

Anleitung LOGINEO Messenger: Sicherheit

Schlüsselsicherung, Sicherungsphrase, Verifizierung.

Das Thema Sicherheit ist bei dem LOGINEO NRW Messenger sehr wichtig. Deshalb müssen nach der Erst-Anmeldung verschiedene Schritte durchgeführt werden, um diese Sicherheit zu gewährleisten.

Grundsätzlich gibt es 3 wichtige "Schlüssel", die sicher verwahrt werden müssen:

- ein selbst gewähltes **Kennwort** zur Anmeldung
- eine selbst gewählte **Sicherheitsphrase**
- ein automatisch generierter 48-stelliger **Sicherheitscode**

Im Folgenden wird gezeigt, wie man die erforderlichen Einstellungen im Browser vornimmt. Je nach Betriebssystem, Gerät und Anwendung (Browser oder App) variieren die Bilder leicht, der Vorgang selbst bleibt jedoch gleich.

Schlüsselsicherung – was ist das?

Die Schlüsselsicherung ist ein abgesicherter Raum auf dem Server, in dem alle Schlüssel hinterlegt sind, die gebraucht werden, damit du deine Nachrichten lesen kannst. Der Raum kann nur mit deinen Passwörtern geöffnet werden.

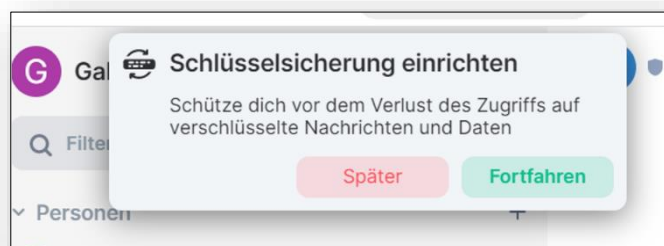
Durch die Aktivierung werden alle Verschlüsselungen, die deine Chatnachrichten und Chaträume unkenntlich machen, sicher in einem Schlüsselserver aufbewahrt. Diesen Server kannst du dir als einen Safe vorstellen, der sich auf dem Hauptserver befindet. Wenn du die Schlüsselsicherung nicht aktivierst, kannst du ältere Nachrichten, die du vielleicht vor einigen Tagen geschrieben oder empfangen hast, nicht mehr lesen.

In diesem Video wird dir erklärt, warum die Schlüsselsicherung so wichtig ist:
[Quelle: <https://www.logineo.schulministerium.nrw.de/>]



Schlüsselsicherung einrichten

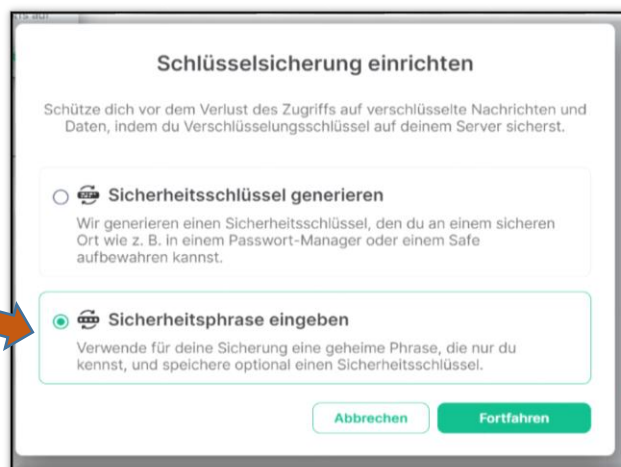
Nach der ersten Anmeldung die folgende Aufforderung:



Falls du das Einrichten auf SPÄTER verschiebst, kannst du den Messenger nicht in vollem Umfang nutzen: ältere Nachrichten werden dann verschlüsselt und können nicht mehr gelesen werden. Klicke deshalb auf FORTFAHREN.

Klicke im nächsten Schritt auf den grünen Kreis: **Sicherheitsphrase eingeben**.

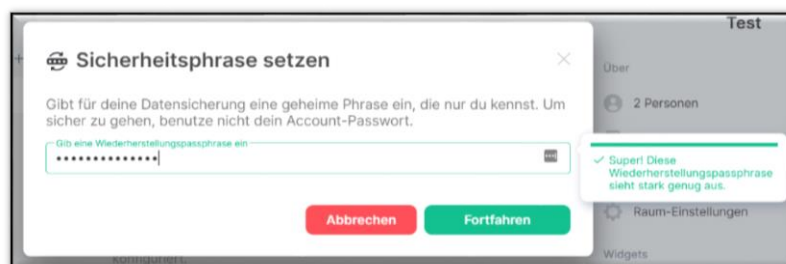
Dann wähle FORTFAHREN.



