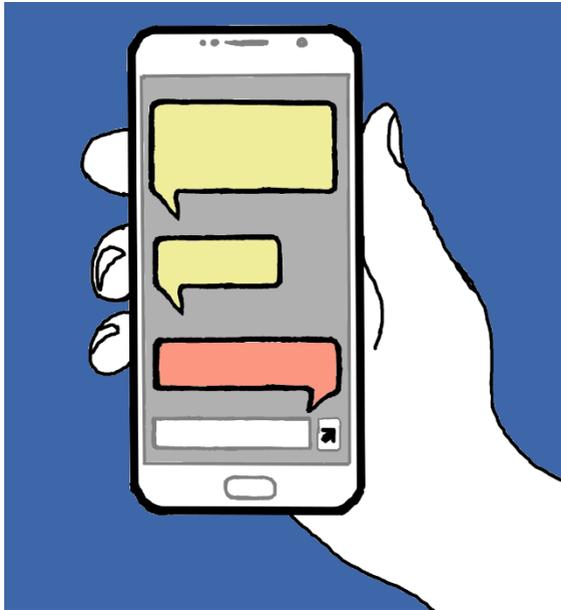


# Messenger sicher und privat nutzen

Tipps in Leichter Sprache



Von  
IntegrationLE

## Vorwort

Wir versuchen, Ihnen das Wichtigste zum sicheren und privaten Benutzen von Messengern (*Programmen zum Senden und Empfangen von Nachrichten*) 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.

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](http://www.bsi.bund.de) .

Aktuelle Informationen in Leichter Sprache finden Sie auch auf unserem Blog [www.it-sicherheit-ganz-leicht.de](http://www.it-sicherheit-ganz-leicht.de) .

Wir wünschen Ihnen sicheres Arbeiten mit Ihren Geräten.

*Inken Hagestedt*

*Stephanie Freundner-Hagestedt*

---

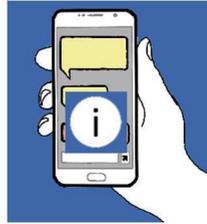
Das vorliegende Dokument wurde ehrenamtlich von IntegrationLE erarbeitet. Die Informationen sind mit größter Sorgfalt zusammengestellt worden. Eine Gewähr für den Inhalt kann trotzdem nicht übernommen werden, insbesondere sind jegliche Haftungsansprüche ausgeschlossen.

---

Dieses Dokument einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung ist ohne Zustimmung der Autorinnen unzulässig. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Copyright © 2021 IntegrationLE, Leinfelden-Echterdingen. Autorinnen: Inken Hagestedt und Dr. Stephanie Freundner-Hagestedt, c/o Postflex #413, Emsdettener Str. 10, 48268 Greven, [integration.le@web.de](mailto:integration.le@web.de)

# Messenger – Allgemeine Informationen



## 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 (*sprechen und schreiben*) und Informationen austauschen können.
- Messenger sind zum Beispiel „WhatsApp“, „Skype“, „Signal“, „Google Hangout“, „iMessage“, „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 (*Firmen*), welche Informationen die Anbieter 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.  
Mehr dazu finden Sie ab Seite 8.
  - Vielleicht können Sie auch Ihre Freunde überzeugen (*mit guten Gründen dazu bringen*), zu Ihrem Messenger zu wechseln.
  - Viele Informationen über Messenger finden Sie beim BSI (*Bundesamt für Sicherheit in der Informationstechnik*).
  - 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 (*Firma*) herunter. Das ist am sichersten. Sonst laden Sie vielleicht auch andere schädliche (*können etwas kaputt machen*) Programme auf Ihre Geräte. 
  - So finden Sie die Original-Seite:  
Geben Sie den Name vom Client 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 (*was privat ist*). 
  - 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. Updates und Upgrades sind Verbesserungen von einem Programm. Mehr dazu finden Sie in unseren allgemeinen Tipps ab Seite 54.   
<https://it-sicherheit-ganz-leicht.de/images/IT-Sicherheit.pdf>
  - Jeder Anbieter hat ein Interesse daran, dass sein Betriebssystem sicher ist. Deshalb verbessert der Anbieter die Sicherheit ständig (*immer wieder*) durch **Sicherheits-Updates**. Laden Sie deshalb immer alle Sicherheits-Updates sofort herunter. 

➤ **Achtung:**

Wenn Sie eine Nachricht bekommen, dass ein **neues Gerät** auf Sie **angemeldet** wurde:

Sie sollten diese Nachricht beachten.

Vielleicht haben Sie selber ein neues Gerät angemeldet.

Dann brauchen Sie nichts zu tun.



➤ 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.

Tipp

➤ **Füllen** (*schreiben*) Sie bei der Anmeldung nur die Felder **aus**, die Sie ausfüllen **müssen**.

