

FAQ: Signal

Viele WhatsApp-Nutzer steigen in jüngster Zeit auf die datenschutzfreundliche Alternative Signal um. Wir beantworten die wichtigsten Fragen für neue und alte Nutzer.

Von Ronald Eikenberg

Lohnt der Umstieg?

? Ist Signal besser als WhatsApp?

! In puncto Datenschutz hat Signal klar die Nase vor. Dahinter steckt die gemeinnützige Signal-Stiftung, die kein Geld mit den Daten der Nutzer verdient, während WhatsApp seit einigen Jahren von der Datenkrake Facebook betrieben wird. Anders als WhatsApp ist Signal zudem Open Source, den Quellcode der App kann somit jedermann einsehen und überprüfen. Auch bei der Sicherheit liegt Signal in Führung: Sowohl Signal als auch WhatsApp nutzen das Signal-Protokoll zur Kommunikation, das gewährleistet, dass Nachrichten Ende-zu-Ende-verschlüsselt an den Empfänger übertragen werden. Signal schützt darüber hinaus Metadaten wie Telefonnummern, Chatkontakte oder Gruppenzugehörigkeiten besser als WhatsApp (siehe c't 8/2021, S. 24). Der Funktionsumfang ist hingegen bei WhatsApp derzeit noch etwas größer, die Signal-Entwickler arbeiten jedoch daran, die von WhatsApp & Co. bekannten Features nach und nach umzusetzen.

Signal auf dem Desktop

? Kann ich Signal auch auf dem PC nutzen?

! Ja, Signal gibts auch für Windows, macOS und Linux (siehe ct.de/y6dw). Sie müssen die Desktop-App vor der ersten Nutzung mit dem Smartphone koppeln. Öffnen Sie hierzu die Einstellungen der Smartphone-App und fügen Sie den PC unter „Gekoppelte Geräte“ hinzu. Anschließend können Sie mit der Smartphone-App den QR-Code scannen, der Ihnen auf dem Rechner angezeigt wird. Anders als WhatsApp funktioniert Signal

auf dem Desktop autark: Sie können die Desktop-App also auch dann nutzen, wenn Ihr Smartphone ausgeschaltet ist. Aufgrund der Verschlüsselung erscheinen auf gekoppelten Geräten ausschließlich Nachrichten, die seit der Kopplung eingetroffen sind, frühere Nachrichten könnte der Rechner auch nicht entschlüsseln. Entkoppeln Sie verknüpfte Clients, die Sie nicht länger nutzen.

Videocalls in Gruppen

? Unterstützt Signal Videokonferenzen?

! Ja, seit Kurzem können Sie verschlüsselte Sprach- und Videotelefonate auch in Gruppen führen. Öffnen Sie hierzu einfach die Chatgruppe und klicken Sie auf das Kamerasymbol oben rechts. Fehlt das Symbol, dann handelt es sich noch um eine Gruppe des alten Typs, der nicht alle modernen Funktionen unterstützt. In diesem Fall können Sie entweder eine neue Gruppe mit den gewünschten Gesprächspartnern erstellen

oder die vorhandene Gruppe auf den neuen Gruppentyp umstellen (siehe „Alte und neue Gruppen“). Signal unterstützt Gruppenanrufe mit bis zu fünf Teilnehmern. Dieses Limit soll in Zukunft angehoben werden. Die Sprach- und Videoanrufe funktionieren auch auf dem Desktop.

Signal statt USB-Stick

? Kann ich Signal nutzen, um Daten zwischen meinen Geräten auszutauschen?

! Ja, Signal kann Dateien und Nachrichten auch innerhalb eines Accounts verschicken und so als Ersatz für den USB-Stick und als digitaler Notizblock dienen. Chatten Sie sich über den Kontakt „Notiz an mich“ einfach selbst an. Die Übertragung erfolgt auch in diesem Fall verschlüsselt. Das Größenlimit liegt bei 100 MByte pro Datei, die Übertragung ausführbarer Dateien ist bei Signal aus Sicherheitsgründen nicht gestattet. Sie können solche Dateien jedoch in ein Zip-Archiv packen und verschicken.