Mit „Phrase“ ist nicht unbedingt ein Satz gemeint, sondern vielmehr ein besonders **sicheres Kennwort**. Es sollte ausreichend Zeichen beinhalten, außerdem mindestens eine Ziffer, ein Sonderzeichen, Groß- und Kleinbuchstaben.

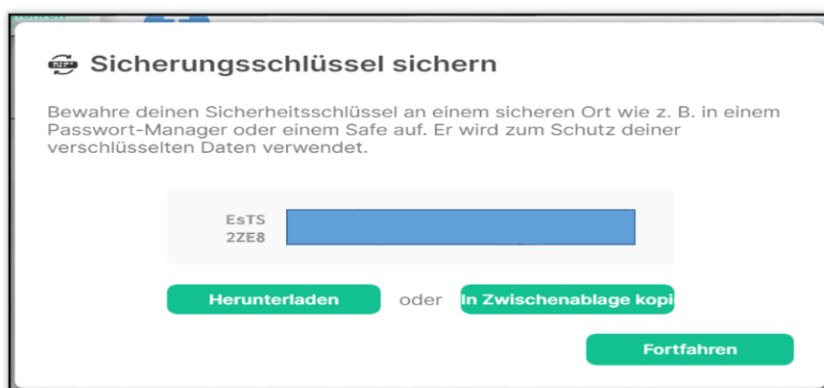
Tipp: Setze Sonderzeichen (#, &, !, ...) hinter das Kennwort, das du zur Anmeldung gewählt hast.

Vermerke es dir an einem sicheren Ort.



Zur Überprüfung wirst du, nachdem du auf FORTFAHREN geklickt hast, ein weiteres Mal aufgefordert, die Sicherheitsphrase einzugeben. Falls du lieber eine andere Wahl triffst, kannst du an diesem Punkt auch noch einmal zurückgehen und ein neues Kennwort wählen.

Nachdem alles bestätigt wurde, wird dein 48-stelliger **Sicherungsschlüssel** generiert.



Diesen Schlüssel kannst du dir herunterladen oder kopieren, um ihn an sicherer Stelle zu verwahren.

Was bedeutet Cross-Signing?

Jede Anmeldung wird beim Messenger als eine eigene Session gesehen. Cross-Signing bedeutet, dass du in jeder Session auf deine Nachrichten sicher zugreifen kannst. Überspringt man die erforderlichen Schritte, kann man die Nachrichten nicht lesen und erhält den Hinweis, dass sie nicht entschlüsselt werden können. Das trifft auf die von dir gesendeten Inhalte ebenso zu wie auf die empfangenen Nachrichten, wenn der/die Sender:in die Sicherheitsvorkehrungen nicht getroffen hat.

Die Nachricht kann auf Deutsch oder Englisch erscheinen, z.B.

"kann nicht entschlüsseln. Die Sitzung des/r Absenders:in hat uns keine Schlüssel für diese Nachricht gesendet."

Durch den Sicherungsschlüssel (s.o.) hast du den sicheren Zugang an *einem* Gerät bereits bestätigt. Wenn du nun ein weiteres Gerät (z.B. dein Handy oder Tablet) nutzen möchtest oder den Messenger im Browser statt der App öffnest, muss nachgewiesen werden, dass dieser Zugriff ebenfalls sicher ist.

Aus diesem Grund wirst du aufgefordert, die neue Session zu verifizieren. Das System gibt dann die entsprechenden Schlüssel weiter, sodass die Nachrichten wieder gelesen werden können.

