

# Messenger

Ein Überblick über verschiedene Messenger

- [Matrix](#)
  - [Was ist Matrix und warum nutzen wir es?](#)
  - [Der Matrix beitreten](#)
  - [Navigation & Tipps und Tricks](#)
  - [Glossar](#)
- [Signal](#)
  - [Warum Signal benutzen?](#)
  - [Signal sicher verwenden](#)
  - [Referenzen](#)

# Matrix

# Was ist Matrix und warum nutzen wir es?

## Matrix

Matrix ist ein **dezentrales**, *föderiertes* Kommunikationsprotokoll. Damit ist es im Prinzip wie E-Mail, nur moderner und mit viel mehr Möglichkeiten.

- **Dezentral:** Jedes kann einen eigenen Server betreiben. Es gibt also keine zentrale Organisation, die alle Server kontrolliert.
- *Föderiert:* Die Server können miteinander kommunizieren. Menschen müssen also nicht alle auf den selben Servern angemeldet sein, um miteinander kommunizieren zu können.

**Stark gegen Zensur:** Der dezentrale Aufbau ist besonders dann von Vorteil, wenn Dienste in Ausnahmezuständen von Regierungen blockiert werden sollen.

- [01/2022 in Kasachstan](#)
- [10/2022 im Iran](#)

## Was kann Matrix?

Matrix bietet Möglichkeiten eure Kommunikation auf einer Plattform zu bündeln und dadurch eure Zusammenarbeit zu optimieren.

- **private Ende-zu-Ende verschlüsselte Räume**
- **öffentliche Räume** (unverschlüsselt, kann nachträglich aktiviert werden)
- **Text, Links, Bilder, Videos, Sprachnachrichten, Umfragen**
- **Formatierung** mit [Markdown](#) (Wie diese Anleitung) => [Tutorial](#), [Cheat-Sheet](#)
- **verschlüsselte Sprach- und Videokonferenzen**
- **Spaces** als Ordner für Räume, damit ihr Arbeitsgruppen bilden könnt
- **Andere Programme, Messenger und Webseiten einbinden** wie z.B. Pads, Telegram, Signal, Blog-Feeds oder E-Mail-Newsletter.

## Was kann Matrix (noch) nicht?

- **Metadaten** (Zeitpunkte, Kommunikationspartner\*innen...) verschleiern
- **Verschwindende Nachrichten**, die sich selbst löschen

- **Große Dateien** > 100MB versenden

### Alternativen:

Metadaten verschleiern	Verswindende Nachrichten	Große Dateien senden
cwtch.im	signal.org	kiki.lecomitedeschats.com
jami.net	bin.disroot.org	upload.disroot.org
<a href="#">simplex.chat</a>	paste.systemli.org	onionshare.org
briarproject.org	pb.envs.net	file.io

## Datenschutz-Hinweis

Die Ende-zu-Ende-Verschlüsselung verhindert zwar, dass ohne Zugriff auf ein Endgerät Überwachende eure Nachrichten lesen können, es ist aber - wie bei fast allen anderen Online-Aktivitäten auch - trotzdem möglich zu überwachen welcher Account mit wem wann kommuniziert hat ([siehe Metadaten](#)). Ihr könnt eure IP-Adresse verschleiern, indem ihr ein [VPN](#) oder [Tor](#) benutzt, dann lassen eure Metadaten weniger Rückschlüsse auf eure Identität zu. Bei manchen Servern ([z.B. Systemli](#), [Hackliberty](#)) ist dies nicht notwendig, weil die IP-Adresse nicht gespeichert wird.

**Beispielraum** *All Cats Are Beautiful*: @Alice:matrix.org -- @Bob:systemli.org -- @Carol:systemausfall.org => Der Chatverlauf liegt hier auf allen drei Servern (verschlüsselt), sowie auf allen Endgeräten von Alice, Bob und Carol, die eingeloggt sind (verschlüsselt, zusammen mit den Schlüsseln). Eure Endgeräte sind also der beste Angriffspunkt um eure Nachrichten zu lesen.

