Signal - Messenger

- Überblick (Vor-/Nachteile, Fazit und Tricks)
- Warum Signal benutzen?
- Signal sicher verwenden
- Referenzen
- Verschwindende Nachrichten (Funktionsweise)

Überblick (Vor-/Nachteile, Fazit und Tricks)

> Auf dieser Seite findest du eine Übersicht der Vor- und Nachteile von Signal, sowie ein Fazit für welche Anwendungsfälle es gut geeignet ist und welche Tricks es gibt um häufig auftretende Probleme zu umgehen :)

Vorteile:

- Vergänglichkeit: verschwindende Nachrichten & temporäres Speichern auf Servern
- Daten-Sicherheit: Ende-zu-Ende-Verschlüsselung & Open Source Software
- Zugänglichkeit - klassisches, einfaches Design mit vielen Features
- Bekanntheit - 12% in DE, in sozialen Bewegungen weltweit stark verbreitet
- Stabilität - Funktioniert seit 10 Jahren, steht auf relativ soliden Beinen, Spenden ist gut
- Dokumentation - Eine der besten Dokumentationen für Messenger, die es gibt
- Anonymität - Keine Metadaten-Leaks möglich & Telefonnummer ist nicht für Kontakte sichtbar

Nachteile

- Kollaboration und Teams - Es kann im Chat schnell unübersichtlich werden, weil es kaum Features gibt die über Messaging hinaus gehen. Aber immerhin gibt es jetzt Call-Links für Meetings.
- Widerstandsfähigkeit - zentrale Server, die in manchen Ländern blockiert werden

Fazit:

> **Signal ist ein guter Allrounder wenn es darum geht sich sicher, unkompliziert und einfach zu verständigen.**
> **Signal ist super für alle Anwendungsfälle, in denen:**
> - ihr eine Telefonnummer für die Registrierung nutzen könnt
> - eure Handys wahrscheinlich nicht in falsche Hände geraten werden
> - ihr mit einer einzigen Gruppe auskommt und nicht mehrere Untergruppen benötigt
> - ihr euch in einem Land befindet, in dem die Regierung Signal nicht blockiert

Tipps & Tricks

- Signal lässt sich mit jeder beliebigen Telefonnummer nutzen, auch mit Festnetznummern, einmaligen Nummern oder anonymen SIM-Karten
- Es ist möglich zwei Signal-Accounts auf einem Gerät zu haben: Android, Linux
- Wenn Signal blockiert wird, gibt es die Möglicheit einen TLS-Proxy zu nutzen

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 (Sitz Kalifornien) ohne Profitinteresse.

Anrufe & SMS sind unsicher

Rechtliche Situation in Deutschland

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 -> Aufs Profilbild klicken -> @Nutzername
IOS: Profil-Icon -> Einstellungen -> Aufs 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

Verschwindene Nachrichten

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

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

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

https://www.kicksecure.com/wiki/Signal

Verschwindende Nachrichten (Funktionsweise)

Verschwindende Nachrichten in Signal funktionieren so:

1. Die Nachricht wird an den Server übermittelt (wenn sendendes Gerät Online ist)
2. Der Server speichert die Nachricht so lange verschlüsselt zwischen, bis er sie an mind. 1 Gerät aller Accounts in dem Chat geschickt hat. Dafür muss jeder Account mal kurz online sein mit einem Gerät. Dies **führt dazu, dass die Nachricht auch nach Monaten noch zugestellt werden kann, wenn der Account so lange offline war.**
3. Das Gerät 1 der Accounts in der Gruppe, das die Nachricht als erstes empfängt speichert die Nachricht so lange (verschlüsselt im Speicher & entschlüsselt wenn die App offen ist) bis sie gelesen wurde + die Zeit die eingestellt wurde.
4. Andere Geräte der Accounts synchronisieren die Nachrichten von dem Gerät 1 auf dem sie empfangen wurden - nach X Zeit geht das aber nicht mehr, weil die Nachricht ja auf Gerät 1 garnicht mehr existiert (Also das keine Angriffsfläche).

> Verschwindende Nachrichten verhindern nicht, dass Menschen Screenshots machen können (auch nach X Zeit nach absenden) - es verhindert nur, dass Nachrichten gelesen können werden, wenn bspw. ein Handy in deren Finger gerät und die Nachricht von diesem Account bereits vor länger als X Zeit **gelesen** wurde. **Wenn sie jedoch nicht gelesen wurde, ist die Nachricht auch nicht sicher gelöscht.**

Alternativen

> Mit paste.systemli.org/ würde mensch aber erreichen, dass **der Inhalt in jedem Fall nach X Zeit nach abschicken gelöscht wird.** Es gibt dort auch die Möglichkeit Kommentare zu erlauben. Zudem steht dort kein Signal-Name dabei wenn die Nachricht gescreenshottet wird. Das Tool basiert auf *privatebin.info* und wird von vielen linken Tech-Kollektiven gehostet.