sie in Ihre Suchmaschine „BSI Virenschutzprogramme“ eingeben.

- Für Ihren Browser können Sie auch kleine **Zusatzprogramme** aktivieren oder herunterladen.
- Ein solches Zusatzprogramm heißt **Erweiterung** oder auch **Add-on**.
- Laden Sie Add-ons nur über den **Store** von Ihrem **Browser** herunter.
  Den Store finden Sie meist in den Einstellungen unter dem Namen „Add-on“.
- Achtung:
  Schalten Sie in den Einstellungen von Ihrem Browser **ein**: **Warnung vor** dem **Installieren von Add-ons** durch Internetseiten auf Ihre Geräte.
  Dann kann keine Person von außen Ihnen unerwünschte Add-ons auf Ihren Geräten installieren (*aufspielen, speichern*).

- Eine Gruppe von Add-ons nennt man auch **Plug-ins**.
- Ein Plug-in unterstützt (*hilft*) bei der Darstellung (*Zeigen*) von Internetseiten.
- Es gibt Plug-ins, die nicht sicher sind,
  zum Beispiel „Java“ und „Flash Player“.
  Java und Flash Player sind veraltet (*zu alt*).
  Deshalb gibt es keine Sicherheits-Updates mehr für diese Programme.

- Viele Angriffe von Hackern gehen über diese Plug-ins, weil sie bei einem offenen Browser immer aktiv sind.
- **Überlegen** Sie:
  Für welche Internetseiten brauche ich diese Plug-ins?

- Sie können diese Plug-ins
  - nur für bestimmte Internetseiten aktivieren,
  - komplett deaktivieren,
  - sich immer fragen lassen, ob die Plug-ins aktiv sein sollen.

Tipp

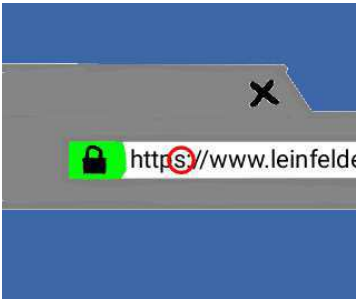
- So sind Sie sicherer:
  Aktivieren Sie die Plug-ins nur, wenn Sie sie wirklich brauchen.

- Sehen Sie sich **nur** Internetseiten an, die eine **Adresse mit https** am Anfang haben.

- Die Kommunikation Ihrer Geräte mit einer https-Seite ist **verschlüsselt**.
- Das heißt: Ein anderes Gerät kann Ihre Kommunikation mit einer https-Seite nicht mitlesen.
- Bitte **nicht** mit http **verwechseln**.
  Das kleine „**s**“ macht einen großen Unterschied!

!

- Die Kommunikation mit einer http-Seite ist nicht verschlüsselt und kann von anderen Geräten mitgelesen werden.
- Achten Sie auf das **kleine Schloss** in der Adress-Zeile von Ihrem Browser.
- Achtung: Das Schloss muss so aussehen, wie auf dem Bild. Sonst könnten Sie auf einer gefälschten Internetseite sein, die nur aussieht wie die echte Seite.



!

- **Schauen** Sie sich beim Aufrufen (*öffnen*) von wichtigen Internetseiten **immer** genau die **Adresse**, das **https** und das **Schloss-Symbol an**, zum Beispiel von ihrer Bank.
  Dann erkennen Sie sofort den Unterschied, wenn Sie auf einer gefälschten Internetseite sind.

Tipp

- Wenn Sie denken, dass Sie vielleicht auf einer gefälschten Internetseite sind:
  Schließen Sie die **Internetseite** sofort und auch Ihren **Browser**.

- Achtung: Wenn Ihr Browser Ihnen einen **Zertifikatsfehler** anzeigt, **öffnen** Sie diese Internetseite **nicht**.
  Es kann eine gefälschte oder unsichere Internetseite sein.

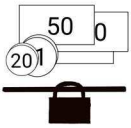
- Laden Sie immer **sofort Sicherheits-Updates** für Ihren Browser herunter.

- Mit jedem Update werden Sicherheitslücken geschlossen.
  Dann arbeiten Sie immer mit der sichersten Version (*Ausgabe, Form*) von Ihrem Browser.

- Wenn sich **Fenster** beim Ansehen einer Internetseite öffnen:
  - **Lesen** Sie, was in dem Fenster steht.
  - **Überlegen** Sie, **was** Sie **erlauben** wollen oder nicht.
  - Schließen Sie nie das Fenster, ohne es zu lesen.

- **Erlauben** Sie **möglichst wenig**.
  Dann gehen nur wenige Informationen von Ihnen an die Anbieter.
  So schützen Sie Ihre Privatsphäre.

Tipp



- Beim **Online-Banking** sollten Sie **besonders vorsichtig** sein.
- Banking über die **Internetseite** von Ihrer Bank ist **sicherer** als über eine App auf Ihrem Smartphone.
- Benutzen Sie **zwei Geräte** für Ihr Banking. Dann müsste ein Hacker beide Geräte hacken, um an die Zugangsdaten für Ihre Bank zu kommen.

- Wenn Sie nur ein Gerät haben, benutzen Sie einen Tan-Generator (*Erzeuger von Tans*) als zweites Gerät. Einen Tan-Generator bekommen Sie zum Beispiel bei Ihrer Bank.

Tipp

- **Löschen** Sie vorm Online-Banking alle **Cookies**. Die Cookies könnten sonst wichtige Daten von Ihrem Online-Banking an Anbieter von anderen Internetseiten weitergeben.

- Stellen Sie Ihren Browser auf **privates Surfen**.
- **Schließen** Sie **alle anderen Internetseiten**, bevor Sie die Seite von Ihrer Bank öffnen.

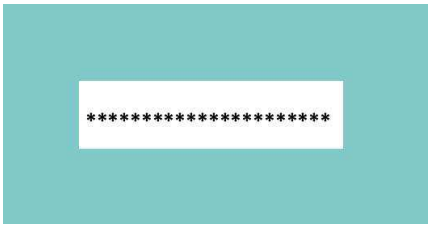
- Am sichersten ist es, wenn Sie beim Banking **nur die Internetseite** Ihrer **Bank offen** haben. Dann können keine Daten über Ihr Banking an andere Personen gesendet werden.
- **Achten** Sie **immer** darauf, dass vor der Adresse von Ihrer Bank **https** steht.