# Der Matrix beitreten

## Zusammenfassung von Oben

Matrix ist wie **E-Mail in modern**. Ein gutes Tool um damit unverschlüsselte **E-Mail-Listen** oder **Telegramgruppen** zu ersetzen, da es mehr **Verschlüsselung und Datenschutz** bietet. Es ist **einfacher** einen Matrix-Raum zu erstellen als eine E-Mail-Liste. Es braucht **keine Telefonnummern** und **kein Smartphone** und ihr habt **freie Server-Wahl**.

Um **Metadaten** zu verschleiern und für **verschwindende Nachrichten** würde ich **Signal** oder [andere Alternativen](#) empfehlen, weil es schwer ist **Chats** aus Matrix komplett **zu löschen** - der beste Weg ist, wenn alle aus einem Raum rausgehen und ihn vergessen, weil dann niemand mehr Zugriff auf die verschlüsselten Nachrichten hat. Irgendwann löschen die Server sie dann automatisch.

## 1. Einen Server auswählen

Um dich zu registrieren, musst du einen von mittlerweile über 40.000 "Homeservern" (siehe [Glossar](#)) auswählen. Dieser ist vergleichbar mit deinem Email-Anbieter.

### Empfehlungen:

- [chat.livingutopia.org/#/register](https://chat.livingutopia.org/#/register)
- <https://systemausfall.org/kontoanfrage> (Nachrichten werden [nach 1 Jahr gelöscht](#))
- <https://hackliberty.org/register>
- <https://registration.matrix.catgirl.cloud/>
- <https://users.systemli.org/en/register> (Du brauchst einen Einladungscode)
- [einen eigenen Server hosten](#)

### Eine E-Mail-Adresse muss angegeben werden:

- <https://element.envs.net/#/register>
- <https://element.gemeinsam.jetzt/#/register>
- <https://element.matrix.im/#/register>

## 2. Verschlüsselung einrichten

Das Verschlüsselungssystem von Matrix basiert auf **Cross-Signing**. Das heißt, jedes Mal, wenn du dich einloggst, musst du mit einem anderen Gerät oder einem Passwort **verifizieren**, dass du auch wirklich du bist. Erst dann hast du **Zugriff** auf verschlüsselte **Nachrichten**. Das ist ähnlich wie PGP-Verschlüsselung, nur leichter zu benutzen.

Damit Verschlüsselung immer in allen **Sitzungen** (siehe [Glossar](#)) funktioniert, solltest du ein **per Passwort verschlüsseltes Backup** auf deinem Homeserver einrichten.

### 1. Klicke auf: Profilbild > Einstellungen > Sicherheit > Sicheres Backup

Eingegebenes Passwort eingeben (Bild)

**2. Alles abspeichern:** Den angezeigten Schlüssel und das eingegebene Passwort kopieren und in einem Passwort-Manager abspeichern - Empfehlung: [KeepassXC](#), [KeepassDX \(Android\)](#), [Keepassium \(iOS\)](#).

**Bei Verlust** kannst du alte verschlüsselte Nachrichten nicht mehr **lesen**, weil deine Schlüssel fehlen (neue aber schon)! Zudem können andere sehen, dass du dich **nicht verifiziert** hast, und werden dir gegebenenfalls nicht mehr **Vertrauen**. Unter [Verschlüsselung](#) steht, was du in so einem Fall tun kannst, um deinen Account zu retten.

## 3. Client Installieren

**Clients** (siehe [Glossar](#)) werden wie E-Mail-Clients unabhängig vom Chat-Protokoll entwickelt und unterstützen deshalb nicht alle die selben Features.

### Empfehlungen

- **[Element](#):** Empfehlung, wenn du mit deiner Gruppe auf Matrix wechselst und alle Features nutzen möchtest. Kein Multi-User-Support. => hat eine [gute Bedienungsanleitung](#)

Ich empfehle anfangs Element auszuprobieren, um einen Überblick zu bekommen was alles möglich ist. Andere Clients sind Datenschutzfreundlicher haben aber keine [Integrationen](#).

