Wirtschaftsschutz

Sicherheitshinweis 2/26

Sicherheitshinweis zu andauernden Phishing-Angriffen über Messenger-Dienste wie Signal

Im Februar 2026 hat das Bundesamt für Verfassungsschutz (BfV) zusammen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) einen gemeinsamen Warnhinweis zu **Phishing-Angriffen über Messenger-Dienste wie Signal und WhatsApp**[1] veröffentlicht und der Bundesgeschäftsführung Ihrer Parteien zukommen lassen.

Diese Phishing-Kampagne dauert weiter an. Nachrichtendienste aus den USA[2] und den Niederlanden[3] haben die Angriffskampagne bereits zu Russland attribuiert.

Es handelt sich um eine koordinierte, internationale Angriffswelle, in deren Fokus hochrangige Entscheidungsträger aus Politik, Militär und Verwaltung sowie Vertreter aus Journalismus und Wirtschaft stehen. Diese werden durch einen maliziösen Nutzer mit dem Namen „Signal Support“ in der Messenger-App angeschrieben und zur Weitergabe der persönlichen Sicherheitsdaten verleitet. Im Anschluss erfolgt eine Übernahme des Messenger-Kontos durch die Angreifer. Oft bleibt diese feindliche Übernahme unbemerkt. Unter Nutzung des übernommenen Messenger-Kontos erhalten die Angreifer Zugriff auf das Signal-Adressbuch sowie zu allen Gruppenchats, in denen das Messenger-Konto Mitglied war.

Es ist davon auszugehen, dass so zahlreiche Signal-Gruppen im parlamentarischen Raum derzeit von den Angreifern nahezu unbemerkt ausgelesen werden. Dem BfV sind bereits zahlreiche hochrangige Betroffenheiten bekannt geworden. Angesichts der Natur der Angriffe ist jedoch von einer deutlich höheren Dunkelziffer auszugehen.

---

[1] www.verfassungsschutz.de/SharedDocs/kurzmeldungen/DE/2026/2026-02-06-gemeinsamer.sicherheitshinweis-phishing.html

[2] FBI & CISA, USA: Russian Intelligence Services Target Commercial Messaging Application Accounts; https://www.ic3.gov/PSA/2026/PSA260320

[3] AIVD & MIVD, Niederlande: Russia targets Signal and WhatsApp accounts in cyber campaign; https://english.aivd.nl/latest/news/2026/03/09/russia-targets-signal-and-whatsapp-accounts-in-cyber-campaign

65187 Wiesbaden, Konrad-Adenauer-Ring 49
Telefon: (0611) 720-0
Telefax: (0611) 720-1139
E-Mail: poststelle@lfv.hessen.de
Internet: www.verfassungsschutz.hessen.de

KEIN RAUM FÜR SPIONAGE
verfassungsschutz.hessen.de

Vor diesem Hintergrund wende wir uns heute direkt an Sie, um Ihnen nachfolgend weitere Informationen und Handlungsempfehlungen zum Umgang mit diesen Angriffen zukommen zu lassen. Die dargestellten Maßnahmen sind in drei Eskalationsstufen unterteilt, gemäß der unterschiedlichen möglichen Angriffsvektoren des Akteurs.

Das Landesamt für Verfassungsschutz Hessen (LfV Hessen) regt in diesem Zusammenhang an, dass Sie in Zusammenarbeit mit Ihren IT-Fachkräften Ihre Sicherheitsmaßnahmen überprüfen. Zudem finden Sie unter folgendem Link eine in Zusammenarbeit von BfV und BSI entwickelte Webseite, welche Ihnen ebenfalls Empfehlungen zum Umgang mit der aktuellen Angriffskampagne gibt:

https://www.bsi.bund.de/dok/phishing-messengerdienste

https://www.bsi.bund.de/dok/phishing-signal-support

Bei dem Verdacht einer möglichen Betroffenheit oder einem weitergehenden Sensibilisierungsbedarf wenden Sie sich vertrauensvoll per E-Mail (wirtschaftsschutz@lfv.hessen.de) oder telefonisch (0611/720-3600) an den Wirtschaftsschutz des Landesamts für Verfassungsschutz Hessen.

DER SACHVERHALT

Das Ziel der Angreifer

Die Angreifer verfolgen ein klares Ziel: Sie wollen Zugriff auf Ihre vertrauliche Kommunikation erhalten – einschließlich Nachrichten, Bildern, Videos und Dokumenten in Einzel- und Gruppenchats. Zusätzlich nutzen sie kompromittierte Konten, um weitere Kontakte für neue Angriffe zu gewinnen.