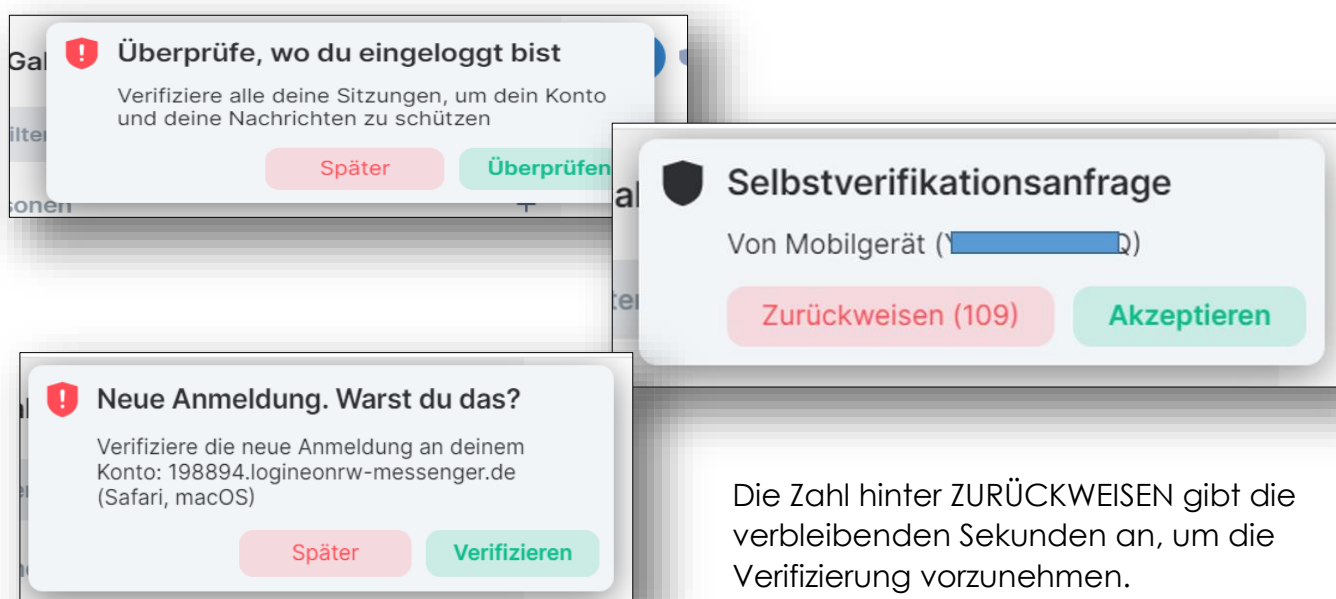
Dieser sichere Austausch findet über die Verifizierung statt.

Verifizierung

Am besten ist es, wenn du die Verifizierung direkt für alle Geräte durchführst, die du regelmäßig nutzt. Es ist möglich, dass du später ein weiteres Mal aufgefordert wirst, die Verifizierung zu wiederholen. Die folgenden Bilder können je nach Gerät/Anwendung variieren, das wording bleibt ähnlich.

Ausgangslage ist, dass du dich an einem Gerät angemeldet hast, inklusive Erstellung der Sicherheitsphrase und Speichern des Sicherheitscodes.

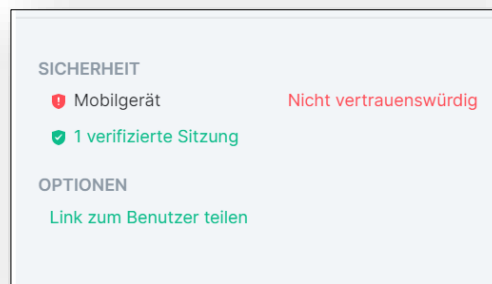
Wenn du dich nun über ein anderes Gerät oder über den Browser statt App anmelden möchtest, erscheint eine der folgenden Anzeigen:



Die Zahl hinter ZURÜCKWEISEN gibt die verbleibenden Sekunden an, um die Verifizierung vorzunehmen.

Am PC kannst du auch rechts unten deine angemeldeten Geräte („Sessions“) sowie den Stand der aktuellen Verifizierung sehen.

Diese Anzeige bedeutet, dass ein Mobilgerät/Handy noch nicht verifiziert wurde, also nicht sicher ist.



Was ist zu tun?

Öffne den Messenger auf deinem zweiten, bereits sicher angemeldeten Gerät. Es erscheint ebenfalls eine Aufforderung zur VERIFIZIERUNG. Klicke sie an und bestätige die Freischaltung für das „neue“ Gerät/die „neue“ Anwendung.

Du kannst die Sitzung auch durch den Abgleich mit Emojis verifizieren. Dann erscheint auf beiden Geräten eine bestimmte Auswahl an Bildern.

Stimmen diese überein, wähle auf beiden Geräten: SIE PASSEN ZUEINANDER.



Alternativ kannst du die Sitzung auch durch die Sicherheitsphrase/den Sicherheitscode verifizieren.

Ab jetzt ist die Kommunikation in beiden Sessions sicher!

Wenn du weitere Geräte verifizieren möchtest, wiederhole die obigen Schritte.

Keine Sicherheitsphrase, kein Code, kein zweites Gerät?

Wenn alle Schlüssel verloren sind und kein zweites Gerät für die Verifizierung zur Verfügung steht, kann alles zurückgesetzt werden und der Account neu verschlüsselt werden.

Gruppen bleiben bestehen, allerdings gehen voraussichtlich alle bisherigen Nachrichten verloren.