### Alternativen

- **[FluffyChat](#):**  
Empfehlung, wenn du vor allem mit deinen Freund\*innen chatten und/oder mehrere Accounts gleichzeitig nutzen möchtest. Hat eine Oberfläche, die an Signal erinnert.
- **[Cinny](#):** Empfehlung wenn du einen Client möchtest, der wie Slack, RocketChat oder Mattermost aussieht. Nur für Desktop verfügbar. Keine Sprach-Anrufe.

[Liste mit weiteren Clients](#) & [Feature-Übersicht](#). Wähle mit Bedacht, die Sicherheit deiner Kommunikationspartner\*innen und deine Möglichkeiten hängen davon ab.

## 4. Kontakt aufnehmen

**Per Matrix-ID:** Nun kannst du deine Matrix-ID (siehe [Glossar](#)) teilen und warten bis du eingeladen wirst. `@username:homeserver.tld`

**Per Einladungslink (matrix.to):** Dein persönlicher Einladungslink ist `https://matrix.to/#/` gefolgt von deiner Matrix-ID:

`https://matrix.to/#/@username:homeserver.tld`

# Navigation & Tipps und Tricks

Du hast es geschafft? Glückwunsch! ☺ Falls du nach dem Lesen immernoch Probleme hast, oder du **Hilfe** für deine Gruppe möchtest - egal ob [Bridges](#) oder komplexere [Spaces](#) **einrichten**, schreib mir gerne eine Mail ☺ Auch Feedback, Änderungsvorschläge und Übersetzungen gerne per Mail an [helpmewithmatrix@riseup.net](mailto:helpmewithmatrix@riseup.net) ([PGP-Key](#))

Weiter mit einer kurzen **Einführung**

## Räume

Alle Chats, egal wie öffentlich - egal ob Kanal oder Gruppe, sind in Matrix **Räume**. Alle Räume können entweder verschlüsselt oder unverschlüsselt genutzt werden. Für **Private** Räume und Direktnachrichten ist die Verschlüsselung **standardmäßig** aktiviert. Bei **öffentlichen** Räumen kannst du die Verschlüsselung **nachträglich** aktivieren - bedenke aber, dass der Chatverlauf dann nicht sichtbar ist wenn Menschen beitreten.

## Private Räume

**Direktnachrichten (in manchen Clients so genannt):** Das sind Chats zwischen zwei Accounts - sie können jederzeit um weitere Accounts erweitert werden, und werden dann automatisch zu privaten Räumen.

**Private Räume:** Der Standard, wenn du einen Raum erstellst. Alle müssen manuell eingeladen werden, du kannst einen **Raumnamen und -Thema** festlegen und viele Einstellungen vornehmen.

## Öffentliche Räume

### "Space-Räume"

Diese Räume sind für alle in einem [Space](#) sichtbar. Dies geht sowohl für öffentliche, als auch vormals private Räume. Zuerst musst du die Räume einem Space **hinzufügen**, das machst du



über das jeweilige Space-Menü. Dann stellst du in jedem Raum den **Raumzugang** über die Einstellungen auf "für den Space sichtbar". **Einfacher** ist es **erst** den Space zu erstellen, und dann direkt im Space solche Räume zu erstellen.

### Versteckte Räume mit Einladungslink:

Diese Räume haben nur einen menschlich nicht lesbaren Einladungslink, die `!raum-id` wirkt dabei wie ein **Passwort**: `https://matrix.to/#/!raum-id:homeserver.domain` Du erstellst so einen Raum, indem du einen **privaten** Raum erstellst, und ihn **danach** auf Öffentlich umstellst. Das hat zudem den Vorteil, dass er dann **verschlüsselt** ist und somit einer Signal-Gruppe mit Link ähnelt. Den Einladungs-Link erhältst du wenn du in der Raumbeschreibung rechts oben auf das Teilen-Symbol gehst (Element/Smartphone). **Beachte:** Dieser Raum ist in Spaces auch allen im Space zugänglich!

