

Handreichung zu Threema

1.	Vorwort	1
2.	Systemvoraussetzungen	2
3.	Das Sicherheitskonzept von Threema	2
4.	Die Funktionen von Threema	3
5.	Schnelleinstieg	3
5.1.	Installation	3
5.2.	Inbetriebnahme	3
5.3.	Kontakte und Vertrauensstufen	4
6.	Fortgeschrittene Funktionen	4
6.1.	Backup und Wiederherstellung	4
6.2.	Threema Web	6
6.3.	Textformatierung	6
6.4.	Die Zustimmen/Ablehnen-Funktion	6
6.5.	Anpinnen-Funktion	6
6.6.	Empfangene Medien (Bild/Video/Audio) speichern	7
6.7.	Chats in der Android-App archivieren	7
6.8.	Private Chats	7
6.9.	Troubleshooting Gruppenchats	7
6.10.	Eine Gruppe löschen oder verlassen	8
6.11.	ID-Verwaltung im Profil-Menü	8

1. Vorwort

Nach eingehender Recherche hat sich das SHZ entschieden, den Messenger-Dienst Threema als Alternative zu dem gängigen, aber datenschutztechnisch höchst bedenklichen WhatsApp zu empfehlen.

Die Anwendung ist zwar nicht kostenlos, der einmalige Betrag von ca. 4€ scheint aber für die Leistung und Sicherheit, die Threema bietet, angemessen - Details s.u.

Grundsätzlich ist Threema, wie die meisten Messenger, sehr intuitiv in der Bedienung.

Die vorliegende Anleitung dient in erster Linie dazu, Sie durch die etwas spezielle Inbetriebnahme zu führen und zum schnellen Nachschlagen bei Fragen zu Grundfunktionen.

Hier sei auch auf die sehr ausführlichen Hilfeseiten auf www.threema.ch hingewiesen, auf denen man Antworten auch auf die feinsten Detailfragen findet.

2. Systemvoraussetzungen

Android:

Threema Vers. 4.22 oder höher auf Android Vers. 4.1 oder höher.

Um Anrufe zu empfangen, wenn die App im Hintergrund ist, sind Google Play Services erforderlich.

iOS:

- iPhone: Threema 3.0 für iOS oder höher auf einem iPhone 5s oder höher mit iOS 9 oder höher
- iPad: Threema 3.0 für iOS oder höher auf einem iPad Pro, einem iPad Air, einem iPad der 5. Generation oder höher oder einem iPad Mini 2 der 2. Generation oder höher mit iOS 9 oder höher

Diese Voraussetzungen müssen sowohl beim Anrufer wie auch beim Angerufenen erfüllt sein.

3. Das Sicherheitskonzept von Threema

Anders als die meisten Messengerdienste bietet Threema die Möglichkeit, den Dienst **völlig anonym** zu **nutzen**, d.h., ohne irgendwelche Daten von sich preiszugeben: weder Name noch Telefonnummer oder E-Mail-Adresse werden für die Nutzung oder das Anlegen einer Threema-Identität benötigt. Theoretisch könnte man Threema sogar auf einem Endgerät ohne SIM-Karte nutzen, solange dieses Internetzugang hat.

Lediglich zum Erwerben von Threema muss man eine E-Mail-Adresse angeben, um einen **Lizenzschlüssel** zu erhalten – oder man nutzt sein bereits vorhandenes Google Playstore oder Apple Appstore Account. Es ist auch möglich, mehrere Lizenzschlüssel zu erwerben und an Andere zu verteilen/verschenken.

Andererseits bietet Threema ein ausgefeiltes **Verifizierungssystem** an, das dem Nutzer bei Bedarf erlaubt, die Identität seiner Chat- oder Gesprächspartner so sicher zu überprüfen, dass **Identitätstäuschungen ausgeschlossen** werden können. Es ist also jedem Nutzer überlassen, das gewünschte Maß an Anonymität oder Vertraulichkeit nach eigenem Bedarf herzustellen.

Alle **Datenübertragungen** - auch Anrufe - sind **Ende-zu-Ende verschlüsselt** und laufen, soweit technisch möglich, nicht einmal über Threemas Server.