In alle anderen Felder schreiben Sie nichts.

Tipp

➤ **Verbieten** (*nein sagen*) Sie dem Messenger **möglichst viel**, wenn Sie den Messenger installiert (*heruntergeladen und eingerichtet*) haben.

Erlauben (*ja sagen*) Sie nur die Sachen, die der Messenger braucht, um zu funktionieren.

Dafür müssen Sie in die **Einstellungen** vom Messenger gehen.

Die Einstellungen erkennen Sie meistens:

- An mehreren Strichen eng übereinander.
- Oder an mehreren Punkten nebeneinander.

- Denken Sie daran:  
Alles, was Sie über einen Messenger kommunizieren (*schicken und bekommen*), **kann öffentlich** (*vielen anderen Personen bekannt*) **werden**. 
- Bitte schreiben und sprechen Sie nur über Sachen, die **nicht** sehr **privat** sind. 
- Nehmen Sie ein gutes **Bild** für Ihr Profil (*Angaben / Informationen 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 (*zustimmen*). 
- Solche Kontaktanfragen können auch kommen:
  - von Kriminellen (*Personen, die etwas gegen die Gesetze tun*),
  - 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.
- Sie können **Nachrichten** von einer anderen Person **blockieren** (*sperren / das Empfangen verbieten*), wenn diese Nachrichten Sie stören oder Ihnen Angst machen. 

---

- 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 den 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. 

## Messenger – Spezielle Informationen

### Ein sicherer Messenger ist besser



- Sie kennen die **bekanntesten Messenger** wie zum Beispiel:
    - WhatsApp
    - Telegram
    - Signal
    - iMessage
  - **Nicht so bekannte Messenger** sind zum Beispiel:
    - Threema
    - Wire
    - Viber
    - Ginlo
    - Element
    - Conversations
- 
- Jeder Messenger arbeitet ein bisschen anders.
  - Es gibt **Messenger**,
    - die Sie nur **auf** dem **Smartphone** benutzen können,
    - die Sie **auf** dem **Smartphone** und **auf** einem **Computer** benutzen können.
  - Es gibt Messenger,
    - die Experten (*Leute, die sehr viel über etwas wissen*) für **sehr sicher** halten (*es denken*),
    - die Experten für **nicht so sicher** halten.
- 



- Sie fragen sich vielleicht:

**Warum** soll ein Messenger **sicher** sein?

Brauche ich einen sicheren Messenger?

Ich chatte (*Nachrichten schreiben und empfangen*) und spreche mit meinen Freunden doch nur über Sachen aus dem Alltag. Das interessiert doch niemanden.



- Wir sagen:

Das ist nicht ganz richtig.

---

- Ihre Nachrichten und Telefonate können viel über Sie erzählen.

- Ein Anbieter (*Firma*) von einem unsicheren Messenger kann zum Beispiel:



- Ihre **Nachrichten** auch **lesen**, weil sie nicht verschlüsselt (*für andere unlesbar gemacht*) sind oder schlecht verschlüsselt sind.
  - Ihre **Telefonate** auch **hören**, weil sie nicht verschlüsselt sind oder schlecht verschlüsselt sind.
  - Und **alle** Nachrichten, Telefonate, Dateien und Bilder auf Servern (*sehr großen Computern*) für lange Zeit **speichern**.
  - Und vielleicht können auch andere Personen Ihre Nachrichten lesen oder Ihre Telefonate hören. Zum Beispiel **Hacker** (*Personen, die in elektronische Geräte eindringen / hineinkommen*) oder die Polizei.
  - Oder der Anbieter von Ihrem Messenger kann die gespeicherten **Nachrichten** an andere Firmen **verkaufen**.  
Und Sie wissen nichts davon.
-

- Sie sagen vielleicht: Das ist mir egal.  
Ich tue nichts Illegales (*gegen die Gesetze*).  
Jeder kann lesen, was ich schreibe.  
Und hören, was ich sage.
- Wir sagen:  
Für jeden ist es **wichtig**, dass seine **Nachrichten**  
**und seine Telefonate geheim** (*unbekannt*) bleiben.
- Denn: Eine **andere Person weiß** sehr **viel** über Sie,  
über Ihre Familie und über Ihre Freunde:
  - Wenn diese Person viele von Ihren **Nachrichten lesen kann**.
  - Wenn diese Person viele von Ihren **Telefonaten hören kann**.
  - Wenn diese Person die **Links** (*Adressen von Internetseiten*),  
die **Dateien** und die **Bilder kennt**, die Sie verschicken  
und empfangen.
- Die andere Person **weiß dann** zum Beispiel:
  - **Wie Sie leben**.
  - Wie viel **Geld** Sie ungefähr verdienen.
  - Ob Sie **arbeitslos** sind.
  - Welchen **Beruf** Sie haben.
  - Welche **Krankheiten** Sie haben.
  - Wofür Sie sich interessieren.
  - Welche **Hobbys** Sie haben.
- Wollen Sie wirklich, dass Unbekannte (*Personen, die Sie nicht kennen*) viel über Sie wissen? - Nein?
- Dann ist ein **Messenger mit einer guten Verschlüsselung**  
richtig für Sie.