### Lokal öffentlich zugängliche Räume:

Diese Räume haben einen menschlich lesbaren Alias als Einladungs-Link, der sie über das Raumverzeichnis auf dem eigenen Homeserver sichtbar macht, worüber sie gefunden werden können: `https://matrix.to/#/#raumname:homeserver.domain` Der Raum kann von anderen Homeservern aus betreten werden, wenn Menschen den **genauen** Link kennen. In diesem Fall fungiert also der `#raumname` als (meist schwaches) Passwort. **Beachte:** So einen Raum zu erstellen, bedeutet, dass er **allen** Menschen auf dem Server einfach zugänglich ist. Ein Raum kann auf **mehreren** Servern so eingestellt sein. Dafür brauchst du Accounts auf jedem der Server.

### Global (wirklich komplett öffentlich):

Diese Räume haben einen Alias, der im **öffentlichen Raumverzeichnis** von matrix.org veröffentlicht ist. Dort kann der Raum von **allen** Homeservern aus eingesehen werden, und über **Suchmaschinen** (also auch im Browser) gefunden werden. Du erstellst so einen Raum, in dem du den Haken bei "im Raumverzeichnis veröffentlichen" setzt.

**Kanäle (nur bestimmte Menschen können senden):** Hierfür stelle in den Einstellungen unter **Raum-Berechtigungen** die Berechtigung zum Nachrichten senden auf "Admin", und befördere alle die senden dürfen sollen.

Kanäle in Matrix haben einen entscheidenden **Datenschutz-Mangel**: **Alle** können sehen wer wann was **gelesen** hat und **wer im Kanal** ist, und es gibt keine Möglichkeit anonym zu posten, außer mit Extra dafür registriertem Account. Ich würde stattdessen **Telegram** empfehlen, evtl. mit [Bridge](#) in einen versteckt öffentlichen Raum in eurem Space.

# Spaces

Spaces können benutzt werden um Räume besser zu organisieren. Alle im Space können alle Räume sehen, die dafür zugänglich sind und frei ein- und austreten - wie Räume in einem **Seminarhaus**. Spaces können so eine **Community** oder eine **Gruppe** abbilden, in der alle

Menschen sind die dazu gehören, um sich in **Arbeitsgruppen** oder **themenbezogenen** Räumen auszutauschen und zu **organisieren**.

**Personal Spaces:** Optimiert für dich. Nur du kannst sie sehen.

**Private Spaces:** Optimiert für Gruppen. Alle müssen eingeladen werden.

**Öffentliche Spaces:** Optimiert für Communities. Es gibt einen Einladungslink.

**Tipps:** Wenn ihr mit Spaces anfangt, erstellt einfach einen privaten, fügt darin einen Hauptraum hinzu und dann lasst das ganze organisch wachsen, je nach Bedürfnissen.

**Fun Fact** gefällig? Spaces sind auch nur eine Abwandlung von [Räumen](#) ☐ Daraus folgt, dass fast alles was auf Räume zutrifft, auch auf Spaces zutrifft :) Deshalb hab ich mich hier kurz gehalten - hier sind [noch ein paar Infos](#).

## Räume im Space erkunden

**Element auf dem Handy:** Klicke auf das Space-Menü (Drei Kacheln + Kreis rechts unten), dann lange auf den Space und dann auf "Räume erkunden (und verwalten)" => das #-Symbol mit der Lupe. **Element auf dem Laptop:** Klicke ganz links mit Rechtsklick auf den Space, dann auf "Räume erkunden und verwalten" => das #-Symbol mit der Lupe.