Daten werden ausschließlich auf den Endgeräten der Nutzer gespeichert. Die einzige – freiwillige - Ausnahme bildet das Threema Safe genannte Backup, welches man auf Threemas Server oder auch einem anderen Server seiner Wahl speichern kann.

4. Die Funktionen von Threema

Mit Threema kann man **Internetbasierte Anrufe** tätigen, beliebige **Dateien, Stimm- und Textnachrichten** austauschen. Als praktische Zugabe stehen eine **Abstimmfunktion** sowie eine **Bestätigen/Ablehnen-Funktion** zur Verfügung. Textnachrichten können auf übliche Weisen formatiert und an **Gruppenchats** oder **Verteilerlisten** statt einzelner Partner versendet werden. Threema kann man auf einem **mobilen Endgerät** und einem **Desktop synchron** nutzen, s.u. **Threema Web**.

5. Schnelleinstieg

5.1. Installation

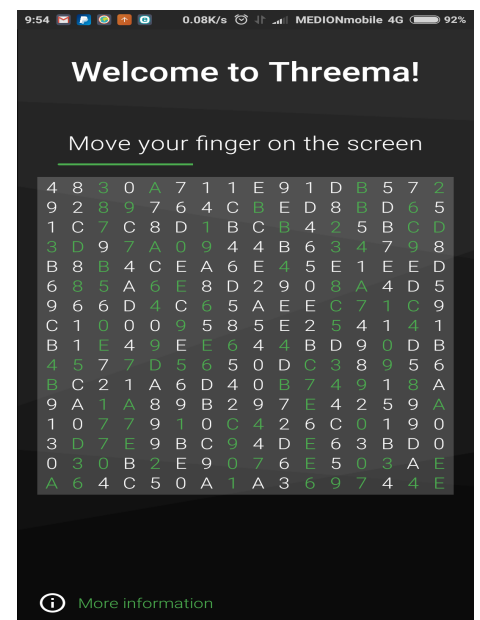
Nachdem man Threema über die Website Threema.ch, den Google Playstore oder den Apple App Store erworben hat, installiert man die App auf dem entsprechenden Endgerät auf die gewohnte Weise und gibt bei einer Erstinstallation den Lizenzschlüssel ein. Diesen sollte man aufbewahren, denn er gilt für alle späteren Neuinstallationen auf demselben Betriebssystem. **Wechselt man das Betriebssystem, braucht man einmalig einen neuen Lizenzschlüssel;** die wichtigsten Daten kann man aber Dank Threema Safe übertragen, s.u.

5.2. Inbetriebnahme

Nach dem erstmaligen Starten der App muss man die Datenschutzerklärung annehmen. Daraufhin legt man durch zufälliges Wischen über eine Matrix ein einzigartiges, nutzereigenes Schlüsselpaar an, mit dem fortan alle Kommunikationsdaten Ende-zu-Ende ver- und entschlüsselt werden. Seinen „**Schlüssel-Fingerabdruck**“ genannten Code findet man danach im Profil.

Nun bekommt man seine **Threema-ID** zugeteilt. Diese völlig anonyme Buchstaben-Zahlenfolge ist nun erst mal das Einzige, was andere Nutzer bei der Kommunikation mit Ihnen zu sehen bekommen.

In den nächsten Schritten können Sie ein Passwort für den **Threema Safe** anlegen (s.u. Backup und Wiederherstellung), sich ein **Nickname** zulegen, Ihre ID mit einer **Telefonnummer verknüpfen** (diese wird von Threema später mit einer Bestätigungs-SMS geprüft, um Identitätstauschung vorzubeugen) und Ihre





Kontaktdaten synchronisieren, um automatisch herauszufinden, welche Kontakte aus Ihrem Telefonbuch ebenfalls Threema nutzen. All diese Schritte können aber auch weitergeklickt werden, falls man völlig anonym bleiben möchte, und später in den Profileinstellungen nachgeholt werden.


Nun ist Threema eingerichtet und man kann seine Threema-Kontakte anrufen oder Nachrichten mit Ihnen austauschen.