- Achten Sie **immer** auf das **Schloss-Symbol** in der Adresszeile von Ihrem Browser.

- Fahren Sie öfter mit dem Cursor (*Pfeil*) über das Schloss-Symbol.
  Dann können Sie lesen, wer die Sicherheit der Internetseite **zertifiziert** (*beglaubigt*) hat.
  Schreiben Sie sich den Namen auf.
  Dann haben Sie einen Vergleich, wenn Sie unsicher sind, ob die Internetseite vielleicht gefälscht ist.

Tipp

Schützen Sie Ihre Geräte und Konten mit einem guten Passwort:



- **Passwort** und **Kennwort** sind das Gleiche:
  Der Nutzer muss es zum Anmelden eingeben.
  Das Passwort **entsperrt** (*den Zugang öffnen*)
  ein elektronisches Gerät oder eine Funktion.
- **Ohne Passwort** kann jeder **alles** von Ihrem Gerät **lesen**, wenn er Ihr Gerät hat.
- Jeder kann auf Ihre Kosten mit Ihrem Smartphone **telefonieren**.
- Jeder kann **schädliche Programme** auf Ihrem Gerät Installieren (*aufspielen, einrichten*).

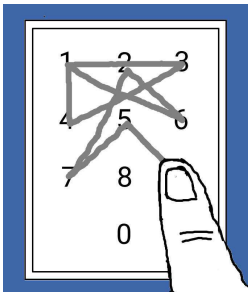
- **Gute Passwörter** bestehen (*sind*) aus **Buchstaben**, **Zahlen** und besonderen **Zeichen** zum Beispiel: § $ % (/ ? !.

- Gute Passwörter sind **lang**.
- So machen Sie selber ein gutes Passwort:

  - Sie denken sich einen Satz aus.
  - Dieser Satz sollte lang sein, zum Beispiel: „Abends laufe ich jeden Tag 30 Minuten und trinke ein Glas Wasser“
  - Sie nehmen von jedem Wort den Anfangsbuchstaben: „AlijT30MuteGW“
  - Jetzt nehmen Sie einige Sonderzeichen und Zahlen für ein paar (*wenige*) Buchstaben, zum Beispiel: „Al1!T30M&t1GW“
  - Fertig ist ein gutes Passwort.

- **Schlechte Passwörter** sind zum Beispiel:
  - 1,2,3,4,5,6
  - Passwort, Hallo, Tag
  - Geburtstage und Namen aus Ihrer Familie

- Auch **Wischzeichen** Können ein Passwort sein.
- Einfache Wischzeichen sind schlechte Passwörter, zum Beispiel Z oder ein Rechteck.



- Besser ist ein **kompliziertes** Wischzeichen.

- Manche Geräte können Sie auch mit **biometrischen Daten** entsperren.
- Biometrische Daten sind zum Beispiel: Fingerabdrücke, das Gesicht, das Auge.
- Aber: Die biometrischen Daten sind nicht so sicher wie ein gutes Passwort.
  Manchmal funktionieren die biometrischen Daten nicht, zum Beispiel, weil die Finger schmutzig sind.

- Wenn **mehrere Personen** in Ihrer Familie ein Gerät benutzen, sollten auch alle das Passwort kennen.
- Ein Fremder kann das Gerät dann nicht benutzen.

- Benutzen Sie für **jedes Gerät** ein **eigenes Passwort**.
- Benutzen Sie für **jeden Login** (*Anmeldung für ein Benutzerkonto*), für jeden Account (*Benutzerkonto*) und für Ihr Online-Banking ein **anderes Passwort**.
- Wenn Sie **verschiedene Passwörter** haben:
  Kennt eine andere Person ein Passwort von Ihnen, kann sie **nur ein Gerät oder einen Dienst oder ein Konto** von Ihnen benutzen.
  Der **Schaden** bleibt **klein**.

- Wenn Sie nur **ein Passwort für alle** Geräte und alle Logins haben:
  Eine andere Person kann **alles benutzen**, wenn sie Ihr Passwort kennt.
  Der **Schaden** kann **groß** werden.

- Sie sagen vielleicht:
  So viele Passwörter kann ich mir nicht ausdenken.
  Und: So viele Passwörter kann ich mir nicht merken.
  Wir sagen: Wir können das auch nicht.

- **Benutzen Sie einen Passwort-Manager**.

Tipp

- Ein **Passwort-Manager** ist ein besonderes Programm.
  Die meisten Passwort-Manager können gute **Passwörter erzeugen** (*machen*).
  Alle Passwort-Manager können die Logins und die passenden Passwörter **verschlüsselt** (*nicht direkt zu lesen*) **speichern**.
  Ein Passwort-Manager ist also ein Generator (*Erzeuger*) und ein Tresor (*sicherer Schrank*) für Ihre Passwörter.

- Ihren Passwort-Manager sichern Sie mit einem guten Passwort.
  Sie brauchen sich nur noch ein Passwort zu merken:
  das Passwort für Ihren Passwort-Manager.
  Das ist **leicht** und bequem.
- Ein Passwort-Manager ist **sicher**. – Warum?
  - Wenn jemand Ihr Gerät stiehlt oder Zugriff auf Ihr Gerät hat, kann er den Passwort-Manager nicht lesen.
  - Denn: Alles darin ist verschlüsselt.
    Und: Man braucht das Passwort für den Passwort-Manager.
  - Der **Schaden** bleibt **klein**.
- Passwort-Manager gibt es für
  - Smartphones, Tablets, Laptops, Computer, PCs
  - alle Betriebssysteme
- Informationen zu Passwort-Managern finden Sie beim BSI (*Bundesamt für Sicherheit in der IT-Technik*).
  Geben (*schreiben*) Sie in Ihre Suchmaschine die Wörter „BSI Passwort-Manager“ ein.
  Zurzeit (*jetzt*) ist „keypass“ ein guter Passwort-Manager, sagt das BSI.
  Mehr Informationen finden Sie unter https://keepass.info/

- Sie sagen vielleicht:
  Ich möchte keinen Passwort-Manager benutzen.
- Wir geben Ihnen Tipps, was Sie dann tun können.
- Wir sagen aber auch:
  Ein Passwort-Manager ist sicherer.

