

## Instahelp setzt neue Maßstäbe im Bereich der Datensicherheit

Mit [Instahelp](#), der Plattform für psychologische Online-Beratung, bieten wir eine anonyme Möglichkeit für Personen, sich mit intimen und geheimen Anliegen und Problemen an erfahrene Psychologen zu wenden. Unsere Psychologen helfen Ratsuchenden via Chat, durch Selbsthilfe zu Lösungen zu finden und die eigene Persönlichkeit weiterzuentwickeln. Diese Kommunikation baut auf einem enormen Vertrauensverhältnis auf, das mit allen Möglichkeiten geschützt werden muss. Aus diesem Grund wurden für Instahelp drei unterschiedliche Sicherheits-Mechanismen umgesetzt, welche die sensiblen Nachrichten vor Zugriff von außen schützen.

### 3-fache Sicherheit für Instahelp Nachrichten

1. Verschlüsselung der Daten vor dem Versand (Ende-zu-Ende-Verschlüsselung)
2. Abgesicherte Datenübertragung (TLS)
3. Zwei-Faktor-Authentifizierung (2FA)

#### 1. Verschlüsselung der Daten vor dem Versand

Bei Instahelp werden alle Nachrichten zwischen Ratsuchendem und Psychologen mit einem geheimen Raum-Schlüssel verschlüsselt. Dieser geheime Raum-Schlüssel wird von Instahelp automatisch für jeden privaten Beratungsraum einmalig auf dem Gerät des Ratsuchenden generiert. Damit der Ratsuchende sich den geheimen Raum-Schlüssel nicht merken muss, wird dieser wiederum verschlüsselt auf dem Instahelp Server gespeichert. Zur Verschlüsselung des geheimen Raum-Schlüssels wird das persönliche kryptografische Schlüsselpaar (privater und öffentlicher Schlüssel) des Nutzers verwendet. Dieses Schlüsselpaar wird auf Basis des Passworts des Nutzers generiert und ist somit - aus technischer Sicht - nur dem Nutzer „bekannt“.

Wird dem Ratsuchenden ein Instahelp Psychologe in seinem privaten Beratungsraum zugewiesen, benötigt dieser den geheimen Raum-Schlüssel, um die Nachrichten entschlüsseln zu können. Hierfür wird der persönliche öffentliche Schlüssel vom Psychologen gemeinsam mit der Anfrage um Freigabe des geheimen Raum-Schlüssels an den Ratsuchenden übermittelt. Sofern der Ratsuchende online ist, verschlüsselt Instahelp nun den geheimen Raum-Schlüssel mit dem öffentlichen Schlüssel des Psychologen und sendet diesen über die gesicherte Verbindung zurück. Nun wird der geheime Raum-Schlüssel mit dem privaten Schlüssel des Psychologen (den nur er „kennt“) entschlüsselt, mit welchem wiederum die Nachrichten entschlüsselt und angezeigt werden können.

Zur besseren Verständlichkeit gibt es hier ein einfaches Beispiel:



Der Ratsuchende schreibt eine Chat-Nachricht: „... chronische Schlafprobleme ...“ Zum Absenden der Nachricht klickt er auf den Button „Senden“. Bevor die Nachricht verschickt wird, verschlüsselt die Instahelp App die Nachricht mit dem geheimen Raum-Schlüssel.

1. Die verschlüsselte Nachricht wird nun an den Instahelp Server übertragen und in der Datenbank verschlüsselt gespeichert "%&A(!)A019!1#2%". Die ausfallssicheren Instahelp Server befinden sich im Datacenter des Cloud-Anbieters 1&1 in Deutschland (Frankfurt) und unterliegen deutschem Datenschutz.
2. Der zugewiesene Instahelp Psychologe fordert nun die neue Nachricht beim Instahelp Server an und bekommt die verschlüsselte Nachricht an seinen Computer geschickt. Da der Psychologe im Besitz des gemeinsamen geheimen Raum-Schlüssels ist, kann er die Nachricht entschlüsseln und lesen.