5.3. Kontakte und Vertrauensstufen

Hat man seine Kontaktdaten mit dem Telefonbuch synchronisiert oder Kontakte händisch angelegt, wird man den feststellen, dass jedem Kontakt eine Vertrauensstufe zugeordnet ist, die mit farbigen Punkten ausgedrückt wird. Diese Punkte sind ein Maß für die Sicherheit, dass die ID eines Kontakts wirklich zu diesem gehört:

 **Stufe 1 (rot):** Da kein passender Kontakt im Adressbuch gefunden wurde (mit Handynummer/E-Mail), kann man sich nicht sicher sein, ob die Person wirklich die ist, die sie in ihren Nachrichten vorgibt zu sein.

 **Stufe 2 (orange):** Der Kontakt wurde im Adressbuch gefunden (mit Handynummer oder E-Mail). Da der Server Handynummern und E-Mail-Adressen prüft (SMS bzw. E-Mail mit Aktivierungslink), kann man sich ohne zusätzliches Verifizieren relativ sicher sein, dass diese Person wirklich diejenige ist, die man meint.

 **Stufe 3 (grün):** Der öffentliche Schlüssel der Person wurde persönlich durch Scannen des QR-Codes verifiziert. Dies ist eine Besonderheit von Threema: um eine Person, der man persönlich begegnet, seinen Kontakten hinzuzufügen, kann man Ihren einzigartigen ID-QR Code scannen. Dieser befindet sich in den Profileinstellungen. Solange das Gerät dieser Person nicht gestohlen/gehackt wurde, ist damit ausgeschlossen, dass ein Dritter Nachrichten von dieser Person fälschen oder Nachrichten an diese Person mitlesen kann.

6. Fortgeschrittene Funktionen

6.1. Backup und Wiederherstellung

Threema speichert stillschweigend nur den sog. öffentlichen Schlüssel und Ihre ID auf dem Server; Es ist daher essentiell wichtig, Backups anzulegen, um den Verlust von Daten, Nachrichten oder sogar seiner ID zu vermeiden, falls man sie sich nicht notiert hat.

Hierzu stehen Ihnen **2 Möglichkeiten** zur Verfügung: das **serverbasierte Threema Safe** und das auf dem Endgerät **lokal zu speichernde Daten-Backup**. Beide Optionen sind aus dem Threema-Hauptmenü verfügbar (drei Punkte rechts oben), die Backups werden mit einem frei gewählten Passwort geschützt und können daher nur von Ihnen selbst wiederhergestellt werden.

Threema Safe sichert regelmäßig **grundlegende Daten** auf dem Threema-Server oder einem anderen Server Ihrer Wahl. **Threema Safe ist plattformunabhängig**. Egal, in welcher Threema-Version (Android, iOS oder Windows Phone) ein Threema Safe-Backup erstellt wurde, es lässt sich auf jeder Plattform wiederherstellen. Das erlaubt Ihnen, Ihre folgend aufgeführten, grundlegenden Daten bequem von einer Plattform auf eine andere zu übertragen:

- Ihre Threema-ID
- Ihr Nickname
- Ihr Profilbild
- Ihre Kontakte (inkl. Vertrauensstufe)
- Ihre Gruppenzugehörigkeiten
- Android: Ihre Verteilerlisten

Zudem enthalten Threema Safe-Backups folgende Privatsphäre-Einstellungen:

- Kontakte synchronisieren
- Unbekannte blockieren
- Lesebestätigungen senden
- Melden wenn ich tippe
- Ausschlussliste
- Blockierte Kontakte
- Threema-Anrufe aktivieren
- Anrufe immer über Server
- Android: Miniaturen in Screenshots verhindern
- Android: Inkognito-Tastatur anfordern

In Threema Safe-Backups nicht enthalten sind Nachrichtenverläufe und Medien sowie Profilbilder von Kontakten und Gruppen.

Um Nachrichtenverläufe zu sichern, legen Sie **Daten-Backups** an. Diese lassen sich einfach als Datei auf unterschiedliche Geräte **übertragen**; jedoch **nur auf demselben Betriebssystem!**

Zum **Wiederherstellen** gespeicherter Daten wählt man beim Einrichten einer neu installierten Threema-App einfach die entsprechende Option aus.