- Wenn Sie keinen Passwort-Manager benutzen wollen:
  - Machen Sie sich ein gutes Passwort.
    Wir nennen es: das **Master-Passwort**.

  - Setzen Sie vor dieses Master-Passwort **für jeden Login** andere wenige **Zahlen, Buchstaben oder Sonderzeichen** und hängen Sie noch welche an das Master-Passwort an.
  - Dann haben Sie für jeden Login ein eigenes gutes Passwort.
  - Ihre Passwörter und Logins **notieren** Sie auf einen Zettel.

  - Den Zettel legen Sie an einen **Platz**, an dem eine fremde Person den Zettel **nicht leicht finden** kann.
  - Legen Sie den Zettel mit den Passwörtern **nicht neben den PC oder in eine Schublade** von ihrem Schreibtisch.
  - **Kleben** Sie das Passwort für Ihr Gerät **nicht an das Gerät**.

- **Loggen** (*abmelden*) Sie sich immer **aus**, wenn Sie auf einer Homepage oder mit Ihrem Online-Banking fertig sind.
  Wenn Sie angemeldet bleiben, hat jede Person Zugriff auf Ihre Konten, wenn Sie Zugriff auf Ihr Gerät hat.

- **Ändern** Sie sofort alle **Passwörter von neuen Geräten**.
  Personen, die die Passwörter von Herstellern (*Firmen*) der neuen Geräte kennen, können sonst auf Ihr Gerät zugreifen.

- **Ändern** Sie ab und zu Ihre Passwörter, **mindestens einmal im Jahr**.
  Wenn jemand Ihr Passwort kennt und Sie es ändern, kann diese Person sich nicht mehr bei Ihren Logins anmelden.

- Loggen Sie sich auf Internetseiten **immer direkt über** das **Login** dieser Seite ein.
  Loggen Sie sich **nicht über andere** Dienste oder Internetseiten ein, zum Beispiel über „Facebook“, „Amazon“, „Paypal“, und „Google“.
  Diese Firmen lesen dann alles mit.
  Die Firmen kennen dann Ihre Konten von anderen Anbietern und schicken Ihnen noch mehr Werbung oder sie verkaufen Informationen über sie.
  Und: Wenn Ihr Zugang zu diesen Firmen gehackt wird, hat der Hacker auch Zugriff auf Ihre Konten bei den anderen Anbietern.

- Geben Sie **nie** Ihre Passwörter **in Mails** oder **am Telefon** anderen Personen.
  Seriöse (*zuverlässige, vertrauenswürdige*) Firmen und Banken fragen nie nach Ihren Passwörtern oder Zugangsdaten.
  Das machen nur Betrüger (*jemand, der auf Ihre Kosten Vorteile haben will*).

- Für wichtige Logins gibt es etwas Sichereres als ein Passwort: die **Zwei-Faktor-Authentifizierung** (*Ausweisen in 2 Schritten*).

- Wie geht das? – Ein Beispiel:
  - Sie melden sich mit Ihren **Zugangsdaten** über eine Internetseite an.
  - Sie bekommen eine SMS auf ihr Handy mit einem **Code** (*geheimes Wort oder geheime Zahlenkombination*).
  - Diesen Code müssen Sie auch auf der Internetseite eingeben.
  - Erst dann sind Sie richtig authentifiziert (*ausgewiesen*).
- Für die Zwei-Faktor-Authentifizierung sollten Sie zwei **unterschiedliche Geräte** benutzen.

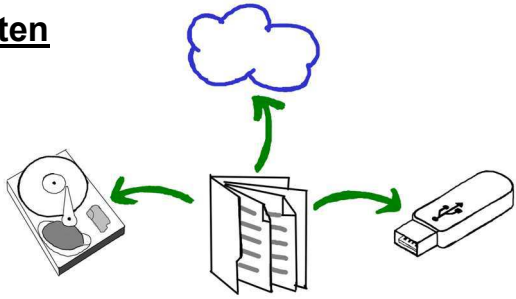
- Warum? – Wenn Sie nur ein Gerät benutzen und dieses Gerät gehackt wurde, kann der Hacker beide Schritte der Authentifizierung beobachten.
  Er kann dann Ihre Authentifizierung für seine Aktivitäten benutzen.
- Achten Sie beim Online-Banking und anderen wichtigen Logins auf eine Zwei-Faktor-Authentifizierung.
- Wenn eine Zwei-Faktor-Authentifizierung möglich ist, nutzen Sie diese.

- Beim Einrichten von einem neuen Konto stellen manche Anbieter **Sicherheitsabfragen**.

- Sie müssen die Sicherheitsabfrage richtig beantworten, wenn Sie Ihre Zugangsdaten vergessen haben.
  Nur so können Sie sich dann authentifizieren.
- Bei den Sicherheitsabfragen müssen Sie eine Frage aussuchen.
- Suchen Sie eine Frage aus, die nur Sie richtig beantworten können, zum Beispiel Ihre Lieblingspflanze oder Ihr Lieblingstier.

- **Notieren** Sie sich die **Frage** und die **Antwort**.

Backup Ihrer Daten



- Ein Backup ist eine **Sicherungskopie**.
- **Ohne Backup können alle Ihre Daten weg sein**,
  - wenn Ihr Gerät kaputt geht,
  - wenn Ihr Gerät gestohlen wird,
  - wenn ein Hacker (*Angreifer*) Ihre Daten verschlüsselt (*unlesbar macht*)
  - oder Sie durch einen Fehler selber Ihre Daten löschen. Das kann passieren.