Signal gibts auch für den Rechner. Der Account ist per QR-Code-Scan schnell eingerichtet.



PIN-geschützt

? Warum muss ich eine Signal-PIN setzen?

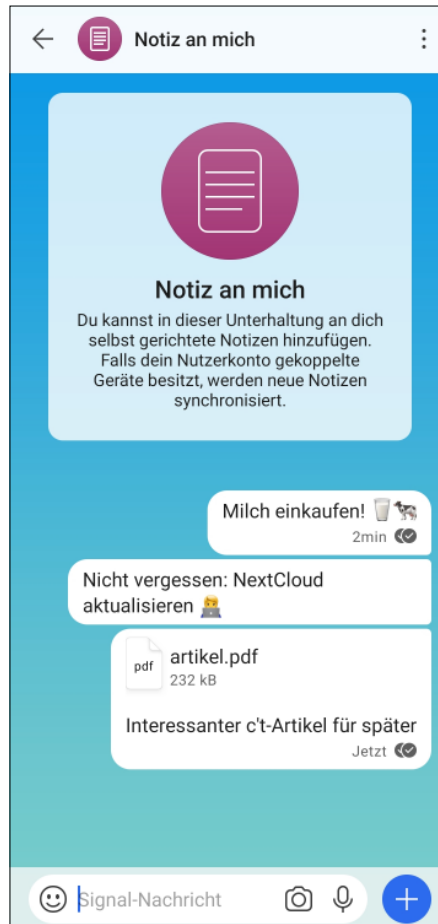
! Die Signal-PIN schützt die Daten, die mit Ihrem Account verknüpft sind, darunter Ihre Kontakte, Ihr Profil und die Einstellungen. Ist keine PIN gesetzt, können diese Daten nicht wiederhergestellt werden, wenn Signal auf einem neuen Gerät eingerichtet wird und Sie kein Backup haben – Sie müssen dann bei null anfangen. Dies ist ein wichtiger Schutz, da die Verknüpfung mit der Rufnummer allein zu unsicher wäre: Wird Ihre Rufnummer einem neuen Mobilfunkkunden zugewiesen, könnte diese Person sonst auf Ihre Daten zugreifen. Auch Angriffe, bei denen der Täter eine weitere SIM-Karte für Ihren Mobilfunkvertrag bestellt, werden so vereitelt. Sie können in den Signal-Einstellungen unter „Datenschutz“ zudem eine Registrierungssperre aktivieren, die verhindert, dass neue Geräte ohne Ihre Zustimmung mit Ihrer Rufnummer verknüpft werden. Diese Sperre gilt sieben Tage: Sind Sie eine Woche inaktiv, wird Ihre Rufnummer wieder für neue Clients freigegeben.

Mehr Privatsphäre

? Was kann ich tun, um meine Privatsphäre bestmöglich zu schützen?

! Signal bietet eine Reihe optionaler Funktionen, mit denen Sie den Datenschutz verbessern können. Aktivieren Sie in den Einstellungen unter „Datenschutz“ die Option „Inkognito-Tastatur“, damit Signal Ihrer Bildschirmtastatur signalisiert, dass Texteingaben nicht im Wörterbuch – und damit oft auch in der Cloud – gespeichert werden. Deaktivieren Sie bei Bedarf die Lesebestätigungen und Tipp-Indikatoren, um zu verhindern, dass Ihr Gesprächspartner erfährt, wann Sie eine Nachricht gelesen haben und wann Sie tippen. Wenn Sie „Anrufe immer indirekt“ aktivieren, dann leitet die App Ihre Anrufe generell über Signal-Server. Dadurch verhindern Sie, dass der Angerufene Ihre IP-Adresse erfährt. Darunter kann allerdings die Anrufqualität leiden.