6.2. Threema Web

erlaubt es, auf einem mobilen Gerät und einem Computer synchron zu arbeiten. Zum Starten öffnen Sie auf Ihrem Computer web.threema.ch (mit einem unterstützten Browser), wählen in der Threema-App durch Antippen der drei Punkte oben rechts «Threema Web» und folgen Sie den Anweisungen, die je nach Endgerät etwas variieren können. Schließlich scannen Sie mit Ihrem Mobilgerät den auf web.threema.ch angezeigten QR-Code.

6.3. Textformatierung

Flankieren Sie einfach den zu formatierenden Text mit dem entsprechenden Zeichen:

- ***fett***
- *_kursiv_*
- ~~~durchgestrichen~~~

6.4. Die Zustimmung/Ablehnen-Funktion

erlaubt, eingehende Nachrichten zu bestätigen oder abzulehnen, ohne beim Chat-Partner eine Push-Benachrichtigung auszulösen. So kann unaufdringlich die eigene Haltung gegenüber einer Nachricht signalisiert werden.

Tippen Sie in einem Einzel-Chat lange auf eine empfangene Nachricht, um das Kontext-Menü aufzurufen. Wählen Sie «Bestätigen / Daumen hoch», um der Nachricht zuzustimmen, oder «Ablehnen / Daumen runter», um sie abzulehnen. In Gruppen-Konversationen steht das Zustimmung und Ablehnen von Nachrichten nicht zur Verfügung.

6.5. Anpinnen-Funktion

setzt eine visuelle Erinnerung, wenn in einem Chat Handlungsbedarf besteht oder noch Fragen offen sind. Angepinnte Chats stehen in der Chatübersicht zuoberst und sind mit einem gelben Balken markiert. Unter Android wird zudem ein Pinnadel-Symbol angezeigt.

- **Android/iOS:** Streichen Sie in der Chatübersicht von links nach rechts über den gewünschten Chat, um ihn anzupinnen bzw. zu entpinnen
- **Threema Web:** Öffnen Sie den gewünschten Chat, und tippen Sie rechts oben auf das Pinnadel-Symbol, um den Chat anzupinnen bzw. zu entpinnen

6.6. Empfangene Medien (Bild/Video/Audio) speichern

Tippen Sie das gewünschte Medium im Chat lange an und wählen Sie dann den Menüpunkt «Speichern» (Disketten-Symbol). Das gespeicherte Medium befindet sich danach im Verzeichnis «Threema/Threema Pictures» (resp. «Threema Videos» oder «Threema Audio»). Dateien werden im globalen «Download»-Verzeichnis des Geräts gesichert und sind über die «Downloads»-App abrufbar.

6.7. Chats in der Android-App archivieren

Wischen Sie in der Chat-Übersicht auf einem Chat von rechts nach links, um ihn zu archivieren. Dabei wird der Chat nicht gelöscht, sondern bloß aus der Chat-Übersicht entfernt.

Sie gelangen zu den archivierten Chats, indem Sie ans Ende der Chat-Übersicht scrollen und dort die «X archivierte Chats»-Schaltfläche betätigen.

Um einen Chat aus dem Archiv zurück in die Chat-Übersicht zu verschieben, tippen Sie darauf, bis in der Titelleiste die Aktions-Symbole eingeblendet werden, wo Sie auf das Symbol neben dem Abfalleimer-Symbol tippen.

6.8. Private Chats

Sie können **Chats durch eine PIN schützen** und nach Wunsch **in der Chatübersicht ausblenden**. Damit sind vertrauliche Inhalte vor neugierigen Blicken geschützt. Bei privaten Chats wird in den Push-Benachrichtigungen nur der Name des Absenders angezeigt.

Um diese Funktion unter Android zu nutzen, aktivieren Sie in den Threema-Einstellungen unter «Sicherheit» den PIN Code oder die Android System-Displaysperre.

Unter iOS stehen Private Chats derzeit nicht zur Verfügung.

Um einen Chat als privat zu markieren, tippen Sie lange auf den betreffenden Chat und wählen Sie anschließend «Chat verstecken». Beim Öffnen des Chats muss nun der PIN-Code oder die System-Displaysperre eingegeben werden.