Dabei greifen sie gezielt auf legitime Sicherheitsfunktionen von Signal zurück, etwa die Verknüpfung zusätzlicher Geräte oder die Eingabe von Verifizierungscodes.

Das Vorgehen der Angreifer

Variante 1

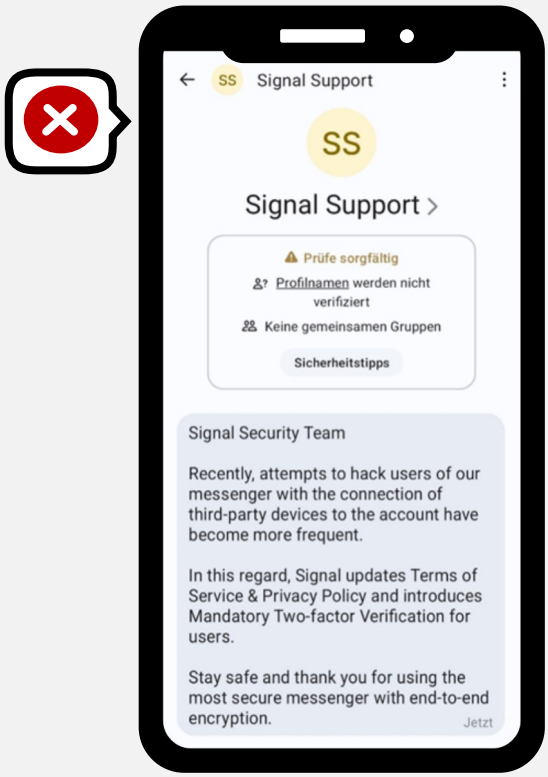
Am Anfang senden Ihnen die Angreifer unter dem Deckmantel des angeblichen „Signal Support“ eine täuschend echt wirkende Chatnachricht. Die Inhalte variieren, zielen jedoch immer darauf ab, Ihr Sicherheitsbewusstsein anzusprechen und Sie zum Handeln zu bewegen – z.B. sei ein Sicherheitsvorfall festgestellt worden und Ihre Mithilfe von Nöten.

Im Hintergrund lösen die Angreifer den Versand eines legitimen Verifizierungscodes per SMS aus. Kurz darauf werden Sie dann ebenfalls via Chatnachricht aufgefordert, diesen per SMS erhaltenen Verifizierungscode sowie Ihre Sicherheits-PIN einzugeben.

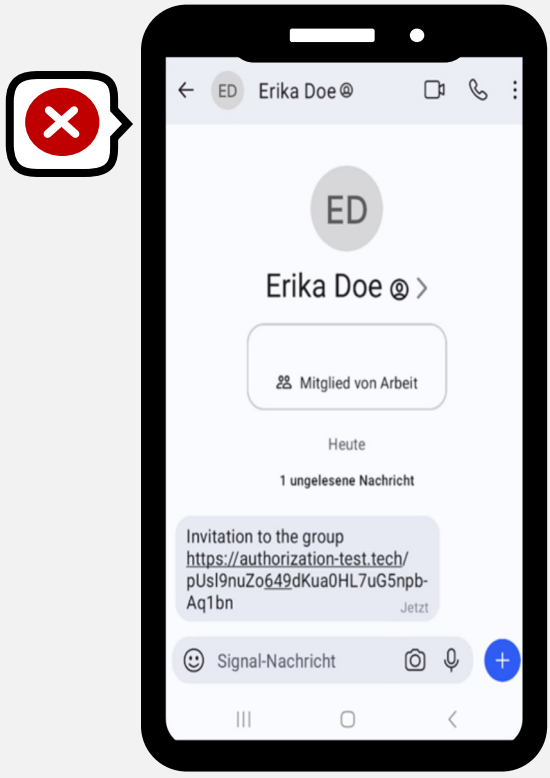
Variante 2

Sie bekommen eine Chatnachricht von einer Ihnen bekannten Person. Diese Nachricht enthält einen Einladungslink z.B. zu einer neuen Chatgruppe. Folgen Sie dem Link, gelangen Sie auf eine täuschend echt gestaltete Webseite, die vorgibt, zu WhatsApp oder Signal zu gehören. Um der angeblichen neuen Chatgruppe beizutreten kann es sein, dass Sie aufgefordert werden einen QR-Code zu scannen. Alternativ sollen Sie einen Button anklicken.