- Auch die **Metadaten** (*Informationen, die beim Senden und Empfangen von Nachrichten entstehen*) **erzählen viel** über Sie, Ihre Familie und Ihre Freunde.
- Und auch das **Telefonbuch auf Ihrem Gerät** gibt viele **Informationen** über Sie.
- Ihre **Dateien** und Ihre **Bilder auf Ihrem Gerät** auch.



➤ **Metadaten** sind alles:

- Was für das Verschicken und Empfangen von Nachrichten gebraucht wird.
- Und was zusätzlich (*mehr*) mitgeschickt wird.



Zum Beispiel:

- Die **Telefonnummern** von Ihnen und der Person, mit der sie schreiben oder sprechen.
  - Ihr Nutzernamen und die **Nutzernamen** der anderen Personen.
  - **IP-Adressen** (*Adressen von den Geräten im Internet*).
  - **Datum** und **Uhrzeit**, wann Nachrichten verschickt und gelesen werden.
  - Der **Standort** (*wo es ist*) von Ihrem Gerät.
- 
- Wenn die Metadaten vom Messenger gespeichert werden, **weiß** der Anbieter vom **Messenger** zum Beispiel genau:
    - **Mit wem** Sie Kontakt haben.
    - **Wann** Sie Kontakt haben.
    - **Wann** Sie wahrscheinlich **zuhause** sind.
    - **Wann** Sie wahrscheinlich **arbeiten**.
    - **Wie oft** Sie mit bestimmten Personen Kontakt haben



- **Wie lange** Sie diese Kontakte haben.
- **Welches Gerät** Sie benutzen.
- **Welche Internetseiten** Sie sich ansehen.
- **Wo** Sie oft hingehen.
- Der **Anbieter verkauft** alle diese **Informationen** vielleicht an andere Firmen.  
Und Sie wissen nicht, an welche Firmen.
- Wollen Sie, dass Unbekannte noch mehr über Sie und Ihre Kontakte wissen? – Nein?
- Dann ist ein **Messenger gut** für Sie:
  - Der **nur wenige Metadaten** für das Verschicken und Empfangen **braucht**.
  - Der **keine Metadaten speichert**.



**Tipp**

- 
- Auch der **Inhalt** von Ihrem Gerät **erzählt viel über Sie**.
    - Viele Messenger **greifen auf** (*lesen*) Ihr **Telefonbuch** in Ihrem Gerät zu.
    - Oder auf andere **Dateien** und **Fotos**.
  - Was bedeutet (*heißt*) das?  
Viele **Messenger benutzen** Ihre **Kontakte**, damit Sie einfacher mit Ihrer Familie und mit Ihren Freunden Kontakt haben können.  
Das ist praktisch.  
Aber Sie wissen nicht, was ein Messenger sonst noch mit den Informationen aus Ihrem Telefonbuch macht.
  - Ein **Messenger** kann alle Ihre **Kontakte**:
    - sich genau **ansehen**,
    - **kopieren**,
    - **speichern**,
    - Ihr **Telefonbuch** an andere Firmen **verkaufen**.



- Warum sind Ihre Kontakte interessant für den Anbieter vom Messenger und andere Firmen?
  - Ihre **Kontakte** geben **viele Informationen über Sie**.
  - Und: Der Anbieter vom Messenger kann die **Kontakte** von vielen Personen **vergleichen**.  
So bekommt der Anbieter noch mehr Informationen über alle seine Nutzer (jemand, der etwas benutzt).

- Wollen Sie, dass der Anbieter von Ihrem Messenger alle Ihre Kontakte kennt? – Nein?

- Dann ist ein **Messenger** für Sie **gut**:

- der Ihre **Kontakte nicht liest**
- oder Ihre Kontakte nur **verschlüsselt benutzt**.

**Tipp**

- Ein Messenger muss auf Dateien auf Ihrem Gerät zugreifen können, wenn Sie eine Datei verschicken wollen.

- Der Anbieter vom **Messenger** kann die verschickten **Dateien lesen, speichern, selber verwenden** oder **verkaufen**.

Sie können nichts dagegen tun.

- Wollen Sie, dass ein Anbieter oder Unbekannte Ihre Dateien kennen und damit Geld verdienen? – Nein?

- Dann ist ein **Messenger** für Sie gut, der Ihre Dateien sehr gut **verschlüsselt verschickt**.