## Verschlüsselung

Die **Ende-zu-Ende-Verschlüsselung** sorgt dafür, dass Nachrichten wirklich nur von denen gelesen werden können, für die sie bestimmt sind. Das setzt voraus, dass die **Schlüssel** nur auf den Endgeräten vorhanden sind. So weit - so gut. Sobald mehrere Endgeräte (**Sitzungen**) ins Spiel kommen, wirds tricky, denn dann müssen Schlüssel von einem Gerät aufs andere übertragen werden. Ein **Schlüssel-Backup** hilft dir dabei.

**Zum Einrichten und Verstehen (mit Screenshots):**

- <https://samuels-blog.de/sichere-chats-mit-matrix-matrix-teil-2/#cross-signing>
- <https://doc.matrix.tu-dresden.de/encryption/>
- [https://matrix-help.envs.net/first-steps/#convenient\\_use\\_of\\_end-to-end\\_encryption\\_e2ee](https://matrix-help.envs.net/first-steps/#convenient_use_of_end-to-end_encryption_e2ee)

**Hilfe!** Ich habe das Passwort für das Schlüssel-Backup verloren und mein Handy ist kaputt gegangen, jetzt komm ich nicht mehr an meine Nachrichten und alle denken ich wurde gehackt - weil ich natürlich nicht den [Passwort-Manager](#) benutzt habe! ☐

**Schritte um dich zu verifizieren:**

1. **Klicke auf:** Profilbild > Einstellungen > Sicherheit > Sitzungen (evtl. musst du suchen)
2. Melde deine alten Sitzungen ab, indem du dein Login-Passwort eingibst.
3. Richte das [Schlüssel-Backup](#) neu ein (siehe auch Anleitungen oben).

# Sprach- und Videoanrufe

Matrix unterstützt verschlüsselte **Sprach-Anrufe** sowie **Videokonferenzen** via [Jitsi](#). Es ist möglich ganze **Plena inklusive Call und Pad** via Matrix zu halten. → [Anleitung](#)

# Integrationen

Für Integrationen wird ein Integrationsmanager benötigt. Von deinem Home-Server wird meist bereits ein Integrationsmanager mitgeliefert, dieser heißt bei matrix.org `scalar.vector.im` (Böse). Wenn du auf einem anderen Server bist, heißt dieser meist `dimension.homeserver.tld` (Gut). Hier findest du [mehr Infos darüber, welche Meta-Daten auf dem Server anfallen wenn du Integrationen nutzt](#).

# Widgets

Ein Widget ist ein **Ausschnitt** einer App, die in einem anderen Programm angezeigt wird. Ihr kennt das vielleicht vom Startbildschirm eures Handys. In Element könnt ihr zu einem Raum z.B. ein **Pad** hinzufügen, und dort eure **Protokolle** ablegen. Es funktioniert gut mit [Etherpad](#) (unverschlüsselt) und [CryptPad](#) (verschlüsselt, rote Box beachten!). → Zur [Cryptpad-Einführung](#).

# Wie nutze ich Widgets?

**1. Aktivieren: Avatar > Einstellungen > Allgemein > "Integrationen verwalten"** **2. Laptop (Element):** In Räumen rechts oben das kleine **i** > Widgets verwalten. **2. Handy (Element):** Rechts oben im Raum auf die drei Punkte klicken > Integrationen verwalten. **3. Custom Widget** hinzufügen und Link eures Pads einfügen.

Wenn du Widgets nutzt, ist die URL der eingebundenen Webseite **nicht Ende-zu-Ende-verschlüsselt**. Bei z.B. Croodle-Umfragen oder **Cryptpads** wird das Passwort für die Verschlüsselung **im Link** mitgesendet, was bedeutet das Passwort mit den **Admins aller beteiligten Homeserver** eines Raumes zu teilen. In CryptPad kannst du ein **zusätzliches Passwort** festlegen. Dies ist in diesem Fall sinnvoll!

Die Webseite, die als Widget eingebunden wird, kann deine **IP-Adresse** sehen. Das wäre aber auch der Fall, wenn du die Webseite einfach im Browser aufrufst ☐☐.