  Dann sind auch alle Ihre Fotos weg.
- **Sichern** Sie Ihre Daten **regelmäßig** auf:
  - einen USB-Stick,
  - auf eine externe (*nicht in Ihrem Gerät*) Festplatte (*elektronisches Bauteil zum Speichern von Daten*),
  - vielleicht auch in eine Cloud (*Speicher von einem Anbieter*), mehr zur Cloud können Sie auf der Seite 52 lesen.
- **Kontrollieren** Sie nach der Sicherung, ob die Daten auch wirklich gesichert wurden.
- Sichern Sie auch die **Daten von** Ihrem **Smartphone**. Wie geht das?
  - Überspielen Sie Daten von Ihrem Smartphone auf Ihren PC und sichern Sie die Daten dann von Ihrem PC aus.
  - Oder: Kaufen Sie sich einen Adapter (*Verbindungsstück*) und sichern Sie Ihre Daten über den Adapter auf einen USB-Stick.

- Wirklich **gut gesichert** sind Ihre Daten nur,
  - wenn Sie regelmäßig **3 Kopien** von Ihren Daten machen,
  - wenn Sie 2 Kopien bei sich zuhause und 1 Kopie woanders haben, zum Beispiel bei einem guten Freund (einer guten Freundin).

  Dann ist alles in Ordnung auch,
  - wenn eine Kopie nicht mehr funktioniert,
  - wenn bei Ihnen zuhause mal etwas Schlimmes passiert und Ihre Sicherungskopien zerstört (*kaputt gemacht*) werden.

- Achtung: Ihr **Backup** darf nach der Sicherung **keine Verbindung zu anderen Geräten** mehr haben. Sonst könnten Ihre Backups auch durch Schad-Software angegriffen werden und sind dann unbrauchbar.

- **Machen Sie für Ihren PC eine Sicherungskopie zur Wiederherstellung Ihres Betriebssystems.** Sonst können Sie Ihren PC im Notfall nicht wieder neu einrichten und er ist dann erst einmal unbrauchbar.

- Machen Sie diese Sicherungskopie auf einen **Stick** oder eine **DVD** (*digitaler Datenspeicher*).
- **Lagern** Sie die Sicherungskopie **ohne Verbindung** zu anderen Geräten.

- Wie man eine Sicherungskopie macht, steht in der Bedienungsanleitung von Ihrem PC.

- Über fremde **USB-Sticks** kann **Schad-Software** auf Ihre Geräte kommen.
- **Stecken** Sie **nur** USB-Sticks **von zuverlässigen Personen** in Ihre Geräte.

- Heute bekommen Sie oft **wichtige Verträge** nur noch in elektronischer Form.
- **Drucken** Sie wichtige Verträge aus und bewahren (*aufheben, lagern*) Sie die Papiere gut auf.
  Dann haben Sie den Vertrag auch in einer anderen Form.

Tipp

- Das Wort „**Cloud**“ kann zwei verschiedene Dienste bedeuten (*meinen*):
  - einen Dienst nur zum **Speichern**, zum Beispiel von Daten und Fotos,
  - oder einen Dienst zum Speichern und **Verarbeiten** von Daten.
- Der **Vorteil** von einer Cloud ist:
  Sie können von **überall** und **mit allen Geräten** die Cloud über das Internet erreichen.
- Achtung:
  - Nehmen Sie ein **gutes Passwort** für Ihre Cloud.
    Mehr zu guten Passwörtern finden Sie auf der Seite 44.
  - Wählen Sie einen **zuverlässigen Anbieter** für Ihre Cloud.
    Informationen zu Anbietern finden Sie, wenn Sie in Ihre Suchmaschine diese Wörter eingeben (*schreiben*): „heise beste Cloud-Speicher“. (*„heise“ ist der Name von einer Internetseite.*)
  - Wenn Sie Ihre Daten in einer Cloud speichern:
    Speichern Sie **zusätzlich** immer auch noch auf USB-Sticks oder auf einer externen Festplatte.

Sichere Software:

- Für das Arbeiten mit elektronischen Geräten brauchen Sie Hardware und Software.
- **Hardware** ist das, was Sie anfassen können: die Geräte und Zubehör (*was dazu gehört, was man dafür braucht*).
- **Software** sind die Programme, mit denen die Geräte arbeiten.
- Bei der Software kennt man zwei Typen:
  die Betriebssysteme und die Anwendungsprogramme.
- Das **Betriebssystem** braucht ein Gerät, um zu starten und zu funktionieren.
  Betriebssysteme sind zum Beispiel „Android“, „iOS“, „Windows“, „Linux“ und „MacOS“.
- Ein **Anwendungsprogramm** nennt man auch **App**.
  Apps haben bestimmte Funktionen, zum Beispiel Schreibprogramme, Internet-Browser (*um ins Internet zu gehen*), E-Mail-Programme und Messenger (*zum Austausch von Nachrichten*).
  Apps müssen zum Betriebssystem von Ihrem Gerät passen.

- Kaufen Sie nur **Programme** von zuverlässigen Anbietern (*Verkäufern, Firmen*).
- Am besten laden (*übertragen*) Sie die Programme nur **vom Original-Anbieter** auf Ihre Geräte.

- Die Original-Internetseiten finden Sie über Ihre Suchmaschine, zum Beispiel „Google“ oder „Startpage“. Geben Sie dort den Namen des Programms ein.
- Apps für Ihr Smartphone laden Sie am besten nur herunter: aus dem „Google Play Store“, vom „Apple Store“ oder vom „Windows Store“.

- **Vorsicht**: Prüfen Sie **billige Angebote** von Programmen genau, die sonst viel teurer sind.
- Kaufen Sie keine Programme ohne Zertifikate (*Bestätigung, dass etwas echt ist*) vom Original-Anbieter.
- Suchen Sie im Internet nach Informationen, wie zuverlässig ein Anbieter und die Qualität von solchen billigen Programmen sind.
  Oft können Sie Berichte darüber finden.

- **Software** zu schreiben, ist **kompliziert**.
- Dabei gibt es immer Schwierigkeiten:
  - Es gibt **Fehler** von Funktionen in den Programmen.
  - Und es gibt Fehler in den Programmen, die Hacker (*Anbieter*) für Angriffe (*Versuche in Ihr Gerät einzudringen und es zu steuern*) benutzen können.
  - Diese Stellen nennt man **Sicherheitslücken**.
  - Jede Software-Firma verbessert ihre Programme immer wieder, um die Sicherheitslücken zu schließen.
  - Diese **Verbesserungen** nennt man **Update**.
  - Jede Software-Firma gibt die Updates an die Benutzer von ihrer Software weiter.
- Ein **Upgrade** ist eine größere Veränderung von Programmen. Mit einem Upgrade gibt es meistens auch **neue Funktionen**. Ein Upgrade hat oft einen etwas anderen Namen als die ältere Version.

