Wissenswertes über Signal

"Signal Sicher benutzen"? Ich dachte Signal ist schon sicher!

So einfach ist das nicht. Signal benutzt sehr sichere Verschlüsselung. Aber es gibt Fallstricke. Bitte achtet darauf, dass eure Geräte (auch der Laptop!) verschlüsselt sind. Anleitungen findet ihr hier. Wenn die Polizei ein Handy beschlagnahmt und dieses benutzen kann, weil keine PIN eingestellt ist, helfen (quasi) keine der Sicherheitsmechanismen etwas.

Warum Signal und nicht Telegram/WhatsApp/Sonstwas?

Signal wurde von einem Hacker mit dem Pseudonym Moxie Marlinspike entwickelt. Moxie ist ein sehr bekannter und anerkannter Hacker und bereits seit mehr als einem Jahrzent bekannt für seine Recherchen zu Angriffen auf Verschlüsselung. Die Vorteile von Signal sind:

- Signal hat ein sehr sicheres Design und ist quelloffen (Open Source)
- Hinter Signal steht die "Signal Foundation", eine gemeinnützige Organisation, die rein auf Spenden basiert. Es gibt daher für Signal auch kein Geschäftsinteresse, auf diese Daten zugreifen zu wollen
- Durch “Verschwindende Nachrichten” werden Nachrichten automatisch gelöscht
- Signal-Chats können gebackuped werden (aktuell leider nur auf Android)

Signal kennt keine Metadaten (wer wann mit wem kommuniziert). Signal kennt auch keine Inhalts-Daten (was wurde kommuniziert, da die Chats Ende-zu-Ende verschlüsselt sind). Signal ist sehr transparent und veröffentlicht Anfragen der Polizei und Signal's Antwort (Beispiel).

Die Chats bei Telegram sind standardmäßig nicht verschlüsselt. Auch Gruppenchats sind nicht verschlüsselt. Um bei Telegram Ende-zu-Ende-Verschlüsselung zu nutzen, müssen explizit “private Chats” erstellt werden. Telegram kooperiert auch mit den Behörden (Tagesschau-Artikel).

Die Chats bei WhatsApp sind angeblich Ende-zu-Ende verschlüsselt. Allerdings kann das nicht verifiziert werden, da der Code von WhatsApp nicht öffentlich ist. Außerdem steckt hinter WhatsApp die Firma Meta (Facebook), die bekannt dafür ist, Daten zu sammeln.

Warum Anrufe über das Mobilfunk und SMS unsicher sind

Mit einem richterlichen Beschluss bekommt die Polizei sehr leicht Zugriff auf alle SMS-Inhalte sowie Telefongespräche. Allerdings ist dafür ein 129er-Verfahren notwendig (kriminelle Vereinigung), Ermittlungsverfahren wegen Straßenblockaden reichen dafür nicht aus.

Falls ein Beschluss (LG Beispiel) zur Überwachung eurer Telefonate vorliegt, wird fast immer die normale Telekommunikationsüberwachung (TKÜ) eingesetzt. Das Abhören der Kommunikation erfolgt über den Mobilfunkprovider und ihr könnt es nicht bemerken. Schlechter Empfang oder komische Geräusche sind kein Zeichen von Überwachung. Der Provider zeichnet die Gespräche auf und schickt sie dann der Polizei in Form von MP3-Dateien.

Das bedeutet, dass Ende-zu-Ende-verschlüsselnde Messenger-Apps einschließlich Signal weiterhin sicher sind, solange keine Quellen-TKÜ (Staatstrojaner) eingesetzt wird, was sehr selten passiert.

PIN für Signal einrichten

Es ist sehr 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. Heißt: Die Polizei kann deinen Signal Account übernehmen, indem sie deinen Account auf einem anderen Handy einrichtet. Dies ist nicht möglich, wenn du eine Signal-PIN hinterlegst.

Wie du die PIN einrichtest, wird in der Signal Dokumentation gut erklärt: https://support.signal.org/hc/de/articles/360007059792-Signal-PIN

Am besten speicherst du deine PIN in deinem Passwort-Manager.

Verschwindende Nachrichten/Disappearing Messages

"Verschwindende Nachrichten" bedeuten: Nach einer eingestellten Zeitspanne (z. B. einer Woche) werden die Nachrichten auf allen Geräten gelöscht. Es lässt sich auch einstellen, dass das Feature für neue Chats automatisch aktiviert ist. Für die genaue Anleitung empfehlen wir die offizielle Signal Dokumentation: https://support.signal.org/hc/de/articles/360007320771-Verschwindende-Nachrichten-festlegen-und-verwalten

Einladungslinks für Gruppen: Die Gruppenbeschreibung ist öffentlich einsehbar

Wenn ihr für Gruppen Einladungslinks verwendet, macht euch bewusst: Wer den Link hat, kann auch die Gruppenbeschreibung lesen - auch ohne vom Admin der Gruppe hinzugefügt worden zu sein. Grundsätzlich solltet ihr keine geheimen Informationen (Links mit Zugangs-Berechtigungen oder Passwörter) in Gruppen nutzen, die ihr öffentlich teilt. Mehr Infos dazu hier:

https://blaeul.de/sonnenschein/signalgruppen-und-einladungslinks

Handynummer? Anonymität mit Signal

Jeder Signal Account benötigt eine Handynummer. Deine Handynummer ist mit deiner Person verbunden. Mittlerweile kann man einstellen, dass die eigene Handynummer in Signal nicht mehr angezeigt wird. Lest euch bitte den Signal Artikel dazu. Er klärt viele Fragen zu dem Thema: https://support.signal.org/hc/de/articles/6712070553754-Datenschutz-bei-Telefonnummern-und-Nutzernamen

Denkt auch daran, was passsiert, wenn ihr den Zugang zu eurem Signal Account verliert (Smartphone defekt/beschlagnahmt/verloren). Wenn ihr die Handynummern eurer Friends nicht mehr habt und euer Signal weg ist, könnt ihr die Menschen nicht mehr kontaktieren.

Version #1
Erstellt: 2025-10-09 14:58:54 UTC von RAZ Migration Bot
Zuletzt aktualisiert: 2025-10-09 14:58:54 UTC von RAZ Migration Bot