# Bots

Bots sind Programme, die innerhalb eines Matrix-Raumes **Nachrichten senden** können. Du kannst z.B. [Blogposts](#) oder [E-Mail-Newsletter/Listen](#) in einen Raum integrieren.

- <https://t2bot.io/>
- <https://hilfe.systemausfall.org/matrix/features/> (Nur für systemausfall.org Accounts)
- <https://matrix.org/bots/>

Es macht aus **Datenschutz**-Gründen Sinn, dies in einem **Extra-Raum** zu tun, weil Bots eure Nachrichten lesen & an den Server übermitteln (auch verschlüsselte).

# Bridges

Bridges zu anderen Kommunikations-**Protokollen** ermöglichen, dass von einem Matrix-Raum aus mit Gruppen und Channels auf Telegram, Signal, Mattermost und **vielen weiteren Plattformen** kommuniziert werden kann, meist in **beide Richtungen**.

- <https://hilfe.systemausfall.org/matrix/telegram/> (nur für systemausfall.org)
- <https://hilfe.systemausfall.org/matrix/signal/> (nur für systemausfall.org)
- <https://gitlab.com/etke.cc/postmoogle>
- [einen Server mieten \(inkl. Bridges\)](#)
- <https://matrix.org/bridges/>

**Verschwindende Nachrichten** auf Telegram oder Signal werden damit **hinfällig**, weil sie auf Matrix-Server verteilt werden!

# Weitere Ressourcen/Links

- Einführung: <https://matrix.org/faq/#intro>
- Matrix-Wikis:
  - <https://doc.matrix.tu-dresden.de/>
  - <https://matrix-help.envs.net/>
  - <https://element.io/help>



# Glossar

- **matrix.org**: Die Organisation, die das Projekt leitet und den größten Homeserver bereitstellt, genau wie Gmail den E-Mail-Verkehr dominiert. Dort einen Account zu haben ist nicht notwendig und nicht zu empfehlen.
- **Matrix**: Das Protokoll, mit dem du kommunizierst. Ähnlich wie E-Mail.
- **Homeserver**: Dein Matrix-Server. Ähnlich wie dein E-Mail-Anbieter.
- **Matrix-ID**: Deine einzigartige Adresse, mit der du gefunden werden kannst.  
`@username:homeserver.topleveldomain`. Ähnlich wie deine E-Mail-Adresse.
- **Top-Level-Domain (tld)**: Der letzte Teil einer Domain, z.B. `.com, .org, .de, .chat, .im`
- **Client**: Eine App um Matrix-Nachrichten zu lesen. Ich empfehle dir einen Client auf dem Handy oder PC zu installieren. Es gibt aber auch Clients, die du aus dem Browser nutzen kannst.
- **Sitzung**: Jedes mal wenn du dich neu einloggst, erstellst du eine Sitzung. (z.B. Browser + Handy + Laptop)
- **Element**: Einer von vielen Matrix-Clients. Element ist auf fast allen Betriebssystemen verfügbar und ist der am weitesten entwickelte Client. Vergleichbar mit Thunderbird für E-Mail.
- **Raum**: Das, was in anderen Messengern Channel oder Gruppe heißt.
- **Space**: Ein Ordner für Räume. Räume können so eingestellt werden, dass alle im Space die Räume sehen und beitreten können. Du kennst das vielleicht von Slack, RocketChat, Mattermost, Discord, etc.

# Signal

# Warum Signal benutzen?

[Signal](#) ist ein Messenger mit Fokus auf Sicherheit und Datenschutz. Signal ist einfach zu installieren und leicht zu verwenden, da es sehr ähnlich wie weit verbreitete Messenger (Whatsapp, Telegram) funktioniert. Hinter Signal steht eine gemeinnützige Firma ohne Profitinteresse.