Bei besonders sensiblen Unterhaltungen können Sie in den Einstellungen des Chats festlegen, dass Nachrichten nach einer definierten Zeit automatisch gelöscht werden. Die Zeit läuft erst, nach-



Notiz an mich: Signal dient auch als digitaler Notizblock und kann Dateien von einem Gerät aufs andere transportieren.

dem der Empfänger die Nachricht erstmalig gelesen hat. Ein böswilliger Chatpartner kann die Nachrichten natürlich trotzdem dokumentieren, etwa, indem er sein Handydisplay abfilmt.

Sicherheitsnummern

? Was bedeuten die Sicherheitsnummern auf den Profilen meiner Kontakte? Muss ich die überprüfen?

! Anhand der Sicherheitsnummer können Sie überprüfen, ob Ihre Nachrichten auch tatsächlich den richtigen Empfänger erreichen. Bei Signal hat jeder Chat eine eigene. Es handelt sich dabei im Wesentlichen um einen Fingerabdruck des eingesetzten Kryptoschlüssels. Ändert sich dieser Schlüssel, dann wurde der Account Ihres Kontakt möglicherweise von einer fremden Person übernommen. Es gibt aber auch legitime Ursachen, etwa,

wenn Ihr Kontakt seinen Account neu eingerichtet hat.

Um sicherzustellen, dass eine Konversation vertraulich ist, sollten Sie die Sicherheitsnummer bei einem persönlichen Treffen überprüfen. Hierzu öffnen beide Gesprächsteilnehmer die Chat-Einstellungen, indem Sie auf den Nutzeramen klicken. Wählen Sie anschließend „Sicherheitsnummer verifizieren“. Die angezeigte Ziffernfolge muss bei beiden Gesprächspartnern identisch sein. Um die Überprüfung der Zahlenkolonnen zu erleichtern, können Sie den angezeigten QR-Code scannen. Stimmt die Nummer überein, klicken beide Teilnehmer auf „Verifiziert“.

Alte und neue Gruppen

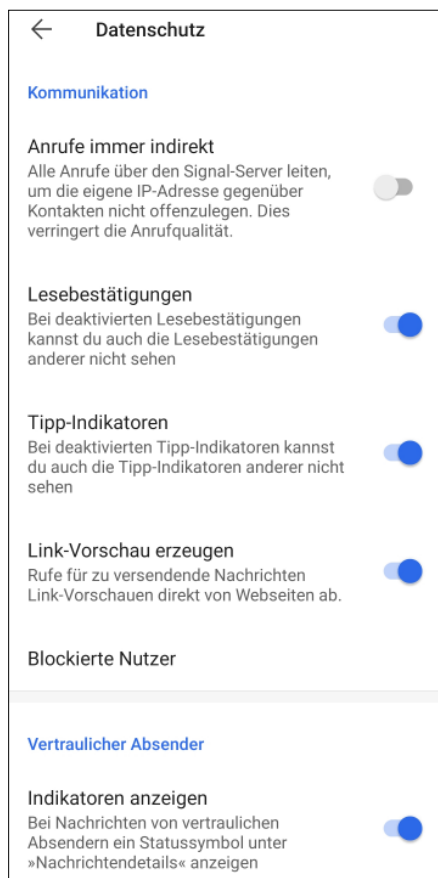
? Was hat es mit dem neuen Gruppentyp auf sich?

! Bei Signal gibt es zwei Arten von Chatgruppen: Das aktuelle Format sowie die alten „Legacy“-Gruppen. Alle neu angelegten Gruppen entsprechen dem aktuellen Format und unterstützen somit moderne Funktionen wie Sprach- und Videoanrufe, Erwähnungen (@username) und Adminfunktionen. Alte Gruppen erkennen Sie daran, dass Signal in den Gruppeneinstellungen ganz oben „Gruppe alten Typs“ anzeigt. Direkt darunter können Sie solche Gruppen auch ganz leicht in den neuen Typ umwandeln („aktualisiere diese Gruppe“). Alle Gruppenteilnehmer müssen hierzu eine aktuelle Signal-Version nutzen, und zwar auch auf allen verknüpften Geräten. Befinden sich Nutzer mit einer veralteten Signal-Version in der Gruppe, werden Sie vor der Umwandlung gewarnt und können die Kontakte gezielt bitten, ihr Signal zu aktualisieren.