Was Sie nicht wissen: das Messenger-Konto Ihrer Kontaktperson wurde bereits zuvor von den Angreifern übernommen und in Wirklichkeit kontrollieren die Angreifer die Webseite, auf welcher Sie sich jetzt befinden.



Beispiel für Variante 1



Beispiel für Variante 2

Die Folgen

Variante 1 - Kontoübernahme

Wenn Sie den per SMS erhaltenen Verifizierungscode weitergeben, reicht dies den Angreifern in vielen Fällen bereits, um **Ihr Konto beim Messenger-Dienst Signal vollständig zu übernehmen**.

Sie verlieren den Zugriff auf Ihr Konto und damit die Kontrolle über alle Inhalte der Signal-App inklusive Bildern, Videos, Dokumenten oder Sprachnachrichten. Gleichzeitig können die Angreifer in Ihrem Namen kommunizieren, in bestehenden Gruppen mitlesen, neuen Gruppen beitreten und Ihre Kontakte einsehen.

Variante 2 - Gerätekopplung

Durch das Anklicken des Einladungslinks und/oder Scannen des QR-Codes ermöglichen Sie unbemerkt die Verknüpfung eines fremden Geräts mit Ihrem Messenger-Konto.

Sie behalten zwar den Zugriff auf Ihr Konto, doch die **Angreifer lesen ab diesem Zeitpunkt unbemerkt alle Nachrichten mit** – sowohl gesendete als auch empfangene Inhalte.

Alles was mit Ihnen geteilt wird oder was Sie anderen mitteilen, wird unbemerkt auch mit dem Angreifer geteilt – sensible Nachrichten, Videos, Bilder, Dokumente, Sprachnachrichten. Dies gilt für Einzel- wie für Gruppenchats.

Anzeichen, dass Sie betroffen sind

Einige der nachfolgenden Anzeichen können auch legitime Ursachen haben. Je mehr dieser Anzeichen Sie jedoch bemerken, desto wahrscheinlich ist es, dass Ihr Konto übernommen wurde oder unbefugte Dritte mitlesen.

Variante 1

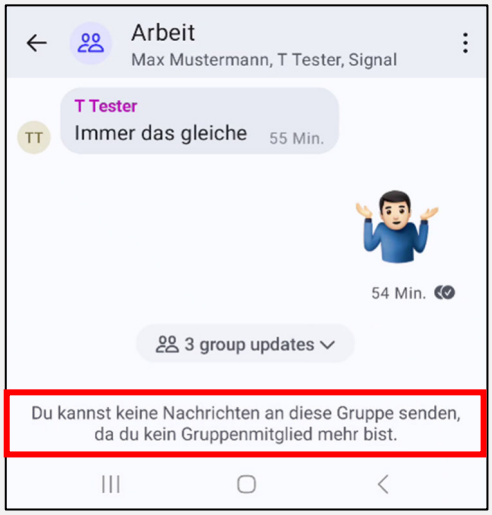
- ☐ Sie haben Nachrichten vom angeblichen „Signal Support“ erhalten und danach Verifizierungscodes via SMS bekommen?
- ☐ Sie wurden plötzlich aus Ihrem Konto ausgeloggt?
- ☐ Beim Öffnen der Messenger-App wurden Sie unerwartet zur Neuanmeldung aufgefordert?
- ☐ Nach der Neuanmeldung waren Kontakte und Gruppenchats teilweise verschwunden oder Sie waren nicht länger Mitglied in Gruppenchats?