**Tipp**

- Ein Messenger muss auf Ihre Bilder zugreifen können, damit Sie Bilder hochladen (*einstellen oder verschicken*) können.

- Der Anbieter von einem **Messenger** kann Ihre **Bilder ansehen, speichern, verwenden** und **verkaufen**.

- Manchmal **verlieren** Sie auch die **Rechte an Ihren Bildern**. Das heißt: Sie dürfen die Bilder nicht mehr verschicken und benutzen, wie Sie möchten. Aber der Anbieter vom Messenger darf das.

- Wollen Sie, dass ein Anbieter oder Unbekannte Ihre Bilder sehen und damit Geld verdienen? – Nein?



- Dann ist ein **Messenger gut** für Sie, der Ihre **Bilder sehr gut verschlüsselt verschickt**.

Tipp

- Das sollten Sie wissen:

- Sie nutzen viele Dienste (*Arbeiten / Sachen*) im Internet kostenlos.
- Das denken Sie, weil Sie dem Anbieter von einem Dienst **kein Geld** dafür **bezahlen**.
- Meistens **bezahlen** Sie aber **mit Informationen** über sich.
- Ein Anbieter kann diese Informationen selber nutzen oder an andere Firmen verkaufen.
- **Anbieter** und andere Firmen können mit diesen Informationen **viel Geld verdienen**.
- Der Anbieter oder andere Firma kann Ihnen viel **Werbung** schicken, die genau zu Ihnen passt.
- Dann **kaufen** Sie wahrscheinlich mehr, als Sie planen.  
Das kostet Sie viel Geld.  
Die Verkäufer verdienen viel.
- Und die Verkäufer bezahlen dem Anbieter oder anderen Firmen viel Geld für diese passende Werbung.



- Wollen alle Anbieter mit Informationen über Sie viel Geld verdienen?



- Manche Anbieter wollen vielleicht viel Geld verdienen.

- Andere **Anbieter** wollen vielleicht nur ihre **Rechnungen bezahlen**.

Denn: Ein Messenger muss die Kosten für Server, Strom, Miete und Personal (*Menschen, die arbeiten*) bezahlen.



Irgendwie muss der Messenger dieses Geld einnehmen (*bekommen*).

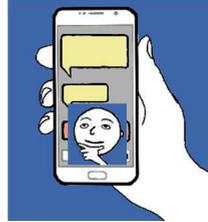
- Deshalb:

- **Manche Messenger verkaufen Informationen** über ihre Nutzer.
- Oder Messenger **verkaufen die Bilder** von ihren Nutzern.
- Manche Messenger bieten zusätzliche (*mehr*) **Dienste gegen Bezahlung** an (*man muss dafür bezahlen*).
- Manche Messenger finanzieren (*Geld haben*) sich durch **Spenden** (*geschenktes Geld*).
- Manche Messenger verlangen für das Herunterladen und Installieren eine **einmalige Gebühr** (*einmal bezahlen*).

- Wie können Sie einen Messenger finden, der zu Ihnen passt?

Das können Sie im nächsten Kapitel ab Seite 17 lesen.

## So finden Sie den richtigen Messenger für sich



- Ein **sicherer Messenger verschlüsselt** die Nachrichten und Telefonate
  - Verschlüsseln heißt:  
**Nur der Sender und der Empfänger** können die Nachrichten **lesen und** die Telefonate **hören**. Keine andere Person kann das.
  - Dann bekommt **keine andere Person Informationen** über Sie aus Ihren Nachrichten und Telefonaten.
  - Sie und Ihre Chatpartner (*Personen, mit denen Sie Kontakt haben*) sind **sicher**.
  - Und: Ihre **Privatsphäre** (*was privat ist*) und die Privatsphäre von Ihren Chatpartnern sind **geschützt**.
- 
- Nicht jeder Messenger verschlüsselt gleich gut.
  - Es gibt Messenger, die nur eine **Transport-Verschlüsselung** haben.
  - Transport-Verschlüsselung heißt:
    - Alles wird **auf dem Weg** von Ihnen zu einem Server (*sehr großem Computer vom Messenger*) **verschlüsselt**.
    - Alles wird auf dem Weg vom Server zu Ihrem Chatpartner verschlüsselt.