Signal als SMS-App

? Mit Signal kann ich auch SMS verschicken. Sind diese auch verschlüsselt?

! Nein. Sie können Signal unter Android zwar als Standard-App für SMS und MMS einrichten, allerdings erfolgt die Übertragung der SMS-Nachrichten wie schon zuvor unverschlüsselt über das Mobilfunknetz. Die Übertragung wird wie sonst auch über Ihren Mobilfunktarif abgerechnet.



Wer möchte, kann über die Signal-Einstellungen noch allherhand optimieren, etwa die Privatsphäre.

Nur für Nerds?

? Viele Krypto-Messenger sind recht kompliziert. Kann ich Signal auch meiner Schwiegermutter empfehlen, die bisher nur WhatsApp nutzt?

! Signal richtet sich an ein breites Publikum, Nutzung und Einrichtung sind genauso leicht wie bei WhatsApp. Sie können Familie, Freunde und Kollegen also ruhig zum Wechsel animieren. Signal ist zwar mit einigen Sonderfunktionen ausgestattet, drängt diese seinen Nutzern jedoch nicht auf. Wer einfach nur wie gewohnt kommunizieren möchte, kommt damit nicht in Berührung. Von dem Plus an Datenschutz und Sicherheit profitiert man bereits mit den Standardeinstellungen.

Chat-Backups

? Kann ich meine Chat-Verläufe irgendwie sichern und bei Bedarf wiederherstellen?

! Ja, das klappt, aber nur unter Android. Zum Sichern öffnen Sie die Einstellungen und „Unterhaltungen“, dort finden Sie die Exportfunktion unter „Datensicherung/Unterhaltungen sichern“. Signal zeigt Ihnen daraufhin eine Passphrase an, die sie unbedingt notieren müssen. Die Backups sind nämlich verschlüsselt und ohne die Passphrase nicht wiederherstellbar. Die Wiederherstellung bietet Ihnen Signal an, wenn Sie die App neu einrichten und sich das Backup am passenden Speicherort befindet (/storage/emulated/0/Signal/Backups).

Unter iOS können Sie keine solchen Backups anlegen, aber immerhin die Nachrichten von einem Gerät auf ein anderes übertragen, wenn beide noch funktionstüchtig sind. Das genaue Vorgehen wird in den FAQ des Messengers erklärt (siehe ct.de/y6dw).

Wenn Sie keinen Wert darauf legen, Ihre alten Chats im Fall der Fälle wiederherstellen zu können, können Sie auf die Einrichtung des Backups verzichten. Für eine Neueinrichtung des existierenden Accounts, etwa nach einem Gerätewechsel, ist kein Backup nötig.

Ein bisschen Spaß muss sein

? Unterstützt Signal animierte Sticker?

! Animierte Chat-Sticker erfreuen sich bei WhatsApp, Telegram & Co. großer Beliebtheit und auch bei Signal kann man sie seit Kurzem nutzen. Klicken Sie in einem Chat einfach auf das Stickersymbol links neben dem Texteingabefeld. Anschließend können Sie einen Sticker auswählen und versenden. Über das Pluszeichen bei der Stickerauswahl fügen Sie neue Sticker-Sets hinzu. Die Auswahl innerhalb der App ist derzeit überschaubar, Sie finden jedoch auf <https://signalstickers.com> etliche Sets, die Sie leicht installieren können. Unter ct.de/y6dw finden Sie Informationen, wie Sie eigene Sticker-Sets erstellen können. Hierzu ist Signal Desktop nötig. Inzwischen können Sie bei Signal in den „Unterhaltungseinstellungen“ übrigens auch den Chat-Hintergrund ändern, wie von anderen Messengern gewohnt.

(rei@ct.de)

Signal Desktop, FAQ und Sticker-Sets:
ct.de/y6dw