1. Nach Eingabe des Verifizierungscodes werden Sie plötzlich abgemeldet/ ausgeloggt.



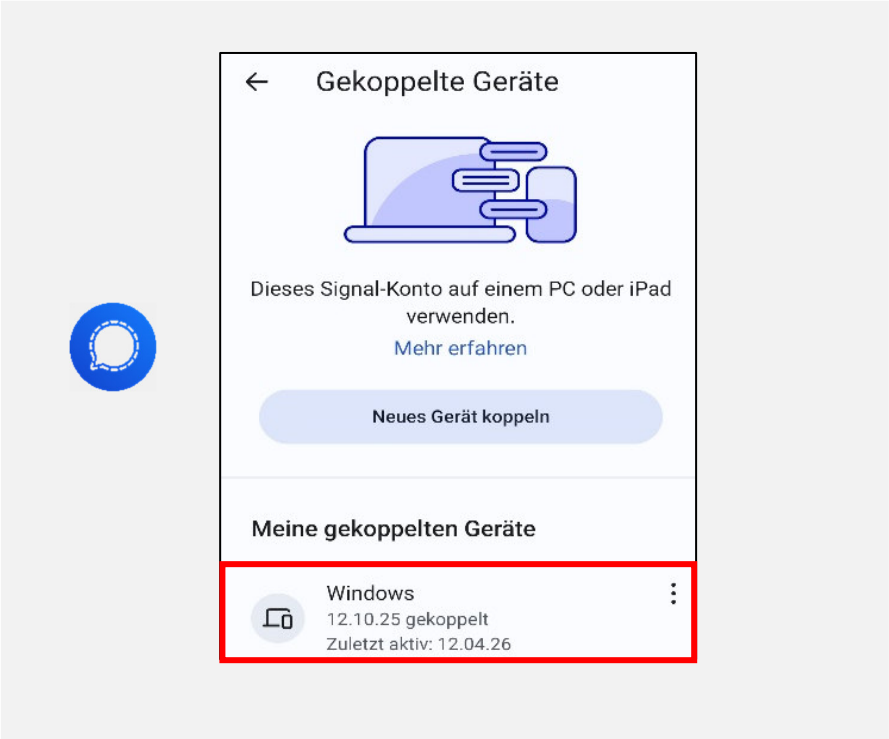
2. Sie müssen sich neu anmelden/ registrieren.



3. Nach der Anmeldung: Gruppenmitgliedschaften sind aufgehoben, Chats fehlen.

Variante 2

- ☐ Sie haben unerwartet einen Link mit einer angeblichen Gruppeneinladung erhalten?
- ☐ Oder Sie werden zum Scannen eines QR-Codes aufgefordert?
- ☐ Sie finden in Ihrer Messenger-App unter *Einstellungen* > *gekoppelte/verknüpfte Geräte* Einträge, die Sie nicht zuordnen können?



Anzeichen das Ihr Umfeld betroffen ist

- ☐ Die Kontaktliste in Ihrem Messenger enthält doppelte oder ungewöhnlich benannte Kontakte wie z.B. den selben Namen in leicht unterschiedlichen Schreibweisen oder mit untypischen Emojis versehen?
- ☐ In Gruppenchats tauchen ebenfalls doppelte Kontakte auf oder Sie bemerken ungewöhnliche Namensänderungen wie „gelöschtes Konto/Deleted Account“?
- ☐ Ihnen fällt auf, dass in Chats die Systembenachrichtigung *„Ihre Sicherheitsnummer mit [NAME] hat sich geändert“* oder *„[NAME] hat seine Telefonnummer geändert“* angezeigt wird?

Wenn Sie solche Hinweise bemerken, kontaktieren Sie die betroffene Person über einen anderen Kommunikationsweg, um die Echtheit der Aktivitäten zu überprüfen.

DIE GEGENMASSNAHMEN

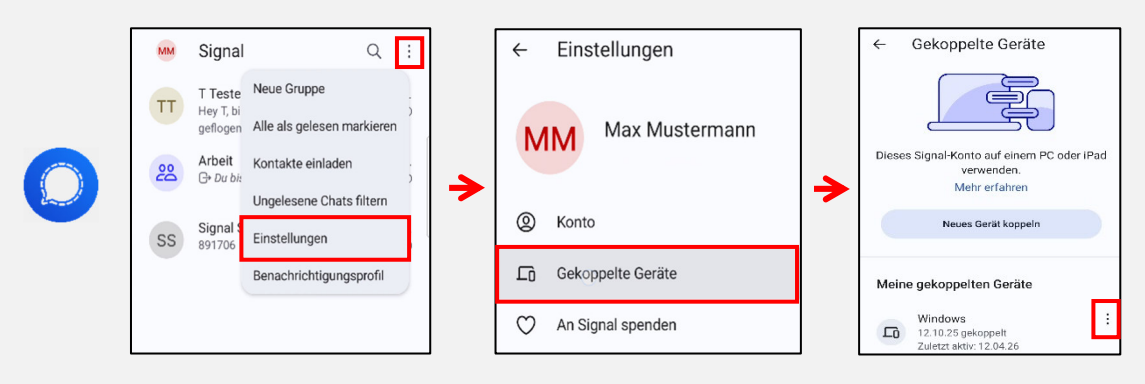
Was Sie tun können

Nachfolgend finden Sie verschiedene Handlungsoptionen, die Ihnen im Fall einer eigenen Betroffenheit oder bei Betroffenheit in Ihrem Umfeld weiterhelfen:

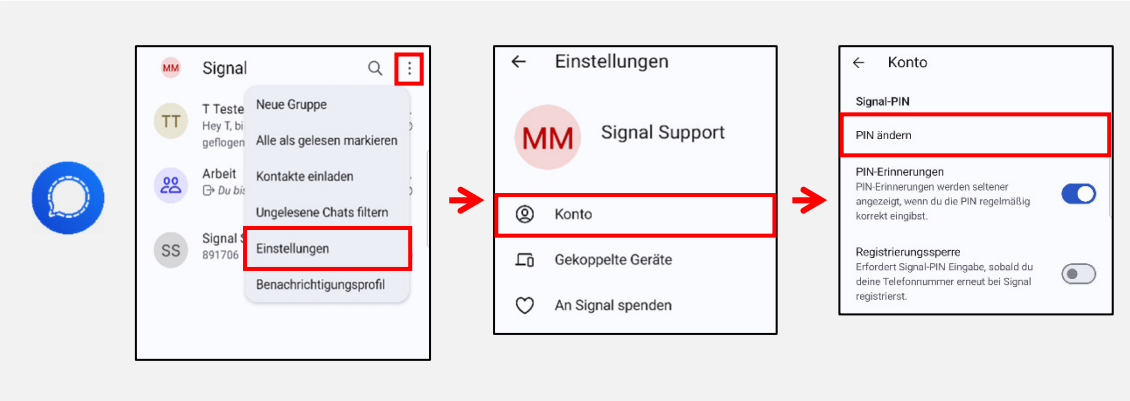
Maßnahmenpaket 1: Sofortige Gefahrenabwehr

Szenario: Sie haben einen **Link oder QR-Code erhalten und angeklickt** bzw. gescannt.
Oder Sie haben eine „Signal Support"-Nachricht erhalten, jedoch **keinen PIN oder SMS-Verifizierungscode** eingegeben.
Oder Ihnen sind Merkwürdigkeiten in Gruppenchats aufgefallen.

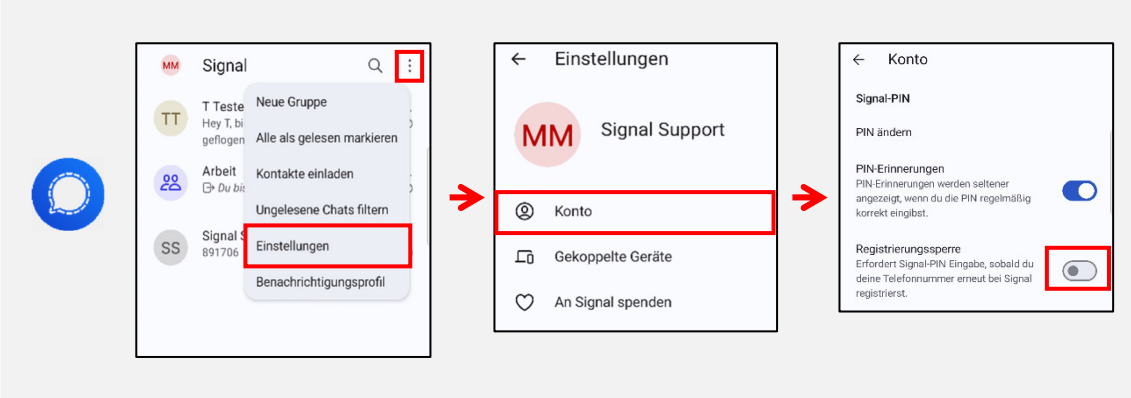
- **Bereinigung gekoppelter Geräte:**
  Öffnen Sie die Übersicht gekoppelter Geräte. **Entfernen Sie umgehend alle Geräte**, die Sie nicht aktuell selbst nutzen oder zuordnen können. Im Zweifel: alle Geräte entfernen.



- **Akutmaßnahme PIN-Änderung:**
  Sofern Sie noch Zugriff auf Ihr Signal-Konto haben, ändern Sie **sofort Ihre Sicherheits-PIN**.