- **Auf den Wegen** kann also **niemand mitlesen** oder **mithören**.
- Aber: **Auf dem Server** vom Messenger können die Nachrichten **unverschlüsselt gespeichert** sein.
- Dann können Mitarbeiter vom Messenger Ihre **Nachrichten lesen**.  
Oder der Messenger kann Informationen aus Ihren Nachrichten herausfinden.
- Und: Der Messenger kann diese **Informationen** oder Ihre Nachrichten an andere Firmen **verkaufen**.
- Das heißt: Ein Messenger mit einer **Transport-Verschlüsselung** ist **nicht sicher**.
- Unser Tipp:  
**Nehmen Sie keinen Messenger mit einer Transportverschlüsselung.**



Tipp

- 
- Es gibt Messenger, die alle Nachrichten **komplett** (*ganz*) **verschlüsseln**.  
Deshalb heißt diese Verschlüsselung auch „**Ende-zu-Ende-Verschlüsselung**“.
  - Das bedeutet (*heißt*):  
**Keiner** kann Ihre Nachrichten **lesen** oder Ihre Telefonate **mithören**.  
Nur Sie und Ihr Chatpartner können das.
  - **Manche Messenger speichern** die Nachrichten und Telefonate verschlüsselt.  
Es gibt dann ein **kleines Risiko** (*Gefahr*),  
dass **Hacker** (*Personen, die in andere Computer eindringen*)  
oder die **Polizei** solche **Nachrichten** und Telefonate **entschlüsseln** (*wieder lesbar oder hörbar machen*).



- Oder ein **Gericht** sagt, dass der Messenger die **Nachrichten** und Telefonate **entschlüsseln** und der Polizei geben muss.

- **Manche Messenger speichern** die Nachrichten und Telefonate gar **nicht**.



Dann sind die **Nachrichten** und Telefonate **nur auf Ihrem Gerät** und auf dem Gerät von Ihrem Chatpartner.

- Dann kann eine andere Person nur Ihre Nachrichten lesen, wenn sie Ihr Gerät hat und Ihr Passwort kennt oder herausfindet.

Schützen deshalb Ihre Geräte mit sicheren Passwörtern.

**Tip**

Mehr zu sicheren Passwörtern finden Sie in unserer Broschüre mit allgemeinen Tipps ab Seite 44.

<https://it-sicherheit-ganz-leicht.de/images/IT-Sicherheit.pdf>

- Gut zu wissen:

- Bei manchen Messengern müssen Sie die **Ende-zu-Ende-Verschlüsselung** von Nachrichten extra **selber einstellen**.



- Messenger können für **Nachrichten** und Telefonate **andere Verschlüsselungen** haben **als für Gruppenchats** (*Nachrichten in Gruppen versenden und empfangen*) und Konferenzen (*Gespräche von mehreren Personen*).



- Bei manchen Messengern können Sie auch dies einstellen:



Eine **Nachricht** soll sich nach einer bestimmten Zeit **selber zerstören** (*kaputt machen*).

Dann ist die Nachricht weg.

Auf dem Server vom Messenger und auf Ihren Geräten.

➤ **Unsere Tipps:**

Tipp

- **Nehmen Sie einen Messenger mit Ende-zu-Ende-Verschlüsselung.**
- **Für sehr private Nachrichten benutzen Sie einen Messenger mit der Funktion „Selbst-Zerstörung“.**

➤ **Messenger arbeiten unterschiedlich mit den Metadaten.**

➤ Es gibt Messenger:

- Die mit **vielen** Metadaten arbeiten.  
Die nur **wenige** Metadaten brauchen.
- Die die Metadaten **speichern**.  
Die **keine** Metadaten **speichern**.



➤ **Unser Tipp:**

**Nehmen Sie einen Messenger:**

Tipp

- **Der nur wenige Metadaten braucht.**
- **Der keine Metadaten speichert.**

➤ Die meisten **Messenger lesen** die **Kontakte** aus Ihrem Telefonbuch auf Ihrem Gerät.  
Dann wird für Sie das Senden und Empfangen von Nachrichten einfacher.



➤ Nur wenige Messenger **lesen** Ihr Telefonbuch gar **nicht**.  
Wenn ein Messenger das Telefonbuch nicht liest, ist das **Benutzen** vom Messenger **schwieriger**.

➤ Bei manchen Messengern können Sie **einstellen**, dass Ihr Telefonbuch **nicht gelesen** wird.

- **Wie** die Messenger **mit den Kontakten** aus Ihrem Telefonbuch **arbeiten**, ist unterschiedlich: 
- Manche Messenger **lesen** und **speichern** alle **Kontakte** aus Ihrem Telefonbuch. Sie **verschlüsseln** die Kontakte **nicht**.
- Manche Messenger **verschlüsseln** die Kontakte aus Ihrem Telefonbuch **sofort**. Es ist eine besondere Verschlüsselung. Diese Verschlüsselung nennt man „**hashen**“. Diese Messenger arbeiten nur mit den gehashten Kontakten. Das heißt: Der Messenger kennt Ihre Kontakte nicht.
- Manche Messenger **speichern** Ihre Kontakte **nicht**.