- Die meisten Geräte zeigen Ihnen automatisch, wenn es Updates oder Upgrades gibt.
- Laden Sie immer **sofort alle Updates und Upgrades** für Ihr Betriebssystem und Ihre Apps auf Ihre Geräte.

- Nur dann haben Sie die **sicherste Version** von diesem Programm und machen es Hackern schwer.
- Wenn Sie ein Programm länger nicht aktualisiert (*Updates und Upgrades herunter geladen*) haben, machen Sie das, bevor Sie das Programm wieder benutzen.

- Wenn Sie unsicher sind, informieren Sie sich auf der Original-Internetseite der Software-Firma von diesem Programm.
  Dort steht, welche Version die neueste Version ist.
  Informationen über die Original-Internetseiten der Firmen und über die neuesten Versionen der Programme finden Sie oft auch auf www.wikipedia.de .

- Installieren (*einrichten, zum Arbeiten bringen*) Sie **nur** die **Programme**, die Sie wirklich **benutzen**.

- Löschen Sie Programme, die sie nicht brauchen.
- Warum? – Wenn Sie weniger Programme und Apps haben, ist das Risiko von Sicherheitslücken kleiner.

- Installieren Sie möglichst **moderne Programme**.

- Warum? – Die Anbieter machen nach einiger Zeit keine Updates mehr.
  Wenn Sie alte Programme haben, bekommen Sie schon bald keine Updates mehr.
- Dann bleiben die Sicherheitslücken offen und Ihre Geräte sind nicht mehr gut geschützt.

- **Überlegen** Sie beim Kauf von Geräten:

  - Möchte ich ein älteres Gerät mit vielen technischen Möglichkeiten und älteren Programmen haben?
  - Oder nehme ich für den gleichen Preis ein neues Gerät mit modernen Programmen, aber mit etwas weniger technischen Möglichkeiten.
    Es ist dann länger sicher.

- Hacker suchen oft **Sicherheitslücken** in Programmen, die sehr viele Menschen benutzen.

- Warum?
  Wenn Hacker eine Sicherheitslücke gefunden haben, können sie die Geräte von sehr vielen Menschen angreifen.
- Was können Sie tun? – **Überlegen** Sie:

  - Welche Funktionen benutze ich von einem Programm?
  - Nehme ich ein **sehr bekanntes Programm**, zum Beispiel Outlook als E-Mail-Programm?
  - Oder nehme ich ein Programm, das nicht so bekannt ist, zum Beispiel Thunderbird als E-Mail-Programm?

- Sie wollen ein **kostenloses Programm** oder eine kostenlose App installieren.

- Informieren Sie sich: Mit welchen Daten von mir bezahle ich für dieses Programm oder für diese App?
- Überlegen Sie: Möchte ich das?
  Werden auch die Kontaktdaten meiner Familie und Freunde von diesem Programm gelesen?
  Möchten die das?

- Sie wollen ein Programm oder eine App installieren?
- Sehen Sie in die **Einstellungen** von diesem Programm oder von dieser App. Die Einstellungen finden Sie im **Menü** (*Liste von möglichen Funktionen*) von dem Programm oder von der App. Oft wird das Menü mit 3 Punkten nebeneinander oder mit 3 kurzen Strichen untereinander angezeigt.

- Erlauben (*ja sagen*) Sie nur das, was Sie wollen.
- Viele Programme und Apps lesen viel mehr von Ihren Daten, als sie für das Funktionieren brauchen.
- Ihre **Privatsphäre** (*was privat ist*) ist besser geschützt, wenn Programme und Apps weniger von ihren Daten lesen können.

- Manchmal öffnet sich plötzlich auf Ihren Geräten ein neues Fenster. Solche Fenster nennt man auch **Popup**.

- Popups stören Sie bei einer anderen Aktivität.
- Aber: Popups können **vom Betriebssystem** oder **von einer App** kommen und Ihnen eine **wichtige Frage** stellen, zum Beispiel nach der Erlaubnis für das Installieren von einem neuen Programm.
- So ein neues Programm kann von Ihnen gewünscht sein. Aber es kann auch Schad-Software sein.
- Lesen Sie immer die Informationen in den Popups und entscheiden Sie bewusst, was Sie machen wollen. Sonst erlauben Sie vielleicht selber das Installieren einer Schad-Software auf Ihren Geräten.

Erste Hilfe bei Problemen

- Sie denken, dass mit Ihrem Gerät etwas nicht mehr in Ordnung ist?
- Sie beobachten (*sehen*) merkwürdige Reaktionen Ihrer Geräte, zum Beispiel:
  - Ihr Gerät arbeitet sehr, sehr langsam und Sie wissen keinen Grund dafür.
  - Ihr Gerät wird warm und der Akku ist schnell leer. Sie wissen keinen Grund dafür.
  - Ein Fenster öffnet sich viele Male, ohne dass Sie das möchten.
  - Ein Programm oder mehrere Programme öffnen sich nicht mehr oder sind nicht mehr da.
  - Sie können Dateien nicht mehr öffnen.
  - Das Hochfahren von Ihrem Gerät dauert sehr lange und Sie wissen keinen Grund dafür.
  - Das Hochfahren (*Aktivieren von Programmen, damit ihr Gerät arbeiten kann*) von Ihrem Gerät bricht (*hört auf*) immer an einer bestimmten Stelle ab.
- Dann könnte **Schad-Software** auf Ihrem Gerät sein.
- Schad-Software wird oft auch **Malware** genannt.
- Die meisten von diesen Problemen kann nur ein **Experte** lösen.
  Sie müssen ihm gute Informationen geben und einiges vorbereiten.