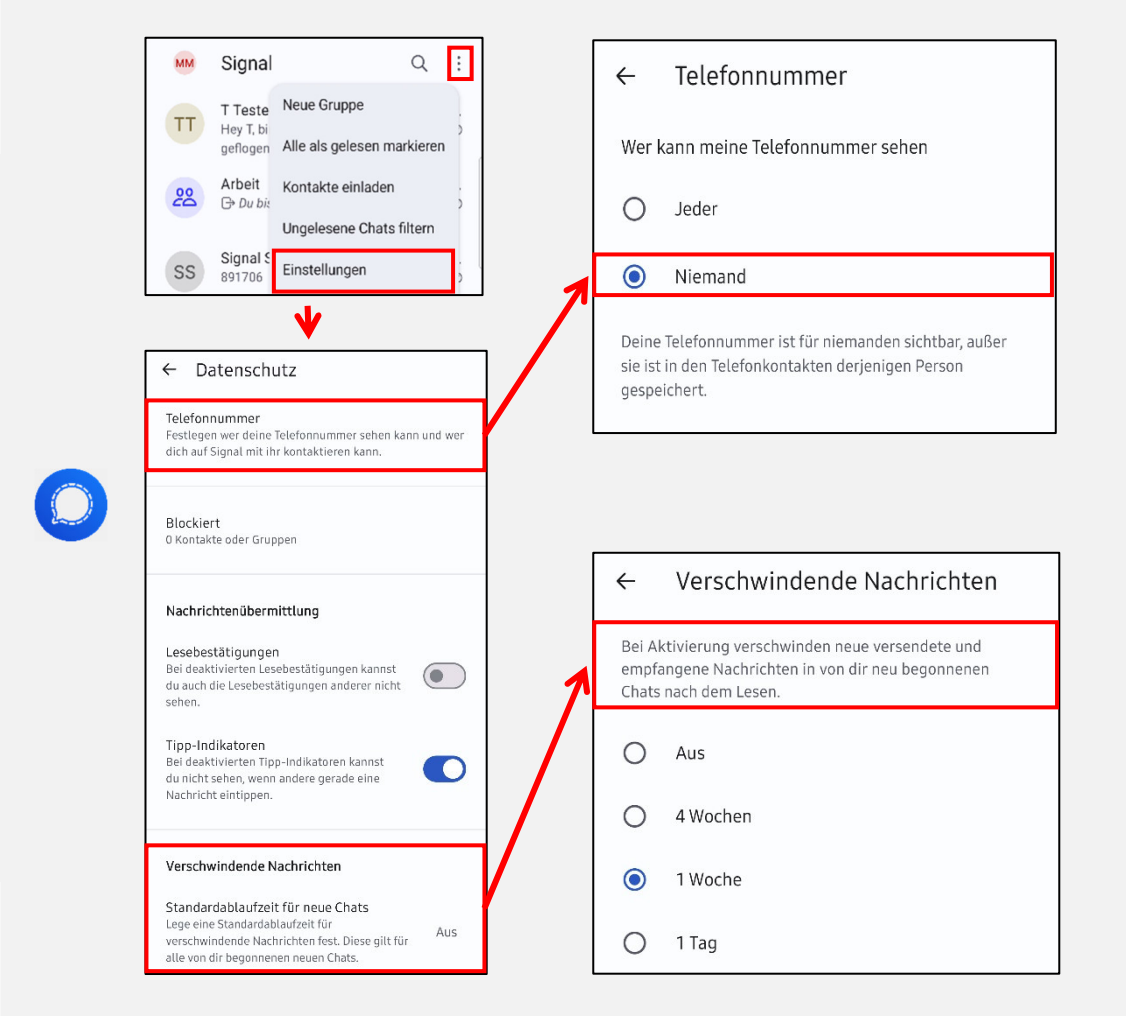


- **Aktivierung der Registrierungssperre:**
  Aktivieren Sie die „Registrierungssperre“. Diese Funktionen verhindern, dass Angreifer Ihr Konto auf anderen Geräten neu anmelden können.



- **Allgemeine Sicherheit erhöhen – Handynummer verbergen & automatische Nachrichtenlöschung:**
  Verbergen Sie Ihre Handynummer vor Anderen.

  Aktivieren Sie zudem die **automatische Löschung von Nachrichten** bei Ihnen und dem Empfänger nach einer von Ihnen definierten Zeitspanne.



- **Melden Sie die Angreifer:**
  Melden und blockieren Sie Profile, die sich als „Support“ ausgeben. Signal wird sich niemals mittels einer Direktnachricht an Sie wenden!

- **Schützen Sie sich und andere:**
  Informieren Sie Ihre Kontakte, dass unbefugte Dritte wahrscheinlich Ihre Kommunikation einsehen konnten. Nutzen Sie für den Schutz Ihres Umfeldes einen anderen Kommunikationskanal als den Messenger (z.B. E-Mail).