Um die privaten Chats auszublenden, tippen Sie in der Chatliste auf das Menü und dann auf «Private Chats verstecken». Um die Chats wieder anzuzeigen, wählen Sie «Private Chats anzeigen» im Menü der Chatliste und geben die PIN ein.

6.9. Troubleshooting Gruppenchats

Es kann vorkommen, dass Gruppen asynchron werden. Grund dafür kann z.B. sein, dass ein Teilnehmer ein Daten-Backup einspielt hat oder längere Zeit offline war. In diesem Fall kann helfen, die Gruppe neu zu synchronisieren. Der Administrator einer Gruppe kann eine Synchronisation anstoßen (in den Gruppen-Details). Sollte die

Synchronisation das Problem nicht beheben, kann man den betreffenden Teilnehmer entfernen und neu hinzufügen.

Die Gruppen-Details können wie folgt aufgerufen werden:

- **Android:** Tippen Sie im Gruppenchat auf die Titelleiste.
- **iOS:** Tippen Sie im Gruppenchat auf die Titelleiste und anschließend auf die direkt darunter erscheinende Leiste.

Sehen einige Teilnehmer keine Nachrichten im Gruppenchat, haben diese evtl. die Option «Unbekannte blockieren» aktiviert. Diese Option schalten sie in Threema > «Einstellungen» > «Privatsphäre» aus, um alle Nachrichten im Gruppenchat zu erhalten.

6.10. Eine Gruppe löschen oder verlassen

Android

Als Administrator einer Gruppe können Sie Gruppen als Ganzes löschen, ohne dass jedes einzelne Mitglied entfernt werden muss. Die Gruppe kann danach auch von den anderen Mitgliedern nicht mehr genutzt werden.

Gruppenchat aufrufen > auf Gruppenname in Titelzeile tippen > Menü > «Gruppe löschen»

Sind Sie nicht der Administrator einer Gruppe, können Sie aus der Gruppe austreten. Die Chat-Inhalte selbst werden dabei nicht gelöscht:

Gruppenchat aufrufen > auf Gruppenname in Titelzeile tippen > Menü > «Gruppe verlassen».

Um einen Gruppenchat aus der Chatliste zu entfernen und den Chatverlauf zu löschen, tippen Sie lange auf den Chat und wählen dann das Papierkorb-Symbol.

iOS

Gruppen, die von einem iOS--Nutzer gegründet wurden, werden erst gelöscht, sobald das letzte Mitglied die Gruppe verlassen hat.

Um eine Gruppe zu verlassen, wischen Sie in der Chat- oder Gruppen-Übersicht von rechts nach links und tippen auf «Löschen».

6.11. ID-Verwaltung im Profil-Menü

Möchten Sie Ihre **ID komplett vom Threema Server löschen**, wählen Sie die Option **ID-Widerruf**. Diese Aktion wird mit einem von Ihnen zu vergebenden Passwort geschützt, um Missbrauch zu vermeiden.

Wollen Sie eine **neue ID auf Ihrem Endgerät einrichten** oder **eine neue Rufnummer/E-Mail Adresse mit Ihrer alten ID** benutzen, wählen Sie auf Ihrem Gerät zunächst die Option **ID löschen**. Damit löschen Sie auch Ihre Chats – denken Sie also daran, zuvor ein **Backup anzulegen!**

Fragen, Ergänzungen, Rückmeldungen bitte an:

Juri Chervinski, Tel.: 089 / 53 29 56-28, juri.chervinski@shz-muenchen.de

© Selbsthilfezentrum München, Westendstraße 68, 80339 München, www.shz-muenchen.de

Trägerverein des Selbsthilfezentrums München: FöSS e.V. (Verein zur Förderung der Selbsthilfe und Selbstorganisation e.V.)



Gefördert von der
Landeshauptstadt
München

Das Selbsthilfezentrum wird gefördert von der Landeshauptstadt München (Sozialreferat und Referat für Gesundheit und Umwelt) sowie von der Fördergemeinschaft der gesetzlichen Krankenkassenverbände in Bayern.