- Sie brauchen möglichst viele **Informationen über das Problem**.
  - Schreiben Sie sich die **Fehlernummer** auf, wenn Ihr Gerät eine Nummer anzeigt.
  - Machen Sie ein **Foto vom Bildschirm**.
  - **Schreiben** Sie sich **alles** genau auf, was Sie beobachtet und auch was Sie vorher gemacht haben.

Tipp

- **Trennen** Sie Ihr Gerät **vom Heimnetzwerk**:
  - Ziehen Sie das LAN-Kabel ab.
  - Oder schalten Sie das WLAN aus.

!

- **Fahren** Sie das Gerät **herunter** und lassen Sie es ausgeschaltet, bis Sie sich Rat von einem Experten geholt haben.
- **Suchen** Sie mit einem anderen Gerät **im Internet** nach dem Fehler, den Ihr Gerät hat.
  Oft haben andere Nutzer so einen Fehler schon gehabt und geben **Tipps**, was Sie tun können.
  Wenn Sie nur ein Gerät haben, fragen Sie einen Freund (oder eine Freundin), ob Sie für diese Suche sein (ihr) Gerät benutzen dürfen.

Tipp

- Bitten Sie einen Freund (oder eine Freundin) um **Hilfe**, der (die) sich wirklich **gut** mit solchen Problemen **auskennt**.
- Manchmal kann ein **Virenschutz-Programm** helfen.
  Dafür brauchen Sie Informationen, welches Virenschutzprogramm für Ihr Problem geeignet (*passt, helfen kann*) ist.
- Manchmal müssen Sie Ihre Gerät ganz **neu aufsetzen** (*einrichten*).
  Dazu brauchen Sie eine **Sicherung** zur Wiederherstellung von Ihrem **Betriebssystem**.
  Mehr dazu finden Sie auf der Seite 51.

!

- **Achtung**, wenn Sie Ihre Gerät neu aufsetzen:
  Es kommt meistens die Frage,
  - ob Ihr Gerät repariert werden soll
  - oder ob alles gelöscht werden soll.

  Die Antwort muss sein: Es soll **alles gelöscht** werden.
  Sonst bleibt die Schad-Software oft auf Ihrem Gerät aktiv.

- Wenn Sie Ihr Gerät neu aufsetzen, müssen Sie **alle** Ihre **Daten neu** auf Ihr Gerät **übertragen**.
  Dazu brauchen Sie ein **Backup** von Ihren Daten.
  Mehr dazu finden Sie ab Seite 51.

- Wenn die Daten auf Ihrem Gerät **verschlüsselt** (*für Sie nicht mehr zu lesen*) wurden und Sie **erpresst** werden:
  Bezahlen Sie nicht!

Tipp

- Meistens werden Ihre Daten nicht wieder entschlüsselt (*die Verschlüsselung zurück genommen*).
  Der Erpresser will nur das Geld haben.
  Er hat kein Interesse, dass Sie wieder an Ihre Daten kommen.
- **Setzen** Sie Ihr **Gerät neu auf**, ohne zu bezahlen.

- Es gibt auch **Zugriff-Versuche** (*Versuch einzudringen und zu steuern*) über **Anrufe**:
  - Sie bekommen einen freundlichen **Anruf vom Anbieter** von Ihrem **Betriebssystem**.
  - Der Anrufer ist aber ein **Betrüger**.
  - Der Anrufer sagt, dass er etwas an Ihrem Gerät kostenlos reparieren möchte.
  - Der Anrufer bittet Sie, ihm **alle wichtigen Zugangsdaten** zu Ihrem Heimnetzwerk und Ihrem Gerät zu nennen.
  - Damit hat der Anrufer alle wichtigen Daten für einen **Zugriff** auf Ihr Heimnetzwerk und Ihr Gerät.

- **Geben Sie nie Zugangsdaten zu Ihrem Heimnetzwerk und Ihren Geräten über das Telefon, über E-Mail oder über eine Internetseite an andere Personen oder eine Firma.**

- Es gibt nur eine Ausnahme:
  Wenn Sie selber einen Auftrag für einen solchen Service erteilt (*gegeben*) haben.

- Achtung: **Kontrollieren Sie Ihr Bank-Konten und Ihre Konten bei Online-Händlern regelmäßig!**

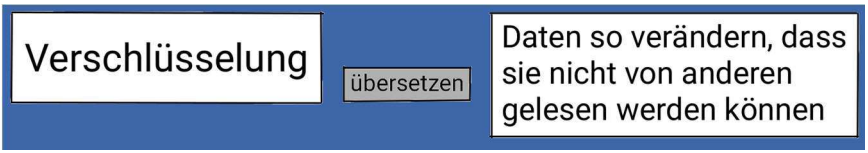
- **Überprüfen** Sie, ob die **Aktivitäten** alle von Ihnen kommen.
- Wenn Sie Aktivitäten finden, die **nicht von Ihnen** kommen:
  - **Ändern** Sie sofort Ihre **Zugangsdaten**.
  - **Kontaktieren** Sie sofort Ihre Bank oder Ihren Online-Händler und informieren Sie **schriftlich** über die Unregelmäßigkeiten (*das etwas nicht in Ordnung ist*).
  - Legen Sie beim Händler **schriftlich Widerspruch** gegen die Bestellungen und Rechnungen ein, mit denen Sie nichts zu tun haben.
  - Lassen Sie falsche Bankeinzüge (*jemand hat Geld von Ihrem Konto abgebucht*) auf Ihr Konto **zurückbuchen** (*zurückholen*). Wie Sie eine Rückbuchung machen, sagt Ihnen Ihre Bank.
  - Nehmen Sie Kontakt mit der **Polizei** auf und erstatten (*machen*) Sie **Anzeige**.
    Aber: Die Polizei kann oft nicht viel helfen.
    Deshalb ist es **wichtig**, **dass Sie sich selber schützen – durch gute Passwörter und sicheres Arbeiten mit Ihren Geräten**.

- Sie finden **peinliche Fotos** oder falsche Fotos von Ihnen in **Social Media** (Soziale Medien).

- Es wird **Schlechtes** über Sie in Social Media (*Sozialen Medien*) **geschrieben**.
- **Verlangen** Sie **schriftlich** die **Entfernung** von der Person, die diese Sachen hochgeladen (*im Social Media gespeichertt*) hat.