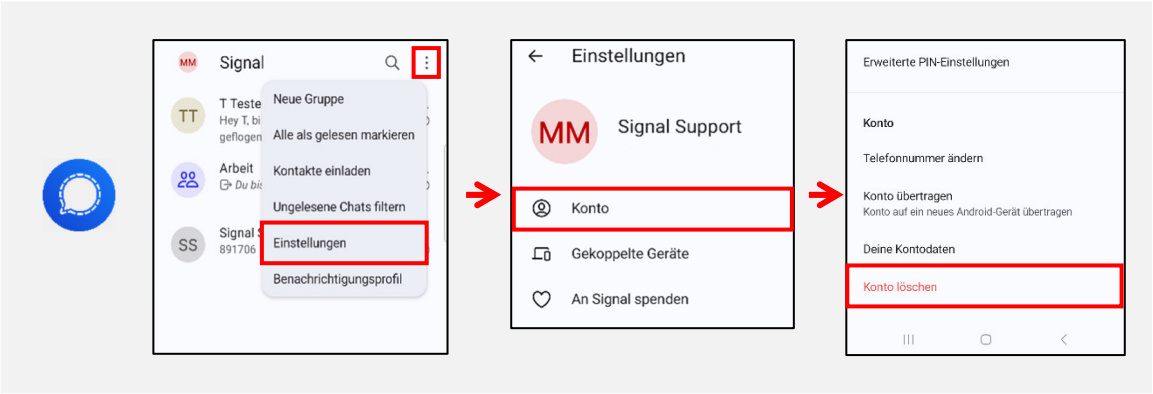
- **Sind Sie Administrator von Gruppenchats?**
  Prüfen Sie in allen Gruppen, ob auffällige Kontakte vorhanden sind – z.B. „Deleted Account" oder doppelte Einträge, oder ob sich auffällige Systemnachrichten über Änderungen von Sicherheitsnummern/ Namen im Chatverlauf häufen. **Entfernen Sie im Zweifel alle auffälligen Konten aus der Gruppe.** Kontaktieren Sie die Kontoinhaber auf einem anderen Weg als den Messenger.

Maßnahmenpaket 2: Erweiterte Gefahrenabwehr

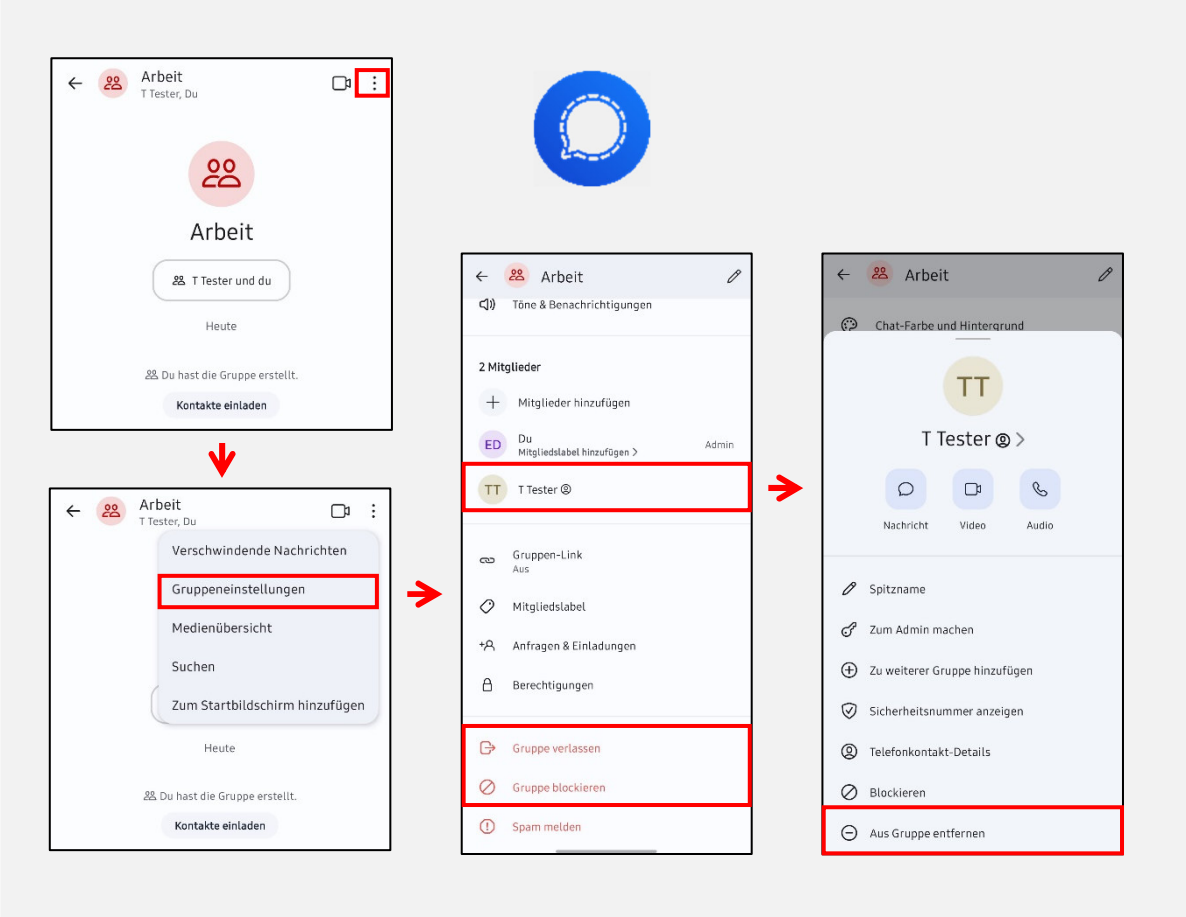
Szenario: Sie haben eine „Signal Support"-Nachricht erhalten, **Ihren SMS-Verifizierungscode und/ oder PIN eingegeben**, besitzen aber **weiterhin Zugang** zu Ihrem Konto