## Anrufe & SMS sind unsicher

Mit richterlichem Beschluss bekommt die Polizei sehr leicht Zugriff auf alle SMS-Inhalte sowie Telefon-Metadaten (wer wann mit wem telefoniert hat). Das passiert über den Provider und ihr könnt es nicht bemerken. Schlechter Empfang oder komische Geräusche sind kein Zeichen von Überwachung. Falls ein Beschluss zur Überwachung eurer Telefonate vorliegt, wird fast immer die normale Telekommunikationsüberwachung (TKÜ) eingesetzt. Das bedeutet, dass Ende-zu-Ende-verschlüsselnde Messenger-Apps einschließlich Signal weiterhin sicher sind, solange keine Quellen-TKÜ eingesetzt wird (sehr selten). Auch auf das Mikro und die Kamera vom Handy hat die Polizei nur bei Quellen-TKÜ Zugriff, nicht bei normaler TKÜ.

## Signal Installieren

1. Installiere die [Signal App](#) aus dem Appstore/Playstore.

Falls du ein Android Handy ohne Playstore verwendest, kannst du auch direkt die [APK](#) herunterladen.

2. Zur Registrierung benötigst du eine Telefonnummer



# Signal sicher verwenden

Signal ist an sich bereits deutlich sicherer als andere Messenger. Allerdings gibt es noch einige Dinge die du bei der Verwendung beachten solltest.

## Signal-Username verwenden

Um nicht deine Telefonnummer preisgeben zu müssen, kannst du bei Signal einen Usernamen einrichten:

**Android:** 3-Punkt-Icon -> Einstellungen -> Auf's Profilbild klicken -> @Nutzername

**IOS:** Profil-Icon -> Einstellungen -> Auf's Profilbild klicken -> @Nutzername

Zum teilen kannst du entweder das Kürzel (@abcd.1234), den Link oder den QR Code verwenden. Du kannst den Usernamen jederzeit wieder löschen und einen neuen vergeben.

## Pin und Registrierungssperre

Es ist wichtig, dass du in Signal eine PIN einrichtest. Diese schützt vor unberechtigter Neuregistrierung. Dein Netz-Provider muss auf richterlichen Beschluss hin SMS an die Polizei umleiten. Ohne PIN kann die Polizei Signal mitlesen - aber das merkst du, weil du dann selbst aus Signal rausfällst: es kann nur ein Handy bei Signal registriert sein.

**Android:** 3-Punkt-Icon -> Einstellungen -> Konto -> Registrierungssperre

**IOS:** Profil-Icon -> Einstellungen -> Konto -> Registrierungssperre

## Verschwundene Nachrichten

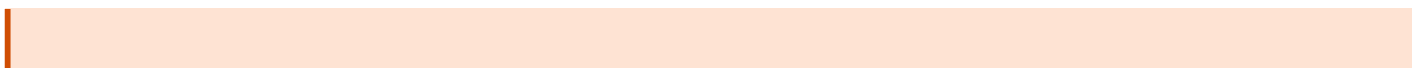
Falls dein Handy doch mal im entsperrten Zustand in die falschen Hände gerät, kannst du den Schaden eingrenzen, indem du die Chat-Historie auf ein paar Tage/Wochen begrenzt.

**Android:** 3-Punkt-Icon -> Einstellungen -> Datenschutz -> Standardablaufzeit für Chats

**IOS:** Profil-Icon -> Einstellungen -> Datenschutz -> Standardablaufzeit für Chat

## Gruppen einrichten

### Gruppen Links



Über Einladungs Links wird die Gruppenbeschreibung geteilt. Wenn der Link in die falschen Hände gerät, werden auch alle Informationen aus der Beschreibung preisgegeben!

## Proxy verwenden, Snowflake

Signal

# Referenzen

<https://ssd.eff.org/module/how-to-use-signal>

<https://wiki.letztegeneration.org/de/oeffentlich/AGs/IT-Hilfe/Signal/Signal-sicher-benutzen>

<https://activisthandbook.org/tools/chat-apps/signal>