#### 2. Abgesicherte Datenübertragung



Obwohl die Nachrichten bereits verschlüsselt sind, werden sie zusätzlich über eine abgesicherte Datenverbindung zum Instahelp Server übertragen. Hierfür wird der Industrie Standard TLS 1.2 (Transport Layer Security) verwendet, um die folgenden Sicherheiten zu gewährleisten:

- Für die Verbindung zum Instahelp Server wird ein Einmal-Schlüssel (AES\_128\_GCM) erzeugt, der zwischen dem Ratsuchenden und dem Instahelp Server automatisch digital ausgetauscht wird. Die zu sendenden Daten werden vor dem Versand mit diesem Einmal-Schlüssel verschlüsselt und an den Instahelp Server geschickt.
- Für jede gesendete Nachricht wird zusätzlich ein einmaliger Nachrichten Authentizitäts-Code (=Sequenz) generiert und nach erfolgreicher Übertragung deaktiviert.

#### 3. Zwei-Faktor-Authentifizierung (2FA)



Mit der dritten Sicherheitsmaßnahme stellen wir sicher, dass der in der Kommunikation involvierte Instahelp Psychologe tatsächlich die erwartete Person repräsentiert. Aus diesem Grund müssen alle Instahelp Coaches und Instahelp Psychologen beim Einloggen eine Zwei-Faktor-Authentifizierung durchführen. Diese zwei Faktoren sind stellvertretend für zwei Eigenschaften, welche die Person **wissen** und **besitzen** muss. Das Wissen bezieht sich auf die Eingabe des selbst festgelegten Passworts. Der Besitz erfordert das Smartphone zur Hand, um einen per SMS zugestellten PIN-Code einzugeben (vergleichbar mit E-Banking). Somit muss der Instahelp Psychologe das Passwort wissen und das Smartphone mit seiner Rufnummer besitzen, um sich erfolgreich einzuloggen.

## Häufige Fragen

### **Warum werden die Nachrichten am Instahelp Server gespeichert?**

Mit Instahelp verfolgen wir das Ziel, psychologische Beratung in den Alltag zu integrieren. Der Psychologe soll jederzeit und von überall aus erreichbar sein. Ratsuchende können sich jederzeit auf dem Smartphone, Tablet oder auch am Computer bei Instahelp einloggen, um den Chat-Verlauf sowie auch neue Antworten vom Psychologen einzusehen und auch sofort darauf zu antworten. Hierfür werden die Chat-Nachrichten am Instahelp Server verschlüsselt gespeichert, um jederzeit abrufbar zu sein.

### **Wie werden die Nachrichten verschlüsselt?**

Zur Verschlüsselung der Daten wird die weit verbreitete und anerkannte [LibSodium Kryptographie Bibliothek](#) verwendet. Jede einzelne Chat-Nachricht wird mit einem symmetrischen Raum-Schlüssel auf Basis des Verfahrens [Salsa 20](#) (64 Bit) verschlüsselt. Zusätzlich wird jede Nachricht nach der Übertragung auf Manipulationen überprüft, mittels Authentifizierung der Nachricht über [Poly 1305 MAC](#).

### **Was passiert, wenn ein Hacker alle Daten vom Instahelp Server stiehlt?**

Falls ein Hacker alle Sicherheitsmechanismen unseres Datacenters durchbricht, findet er nur unlesbare verschlüsselte Nachrichten vor. Da ein jeder Ratsuchende bei Instahelp seinen eigenen geheimen Raum-Schlüssel verwendet, müsste der Hacker pro Ratsuchendem versuchen, den Schlüssel zu knacken.

### **Wie gelange ich zu einem geheimen Raum-Schlüssel mit dem Psychologen? Muss man sich diesen merken?**

Nein, Instahelp verwendet ein ausgeklügeltes System, um den einmalig generierten geheimen Raum-Schlüssel wiederherzustellen. Zunächst wird das beim Login eingegebene Passwort in Kombination mit einem Zeichenzusatz vom Server (SALT) mit einer Hash-Funktion (Salsa 20/8 + SHA-256) zu einer langen Zeichenfolge (=Digest) konvertiert. Der SALT wird verwendet, um ein einfaches Passwort durch Hinzufügen einer langen zufälligen Zeichenfolge komplexer zu machen. Der Vorteil der Hash-Methode ist, dass der generierte Digest (=Zeichenfolge) nicht mehr auf die ursprüngliche Zeichenfolge rückgeführt werden kann und somit das Passwort des Nutzers nicht am Instahelp Server gespeichert werden muss. Mit diesem Digest wird nun der private und öffentliche Schlüssel (Curve25519 (Key exchange) + Salsa 20 (Encryption) + Poly 1305 MAC (Authentication)) des Nutzers generiert. Dieses Schlüsselpaar kann nun den vom Instahelp Server angeforderten verschlüsselten Raum-Schlüssel entschlüsseln.