- **Konto-Löschung:**
  Die Angreifer sind mittels Ihres Verifizierungscodes bzw. Ihrer PIN in der Lage, Ihr Konto zukünftig zu übernehmen. **Löschen Sie Ihr aktuelles Messenger-Konto**.

  Sie brauchen <u>nicht</u> die App zu löschen! Das behebt nicht das Problem.



- **Umfeld kontaktieren und Gruppenbereinigung:**
  Kontaktieren Sie danach Ihr Umfeld und informieren Sie über den Vorfall. Lassen Sie dabei Ihren **alten Kontakt aus allen Gruppenchats löschen**!



- **Neues Messenger-Konto und neue PIN:**
  Erstellen Sie danach ein neues Messenger-Konto mit einer **neuen PIN**.

- **Durchführung folgender Schritte aus Maßnahmenpaket 1:**
  - **Aktivierung der Registrierungssperre**
  - **Handynummer verbergen & automatische Nachrichtenlöschung**
  - **Gruppenadministratoren: Überprüfung von Gruppen hinsichtlich Auffälligkeiten**

- **Angreifer kennen Ihre Handynummer:**
  Gehen Sie davon aus, dass die **Angreifer Ihre Handynummer kennen**. Möchten Sie sicher gehen, legen Sie sich eine **neue Mobilfunknummer** zu und registrieren Ihr neues Messenger-Konto mit dieser Nummer.

Maßnahmenpaket 3: Umfassende Integritätswiederherstellung

Szenario: Sie haben eine „Signal Support“-Nachricht erhalten, **Ihren SMS-Verifizierungscode und/ oder PIN eingegeben** UND haben **keinen Zugang** zu Ihrem Konto bzw. **mussten sich neu anmelden.**

Ihr Messenger-Konto ist vollständig von den Angreifern übernommen worden. Die Angreifer können alle Nachrichten, Dateien sowie Kontakte einsehen und können sich als Sie ausgeben. Eine Wiedererlangung der Kontrolle über Ihr Messenger-Konto ist nicht möglich.

- **Konto durch Signal löschen lassen:**
  Nur der Messenger-Dienst Signal kann jetzt Ihr altes Konto löschen. Kontaktieren Sie deshalb den echten Signal-Support unter

  https://support.signal.org/hc/de/requests/new

- **Schützen Sie sich und andere:**
  Kontaktieren Sie Ihr Umfeld über einen anderen Kommunikationskanal (z.B. E-Mail, Telefon). Informieren Sie darüber, dass ab dem Zeitpunkt der Kontoübernahme wahrscheinlich alle Kommunikation an einen unbefugten Dritten abgeflossen ist.

  Ihre Kontakte sollten unbedingt Ihr altes Messenger-Konto
  - in ihren Kontakten blockieren!
  - in allen Gruppen löschen lassen

  Gehen Sie auf Nummer sicher und raten Sie zudem dazu **die Gruppen selbst zu löschen**. Bei der Neuerstellung sollten nur über einen anderen Weg verifizierte Personen wieder in die Gruppen aufgenommen werden.

- **Durchführung folgender Schritte aus Maßnahmenpaket 1 und 2:**
  - **Angreifer kennen Ihre Handynummer – legen Sie sich eine neue zu**
  - **Neuregistrierung mit neuer Handynummer und neuer Sicherheits-PIN**

- **Aktivierung der Registrierungssperre**

- **Handynummer verbergen & automatische Nachrichtenlöschung**