- **Unser Tipp:**  
**Nehmen Sie einen Messenger, der die Kontakte aus Ihrem Telefonbuch hasht.**  
**Oder: Der die Kontakte nicht speichert.**

Tipp

- **Überlegen, Sie auf welchen Geräten Sie einen Messenger benutzen wollen.**

Tipp

- Es gibt Messenger:
  - Die Sie **nur auf** einem **Smartphone** benutzen können.  Die Sie **auf dem Smartphone und dem Computer** parallel (*gleich*) benutzen können.
  - Die nur **mit bestimmten Betriebssystemen** (*Programme, die die Geräte zum Arbeiten brauchen*) funktionieren. Mit einem anderen Betriebssystem funktionieren sie nicht. Zum Beispiel mit dem Betriebssystem Android oder mit dem Betriebssystem iOS.

- Deshalb: Der Messenger muss zu den **Betriebssystemen** auf Ihren Geräten und zu den Betriebssystemen auf den Geräten von Ihrem Chatpartner **passen**.



- **Überlegen** Sie, **für was** Sie den **Messenger benutzen** wollen, zum Beispiel:



- für geschriebene Nachrichten,
- für Sprachnachrichten,
- für Gruppenchats,
- für Videotelefonieren,
- für Konferenzen,
- für Informationskanäle (*Informations-Sender*).

- **Überlegen** Sie, **mit wem** Sie über einen Messenger **Kontakt haben wollen**:



- **Kennen** sich Ihre Chatpartner **gut** mit Geräten und Messengern **aus**?  
Dann können Sie mit Ihren Chatpartnern Messenger benutzen, die **nur wenige** Personen **kennen**.



- **Kennen** sich Ihre Chatpartner **nicht gut** mit den Geräten und Messengern **aus**?  
Dann ist es besser, einen **bekannten Messenger** zu benutzen.



Bei Problemen kann dann leicht eine andere Person Ihrem Chatpartner helfen.

- **Sprechen** Sie **mit** Ihren **Chatpartnern**, **welchen Messenger** Sie alle benutzen wollen.



- Denn: Die meisten Messenger können keine Nachrichten von einem Messenger zu einem anderen Messenger schicken.



➤ **Tipp**

Sie können auch **mehrere Messenger benutzen**.

Zum Beispiel:

- Einen nicht so sicheren Messenger für Informationskanäle.
- Einen sicheren Messenger für Ihre privaten Nachrichten.

**Tipp**

➤ **Informieren** Sie sich **über** die **Messenger**, die Sie vielleicht nehmen wollen.

**Tipp**

➤ Achten Sie besonders auf diese Punkte:

- **Wo sitzt** (*ist*) der **Anbieter** (*Firma*) vom Messenger? Denn: Es gelten meistens (*so muss es gemacht werden*) die Regeln für den Schutz von Ihren Daten (*Informationen über Sie*) von dem Land, in dem der Anbieter vom Messenger sitzt. Am sichersten ist es, wenn der Anbieter in Deutschland, in der EU (*Europäischen Union*) oder in der Schweiz sitzt.



- Sind die **Programme für den Messenger und für die Verschlüsselung öffentlich**?

Das heißt: Kann jeder diese Programme lesen und **prüfen**?

Dann können **Experten** (*Personen, die viel über etwas wissen*) sehen:

- Was machen die Programme?
- Sind die Programme sicher?

Programme sind **öffentlich**, wenn Sie so etwas lesen:

- Die Programme sind „**Open Source**“.
- Oder: Der „**Quellcode**“ ist **öffentlich** oder veröffentlicht.



- Wichtig ist auch:

**Wie finanziert** sich der **Messenger** (*woher bekommt er Geld*)?



- Meistens sind Messenger **sicherer**, wenn sich die Messenger mit **Spenden** (*geschenktem Geld*) finanzieren.



- Oder: Wenn Sie eine Gebühr (*Geld*) für das Benutzen von einem Messenger bezahlen müssen.
- Dann verkaufen die Messenger meistens keine Informationen.

- 
- Sehr wichtig ist auch:

- Ist der **Messenger mit** einem **sozialen Netzwerk verknüpft** (*verbunden*)?  
Zum Beispiel der Facebook-Messenger.
- **Oder** ist der Messenger **mit** einem **großen Internet-Konzern** (*großer Firma im Internet*) verknüpft?  
Zum Beispiel Google Hangout mit Google.



- Dann gibt es die **Gefahr**, dass die **Informationen** vom Messenger mit den Informationen vom Netzwerk oder Internet-Konzern **zusammengebracht** werden.  
Daraus lassen sich zusätzliche (*noch mehr*) Informationen über Sie herausfinden.