- Verlangen Sie auch schriftlich die Entfernung dieser Sachen vom **Betreiber** (*Anbieter*).
- Sie haben ein **Recht auf Löschung** dieser Sachen. Aber:
  - Oft müssen Sie es **mehrfach versuchen**, bis diese Sachen gelöscht werden.
  - Oft werden diese Sachen auch **wieder hochgeladen**.
  - **Machen Sie weiter**, bis diese Sachen alle weg sind. Auch, wenn das viel Ärger und viel Arbeit macht.

Fachbegriffe



Account	Benutzerkonto
Add-on	kleines Programm, das die Funktion von einem anderen Programm ergänzt oder erweitert (*vergrößert*)
Adapter	Verbindungsstück
aktualisieren	Programme auf den neuesten Stand (*Stufe, Version*) bringen
Anbieter	Firma oder Betreiber

angreifen	In ein elektronisches Gerät eindringen und versuchen, es zu steuern.
Anhang	Datei an einer E-Mail oder einer Nachricht
Anwendungsprogramme	Programme für bestimmte Funktionen
App	Anwendungsprogramm
App-Store	Internetseite von einem Anbieter für Anwendungs-Software
aufrufen	eine Internetseite öffnen
aufsetzen	Ein Gerät neu einrichten. Alle Programme und Daten auf das Gerät übertragen, die Sie brauchen.
Aufspielen	Programme und/oder Daten auf ein Gerät übertragen
ausloggen	abmelden
Backup	Sicherungskopie – Sicherung von Ihren Daten
barriere-frei	kann ohne weitere Hilfe auch von eingeschränkten (*behinderten*) Personen benutzt werden
Berechtigung	was jemand oder ein Programm darf
Betreiber	Anbieter oder Firma
Betriebssystem	Programme zum Starten und Funktionieren von elektronischen Geräten
biometrische Daten	Eine spezielle Form von Passwörtern. Das Gerät wird durch einen Fingerabdruck, das Gesicht oder das Auge entsperrt (*Zugang geöffnet*).
Blockieren	Die Arbeit unmöglich machen, verbieten.
Blog	Internetseite mit Informationen zu einem bestimmten Thema. Es werden zeitlich geordnet neue Informationen zu diesem Thema ergänzt (*dazu geschrieben*).
Booten	Aktivierung von Programmen, damit ein elektronisches Gerät arbeiten kann.
Bot	ein Computerprogramm, das automatisch seine Aufgaben erfüllt (*macht*).
Browser	Programm, um im Internet zu surfen (*Seiten im Internet anzusehen*)
BSI	Bundesamt für Sicherheit in der Informationstechnik
chatten	Textnachrichten oder Sprachnachrichten senden und empfangen und telefonieren
Chronik	Geschichte, sie zeigt, welche Internetseiten Sie nacheinander angesehen haben.
Client	Programm oder App für Social Media (*Soziale Medien*)

Cloud	Speicherplatz bei einem Anbieter oder die Möglichkeit zur Datenverarbeitung und Speicherplatz von einem Anbieter
Code	geheimes Wort oder geheime Zeichenkombination
Cookies	Daten, die der Anbieter einer Internetseite beim Ansehen auf Ihre Geräte überträgt. Diese Daten speichern Informationen über Ihre Aktivitäten für den Anbieter der Internetseite.
Cursor	Pfeil
Datenverarbeitung	elektronisches Arbeiten mit Daten
deaktivieren	ausschalten
digital	elektronisch
Doxing	sammeln und veröffentlichen von Daten anderer Personen im Internet
DVD	digitaler Datenspeicher
einbuchen	verbinden
einloggen	anmelden
einrichten	gewünschte Programme und Daten auf elektronische Geräte übertragen und speichern
einspielen	übertragen und speichern
Einstellungen	Möglichkeiten und bestimmte Funktionen eines Programms
E-Mail-Account	E-Mail-Konto für eine bestimmte E-Mail-Adresse
Erweiterung	kleines Programm, das die Funktion von einem anderen Programm ergänzt (*vergrößert*)
extern	außerhalb (*nicht in*) von elektronischen Geräten
Facebook	weltweit viel genutztes Social Media
Fake-News	gefälschte (*falsche*) Nachrichten
Fehlernummer	eine Nummer, die Ihr Gerät anzeigt, wenn es nicht mehr richtig arbeitet.
Festplatte	elektronisches Bauteil zum Speichern von Daten
Firewall	spezielles Programm, das nur gewünschte Daten von außen in Ihr Netzwerk und auf Ihre Geräte lässt
Gast-WLAN	ein spezieller Teil vom WLAN im Heimnetzwerk für Gäste
hacken	suchen von Lücken in der Sicherheit von Programmen oder Apps und dann steuern von elektronischen Geräten über diese Lücken
Hacker	Angreifer
Hardware	elektronische Geräte und Zubehör (*was dazu gehört*), das man anfassen kann

Heimnetzwerk	lokales (*an einem Ort*) Netzwerk bei Ihnen zuhause
herunterladen	Programme oder Daten auf einem elektronischen Gerät speichern
Hilfeseiten	Erklärungen zu einen Programm – Gebrauchsanleitung
hochfahren	Ein elektronisches Gerät aktiviert (*schaltet an*) die Programme, um arbeiten zu können.
Homepage	Dokument, das Sie über das Internet ansehen können
HTML-Darstellung	Zeigen von Bildern in E-Mails
http	zeigt an, dass die Übertragung einer Internetseite nicht verschlüsselt ist, also für andere lesbar ist
https	zeigt an, dass die Übertragung einer Internetseite verschlüsselt ist, also für andere nicht lesbar ist
Identität	Persönliche Daten
Instagram	Social Media (*Soziales Medium*) zum Teilen von Fotos und Videos
installieren	einrichten, speichern
Instant-Messenger	Dienst für die schnelle Kommunikation (*Austausch von Informationen*)
Internet	weltweite Verbindung von elektronischen Geräten
Internetseite	Dokument, das Sie über das Internet ansehen können
Junk	unerwünschte E-Mails
Kennwort	Passwort zum Anmelden / zum Entsperren (*Zugang öffnen*) von einem Gerät oder einer Funktion
Keylogger	Computerprogramm, das aufzeichnet (*speichert*), welche Tasten Sie auf der Tastatur drücken. Es gibt diese Informationen weiter. So können Hacker Ihre Passwörter herausfinden und Ihre ganze Kommunikation lesen.
Koppeln	verbinden
laden – herunterladen	Programme oder Daten auf einem elektronischen Gerät übertragen und speichern
LAN	lokales (*an einem Ort*) Netzwerk; Heimnetzwerk
Lesezeichen	Funktion von Ihrem Browser, mit der Sie die Adresse von häufig angesehenen Internetseiten schneller eingeben können.
Link	Verbindung zu einer bestimmten Internetseite
Login	Anmeldung
Logout	Abmeldung

