



Sicherheit in Whatsapp-Gruppen



Mit Unterstützung von Pia Lamberty (Sozialpsychologin und Co-Geschäftsführerin von CeMAS)

Wenn ihr WhatsApp-Gruppen verwendet, um Hilfe zu koordinieren, solltet ihr euch bewusst sein, dass andere eure private Nummer sehen können. Das Gleiche gilt für Signal-Gruppen. Telegram wird ebenfalls häufig für die Koordination von Hilfe verwendet, da es einfacher ist, große Gruppen zu verwalten und private Nummern versteckt werden können. Allerdings sind Telegram-Nachrichten nicht verschlüsselt, was ein weiteres Sicherheitsrisiko darstellt.

- Wenn ihr nur Informationen senden wollt, aber keinen Austausch zwischen den Gruppenmitgliedern braucht, könnt ihr entweder die **neue Kanalfunktion von WhatsApp nutzen** oder die Einstellungen so ändern, dass **nur Administratoren Nachrichten senden können**
- Wenn ihr auf WhatsApp eine Gruppe mit Personen gründen wollt, die ihr nicht kennt, solltet ihr den **Link nicht in großen Gruppen auf Facebook oder eurem öffentlichen Instagram-Profil teilen**
- Stellt sicher, dass die Administratoren jedes **neue Mitglied der Gruppe genehmigen** müssen
- Stellt sicher, dass ihr die **Personen verifizieren** könnt, bevor sie den Link erhalten. Man kann den Link zum Beispiel an Personen auf Facebook schicken, nachdem man deren Profil überprüft hat.
- Falls der Link zu Ihrer Gruppe bereits online verbreitet wurde, erstellt einen neuen. Um den **Link zurückzusetzen**, klickt auf LINK ZURÜCKSETZEN

Auf Facebook überprüfen kann, ob ein Profil vertrauenswürdig ist:

- Prüf, wann das Profil erstellt wurde: Gefälschte oder feindliche Profile sind oft neue Profile ohne Freunde oder verdächtige Freundeslisten
- Verwende Google-Bildersuche, um zu sehen, ob das Profilbild von jemandem gestohlen wurde
- Überprüfe, ob das Profilbild künstlich erstellt wurde. Online findest du kostenlose Tools

<https://www.bellingcat.com/resources/2023/09/11/testing-ai-or-not-how-well-does-an-ai-image-detector-do-its-job>
<https://www.aiornot.com/>

Verwaltung auf WhatsApp

- Mitglieder sollten der Gruppe **nur über einen Link beitreten** können. Veröffentlicht den Link nicht in Foren oder auf Websites.
- Schränkt ein, **wer Änderungen an Gruppen vornehmen** kann. Admins bestimmen Änderungen am Betreff, am Symbol oder an der Beschreibung der Gruppe.
- **Löscht unerwünschte Nachrichten** oder entfernt Mitglieder. Admins können unerwünschte Nachrichten löschen oder Mitglieder aus der Gruppe entfernen.
- Admins können **einschränken, wer in der Gruppe posten darf**, wenn Admins nicht sicherstellen können, dass es sich um einen sicheren Raum handelt.
- Macht wiederholt darauf aufmerksam, dass diese **Gruppe möglicherweise nicht völlig sicher** ist.

Allgemeine Cyber-Sicherheit auf WhatsApp

- Vorsicht bei der Weitergabe privater Details: **Kennt ihr die Mitglieder der Gruppe?**
- Aktiviert 2stufige Verifizierung: Richtet eine geheime PIN ein, damit niemand das Konto stehlen kann. Wenn jemand versucht, auf das Konto zuzugreifen, muss er sowohl die PIN als auch einen 6-stelligen Code eingeben, der an die eigene Telefonnummer gesendet wird.
- Selbstlöschende Nachrichten: Man kann festlegen, wie lange Nachrichten sichtbar bleiben, nachdem sie gesendet worden sind - 24 Stunden, 7 Tage oder 90 Tage.
- Einmalige Ansicht für freigegebene Inhalte verwenden: Für mehr Privatsphäre können Fotos und Videos so gesendet werden, dass die nach einmaligem Öffnen aus dem Chat verschwinden.
- Vermeidet Gerüchte, virale Nachrichten und Fake News, indem Ihr Euch vor dem Weiterleiten von Inhalten vergewissert, dass diese korrekt sind - vor allem, wenn es sich um eine Kettennachricht handelt und der Hinweis "Vielfach weitergeleitet" angezeigt wird.

Mitglieder-Tools auf WhatsApp

- Überprüft die Gruppenberechtigungen. Du kannst entscheiden, wer dich zu einer Gruppe hinzufügen kann und ob du in einer Gruppe bleiben willst.
- Mitglieder sollten unangemessene oder schädliche Inhalte an WhatsApp melden.

Wir sind für euch da. We care. אכפת לנו