Instahelp

Instahelp relies on state-of-the-art data protection standards

With Instahelp, the platform for psychological online counselling, we offer an anonymous possibility for people to turn to experienced psychologists with private and professional concerns and problems. Our psychologists help clients via text chat, audio or video to find solutions through self-help and to develop their own personality. This communication is based on an enormous relationship of trust, which must be protected with all possible means. For this reason, three different security mechanisms were implemented for Instahelp, which protect the sensitive messages from external access.

3-fold security for Instahelp messages:

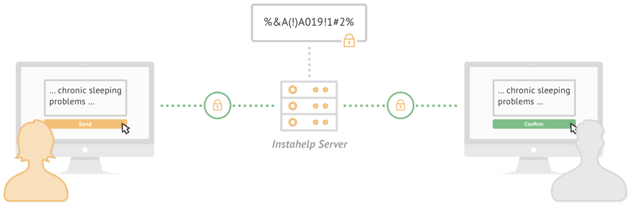
1. End-to-end encryption
2. Secured data transmission (TLS)
3. Two-factor authentication (2FA)

1. End-to-end encryption

At Instahelp, all messages between clients and psychologists are encrypted with a secret room key. This secret room key is automatically generated by Instahelp for each private counselling room on the client's device. So that the client does not have to remember the secret room key, it is stored in encrypted form on the Instahelp server. The user's personal cryptographic key pair (private and public key) is used to encrypt the secret room key. This key pair is generated on the basis of the user's password and is therefore - from a technical point of view - only "known" to the user.

If an Instahelp psychologist is assigned to the client in his:her private counselling room, the client needs the secret room key to decrypt the messages. For this purpose, the personal public key of the psychologist is transmitted to the client together with the request to share the secret room key. If the client is online, Instahelp encrypts the secret room key with the public key of the psychologist and sends it back via the secure connection. Now the secret room key is decrypted with the private key of the psychologist (which only he:she "knows"), which in turn can be used to decrypt and display the messages.

For better comprehension, here is a simple example:


%&A(!)A019!1#2%
... chronic sleeping problems ...
Send
Instahelp Server
... chronic sleeping problems ...
Confirm

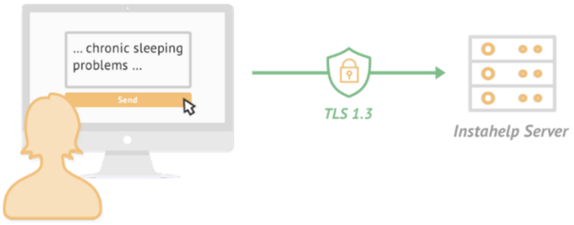
The customer writes a chat message: ".... chronic sleep problems ..." To send the message, he:she clicks on the "Send" button. Before the message is sent, the Instahelp app encrypts the message with the secret room key.

1. The encrypted message is now transmitted to the Instahelp server and stored in the database in encrypted form "%&A(!)A019!1#2%". The fail-safe Instahelp servers are located in the data centre of an European cloud provider in Germany (Frankfurt) and are subject to German data protection.
2. The assigned Instahelp psychologist now requests the new message from the Instahelp server and gets the encrypted message sent to his:her computer. Since the psychologist is in possession of the shared secret room key, he:she can decrypt and read the message.

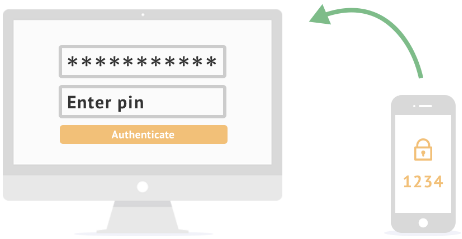
2. Secured data transmission

Although the messages are already encrypted, they are additionally transmitted to the Instahelp server via a secure data connection. The industry standard TLS 1.3 (Transport Layer Security) is used for this purpose to ensure the following security:

- A one-time key (256 bit) is generated for the connection to the Instahelp server, which is automatically exchanged digitally between the customer and the Instahelp server. The data to be sent is encrypted with this one-time key before being sent to the Instahelp server.
- For each message sent, a unique message authenticity code (=sequence) is also generated and deactivated after successful transmission.



3. Two-factor authentication (2FA)



With the third security measure, we ensure that the interlocutors involved in the communication actually represent the account holders. Two-factor authentication was implemented for this purpose. These two factors are representative of two properties that the person must know and possess. Knowledge refers to entering the self-defined password. Possession requires a smartphone with an authentication app or a device with biometric recognition using passkey technology. Thus, the Instahelp psychologist must know the password and identify him:herself via his:her biometric data (or the code of an authentication app) in order to log in successfully.

Frequently asked questions

Why are the messages stored on the Instahelp server?

With Instahelp, we pursue the goal of integrating psychological counselling into everyday life. The psychologist should be accessible at any time and from anywhere. Clients can log in to Instahelp on their smartphone, tablet or computer at any time in order to view the chat history as well as new answers from the psychologist and to respond to them immediately. For this purpose, the chat messages are stored on the Instahelp server in encrypted form so that they can be retrieved at any time.

How are the messages encrypted?

The widely used and recognised LibSodium cryptography library is used to encrypt the data. Each individual chat message is encrypted with a symmetric space key based on the XSalsa 20 method. In addition, each message is checked for tampering after transmission by authenticating the message via Poly 1305 MAC.

What happens if a hacker steals all the data from the Instahelp server?

If a hacker were to break through all the security mechanisms of our data centre, he:she would only find unreadable encrypted messages. Since each Instahelp client uses their own secret room key, the hacker would have to try to crack the key for each client.

How do I get a secret room key with the psychologist? Do I have to remember it?

No, Instahelp uses a sophisticated system to recover the uniquely generated secret room key. First, the password entered at login is converted into a long string (=digest) by the server (SALT) using a hash function (Salsa 20/8 + SHA-256) in combination with a character addition. The SALT is used to make a simple password more complex by adding a long random string. The advantage of the hash method is that the generated digest (=string) cannot be traced back to the original characters and thus the password of the user does not have to be stored at the Instahelp server. With this digest, the private and public key (Curve25519 (Key exchange) + XSalsa 20 (Encryption) + Poly 1305 MAC (Authentication)) of the user is generated. This key pair can now decrypt the encrypted room key requested by the Instahelp server.

Is there also content that is not encrypted end-to-end?

Yes, there is also content that is not encrypted end-to-end. To accompany and complement counselling, registered clients have access to the Mental Health Gym, where several functions (e.g. exercises, videos or audio files) can be used to strengthen mental health. The data is not passed on to third parties and is stored on our server in encrypted form. However, unlike when using our text chat, there is no end-to-end encryption. This enables us to carry out various exercises outside of a counselling room. This data can therefore also be accessed by you on another end device and is also available should you reset your password.