lokal	nur auf einem elektronischen Gerät
mailen	E-Mails senden und empfangen
Malware	Schad-Programm, schädliche Software
Menü	Liste von möglichen Funktionen von einem Programm
Messenger	Dienst für die schnelle Kommunikation (*Austausch von Informationen*)
mobben	Schlechtes über jemanden schreiben oder sagen oder schlimme Fotos von jemandem zeigen
nachladen	etwas später übertragen
Newsletter	Informations-E-Mail
Nutzungsbedingungen	Regeln vom Anbieter, die für die Nutzer gelten
öffentliches WLAN – offenes WLAN	unverschlüsseltes und damit für jeden nutzbares WLAN
offline	nicht mit dem Internet verbunden
online	mit dem Internet verbunden
Online-Banking	über das Internet Geld vom Konto überweisen, Aufträge erteilen oder zurücknehmen, den Kontostand überprüfen
Passwort	Kennwort zum Anmelden / zum Entsperren (*Zugang öffnen*) von einem Gerät oder einer Funktion
Passwort-Manager	Programm zum Generieren (*machen*) und Speichern von Passwörtern
Phishing	Stehlen von Zugangsdaten und anderen Informationen
Plug-in	Programm für das Zeigen von Bildern auf Internetseiten
Popup	Fenster, das sich plötzlich auf Ihren Geräten öffnet
privat	ohne, dass jemand Ihre Aktivität und Daten auf Ihren Geräten mitlesen kann
Privatsphäre	was privat ist
Profil	in Social Media (*Soziales Medium*): Angaben zu Ihrer Person (*zu Ihnen persönlich*)
Provider	Anbieter oder Firma
registrieren	eintragen
Router	elektronisches Gerät, das ein lokales Netzwerk mit dem Internet verbindet.

Sicherheitsabfrage	Spezielle Frage, auf die Sie antworten müssen, wenn Sie Ihre Zugangsdaten (*Anmeldedaten*) vergessen haben. Sie müssen die Frage und die Antwort wissen.
Sicherheitslücke	Stelle in einem Programm, die Hacker für einen Angriff auf elektronische Geräte nutzen können
Sicherungskopie	Sicherung von Ihren Daten und Programmen
Social Media	Soziale Medien, Soziales Netzwerk; digitale Technik zur Kommunikation von Nutzern
Software	Programme für das Funktionieren von elektronischen Geräten
Spam	unerwünschte E-Mail
Spam-Filter	Programm, das unerwünschte E-Mails erkennt
Standort	wo Sie sind
Suchmaschine	Programm für die Suche im Internet
surfen	Seiten im Internet ansehen
TAN	Transaktionsnummer (beim Online-Banking)
TAN-Generator	Gerät zum Erzeugen (*Herstellen*) von TANs
teilen	anderen Personen etwas mitteilen (*weitersagen, weiterschicken*)
Trojaner	Programme, die auf elektronischen Geräten spionieren (*heimlich beobachten und Informationen weitergeben*)
Twitter	Social Media (*Soziales Medium*) für Kurznachrichten
Update	neue Verbesserung von einem Programm
Upgrade	neue größere Verbesserung von einem Programm
UPNP	Funktion von einem Router
USB-Stick	Hardware zum Speichern (ungefähr so groß wie ein Daumen)
verarbeiten von Daten	Ein Programm arbeitet mit den vorhandenen Daten.
verschlüsseln	Daten so verändern, dass sie nicht von anderen Geräten gelesen werden können
Version	Ausgabe, Form
verwalten	Dinge speichern, senden, empfangen, entwerfen, löschen
Virenscanner	Programm, das auf Ihren Geräten nach Schad-Programmen sucht und diese unschädlich macht
Virus	Schad-Programme, die sich selber vermehren, verbreiten und manchmal auch die Software und Hardware zerstören

Web-Browser	Programm, um im Internet zu surfen (*Seiten im Internet anzusehen*)
Webseite	Dokument, das Sie über das Internet ansehen können
weitergeben	anderen Personen etwas weiterschicken
Wischzeichen	Eine spezielle Form von Passwörtern. Man fährt mit dem Finger in einer bestimmen Reihenfolge über die Zahlen auf dem Bildschirm von einem Gerät (meistens ist es ein Smartphone).
WLAN	Wireless LAN – Verbindung ohne Kabel: Funk-Verbindung von elektronischen Geräten in einem Netzwerk
WLAN, öffentliches / offenes	unverschlüsseltes und damit für jeden nutzbares WLAN
WPA2	Typ einer Verschlüsselung von einem WLAN
WPA3	neuerer Typ einer Verschlüsselung von einem WLAN
WPS	eine Funktion von Ihrem Router
Wurm	Schad-Programm, das sich selber vermehrt und verbreitet und die Aktivität der normalen Programme auf Geräten stört
Zertifikat	Bescheinigung, dass etwas echt ist
Zertifikatsfehler	Es gibt keine Bescheinigung, dass die Internetseite echt ist.
zertifiziert	beglaubigt
Zugangsdaten	Anmeldedaten
zugreifen	eindringen in ein elektronisches Gerät und von einem anderen elektronischen Gerät aus steuern
Zusatzprogramm	Programm, das die Funktion von einem anderen Programm ergänzt oder erweitert (*vergrößert*)
Zwei-Faktor-Authentifizierung	Ausweisen in 2 Schritten