- 
- **Lesen Sie die Allgemeinen Geschäftsbedingungen und die Datenschutzerklärungen.**

**Tipp**

- Das ist schwer.  
Aber: Darin finden Sie wichtige Informationen zur Sicherheit und zur Privatsphäre.
-

- Eine **Übersicht über** verschiedene **Messenger** finden Sie bei:



- der „Verbraucherzentrale“  
<https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/whatsappalternativen-messenger-im-ueberblick-13055>
- und bei „MOBILSICHER“.  
<https://mobilsicher.de/ratgeber/verschluesselt-kommunizieren-per-app>

Leider sind diese Informationen nicht in Leichter Sprache geschrieben.

- Bei der Verbraucherzentrale finden Sie auch eine **Tabelle mit den Eigenschaften** von Messengern.  
[https://www.verbraucherzentrale.de/sites/default/files/2021-01/Messenger-Vergleiche\\_Tabelle\\_2021\\_VZNRW.pdf](https://www.verbraucherzentrale.de/sites/default/files/2021-01/Messenger-Vergleiche_Tabelle_2021_VZNRW.pdf)

- Die wichtigsten **Eigenschaften** zu den 3 bekanntesten **Messengern** haben wir für Sie aufgeschrieben. Dann können Sie leichter entscheiden, welcher bekannte Messenger zu Ihnen passt.




---

- **WhatsApp:**

- Sie können WhatsApp **kostenlos** benutzen.
- WhatsApp ist der Messenger mit den **meisten Nutzern**.



- Und: Viele **Kriminelle** (*Personen, die etwas gegen die Gesetze tun*) benutzen WhatsApp. Auch viele Personen, die **unwahre** (*nicht richtige*) **Sachen** schreiben und sagen, benutzen WhatsApp. Deshalb **Vorsicht bei Nachrichten** über WhatsApp von Personen, die Sie nicht aus dem normalen Leben kennen.   

- WhatsApp können Sie:
  - **Auf** vielen **Smartphones mit** den Betriebssystemen **Android und iOS** benutzen. 
  - Und parallel auch **auf Computern mit Windows und** Computern von **Apple** benutzen.
  - Auf älteren Smartphones funktioniert WhatsApp manchmal nicht mehr.
- Die Nachrichten haben eine **Ende-zu-Ende-Verschlüsselung**. WhatsApp benutzt die Verschlüsselungsprogramme von Signal. Diese Programme sind Open-Source. Das heißt: Die Programme sind öffentlich.
- **Links** (*Adressen von Internetseiten*) werden **nicht verschlüsselt**. 
- Es werden **viele Metadaten** gebraucht und benutzt. Die Metadaten werden **nicht verschlüsselt** und sie werden **gespeichert**.
- Alle **Kontakte aus dem Telefonbuch** von Ihrem Gerät werden **gelesen** und **gespeichert**.
- WhatsApp gehört **zum Facebook-Konzern**.

- Die **Informationen** von den Nutzern von WhatsApp werden **mit den Informationen von anderen Facebook-Diensten** zusammengebracht.
- Auch Experten wissen nicht genau, ob WhatsApp Informationen über seine Nutzer verkauft. Die Allgemeinen Geschäftsbedingungen sagen das nicht klar.
- Der Sitz von WhatsApp ist in den **USA**.



## ➤ Telegram:

- Sie können Telegram **kostenlos** benutzen.
- **Viele Nutzer** benutzen Telegram.
- Und: **Viele Kriminelle** benutzen Telegram. Auch viele Personen, die **unwahre Sachen** schreiben und sagen, benutzen Telegram.
- Deshalb **Vorsicht bei Nachrichten über Telegram** von Personen, die Sie nicht aus dem normalen Leben kennen.
- Telegram können Sie:
  - **Auf Smartphones** mit den Betriebssystemen **Android und iOS** benutzen.
  - Und parallel **auch auf Computern mit Windows** und auf **Apple-Computern** benutzen.
- Die **Nachrichten** haben **normal nur** eine **Transportverschlüsselung**.
- Auch die **Gruppenchats** haben eine **Transportverschlüsselung**.



- **Achtung:** Unbekannte **Personen** können auch **anonym** (*ohne zu sagen, wer sie sind*) in eine Gruppe eintreten. **Sie wissen also nicht, welche Personen in einer Gruppe sind.** 
- Sie können **mit einzelnen Chatpartnern Ende-zu-Ende verschlüsselt** kommunizieren. Die Ende-zu-Ende-Verschlüsselung müssen Sie und Ihr Chatpartner **extra einstellen**. Das finden Sie **bei den Einstellungen** bei den Worten „**Secret Chats**“ . 
- Für **Gruppenchats** gibt es **keine Ende-zu-Ende-Verschlüsselung**. 
- **Achtung!** Telegramm **speichert** alles, was Sie auf Ihrer Tastatur **tippen** (*schreiben*). Auch wenn Sie die Nachricht nicht abschicken. 
- Die **Programme** zum Funktionieren und für die Verschlüsselung sind **nicht alle öffentlich**. 
- **Was** Telegram mit den **Metadaten** macht, ist **unbekannt**. 
- **Alle Kontakte** aus dem Telefonbuch von Ihrem Gerät werden **gelesen** und **gespeichert**. 
- Telegram gehört **nicht zu** einem großen **Internetkonzern**. 
- 2 russische Brüder haben Telegramm gegründet.
- Es ist **nicht genau bekannt**, wie Telegram sich **finanziert**.

- Der **Sitz** von Telegram ist **nicht** genau **bekannt**.  
Experten denken, dass der Sitz in  
den Arabischen Emiraten ist.
- 

## ➤ **Signal:**

- Signal hat noch **nicht so viele Nutzer**.  
Aber: In der letzten Zeit sind viele Nutzer  
von WhatsApp zu Signal gewechselt (*gegangen*).
- Sie können Signal **kostenlos** benutzen.
- Signal können Sie:
  - **Auf Smartphones** mit den Betriebssystemen  
**Android und iOS** benutzen.
  - Und parallel auch **auf Computern mit Windows**  
**und auf Apple-Computern** benutzen.
- Alle **Nachrichten** und **Gruppenchats** sind normal  
**Ende-zu-Ende verschlüsselt**.
- Die **Verschlüsselung** ist **sehr gut**.  
Einige andere Messenger benutzen auch  
die sehr gute Verschlüsselung von Signal.
- Alle **Programme** sind Open Source, also **öffentlich**.
- Es werden nur **wenige Metadaten** gebraucht.  
Die Metadaten werden nur **verschlüsselt benutzt**  
und **nicht gespeichert**.
- Alle **Kontakte aus dem Telefonbuch** von Ihrem Gerät  
werden **gehasht** (*besonders verschlüsselt*) und  
nur gehasht damit gearbeitet.
- Signal gehört **nicht zu** einem großen **Internetkonzern**.
- Signal wurde von Personen gegründet,  
die einen sicheren Messenger haben wollten.



- Signal bekommt **Spenden** und **Förderungen** (*Unterstützung / Hilfen*).
  - Der Sitz von Signal **ist** den **USA**.
- 

- Es gibt noch andere **Messenger**, die nur **wenige Nutzer** haben:
- **Manche** von diesen **Messengern** sind **sehr sicher**. **Manche** sind **nicht so sicher**.
- Die **meisten** von diesen Messengern sind auch **kostenlos**.
- Einige Messenger haben ihren Sitz **in Deutschland oder in der Schweiz**.



- Wir schreiben Ihnen einige Beispiele von Messengern auf.

Gute Informationen zu diesen Messengern finden Sie bei „CHIP“ und „MOBILSICHER“.



Leider sind die Informationen zu diesen Messengern nicht in Leichter Sprache geschrieben.

- **Threema:** <https://mobilsicher.de/ratgeber/messenger-app-threema-kurz-vorgestellt-2>
  - **Wire:** <https://mobilsicher.de/ratgeber/messenger-app-wire-kurz-vorgestellt>
  - **Viber:** <https://mobilsicher.de/apps/viber-telefonie-und-messenger-app>
  - **Ginglo:** <https://mobilsicher.de/ratgeber/messenger-app-simsme-kurz-vorgestellt>
  - **Element:** [https://www.chip.de/artikel/Besser-als-WhatsApp-die-3-sichersten-Messenger\\_183110977.html](https://www.chip.de/artikel/Besser-als-WhatsApp-die-3-sichersten-Messenger_183110977.html)
-

- Denken Sie daran, wenn Sie sich für einen Messenger entschieden (*überlegt*) haben:
  - **Laden** Sie den Messenger nur **herunter**:
    - **aus dem App-Store** von Ihrem Gerät: aus dem Google-Play-Store oder aus dem App-Store von Apple
    - **oder von den Original-Internetseiten** vom Messenger.


 A blue rectangular box with the word "Tipp" in white text.

- **Wenn Sie WhatsApp nicht mehr benutzen wollen:** Es **reicht nicht** (*ist nicht genug*), wenn Sie WhatsApp auf Ihren Geräten **deinstallieren** (*löschen*). Ihr **Account** (*Konto*) **bleibt** dann immer noch bei WhatsApp.



- Wie Sie Ihren **WhatsApp-Account löschen** können, können Sie lesen bei:
  - der „Verbraucherzentrale“: <https://www.verbraucherschutz.com/anleitungen/whatsapp-loeschen-android-und-iphone-anleitung/>
  - oder bei „Mobilsicher“: <https://mobilsicher.de/ratgeber/nase-voll-whatsapp-konto-loeschen>

***Blieben Sie sicher und privat – immer.***