Privacy Café

How to use Signal - Private Messenger

Signal – Private Messenger is a free and open source software application for iPhone that employs end-to-end encryption, allowing users to send end-to-end encrypted group, text, picture, and video messages and have encrypted phone conversations between Signal users on iPhone and TextSecure or RedPhone users on Android. Although Signal uses telephone numbers as contacts, calls and messages actually use your data connection; therefore both parties to the conversation must have Internet access on their mobile devices. Due to this, Signal users don't incur SMS and MMS fees.

DOWNLOAD AND INSTALL SIGNAL – PRIVATE MESSENGER

On your iPhone, enter the App Store and search for "Signal." Select the app "Signal – Private Messenger" by Open Whisper Systems. Click to download the app and accept the iTunes Store Terms & Conditions by selecting "Accept." The app will download and install automatically. Click "Open" to launch the app.

REGISTER AND VERIFY YOUR PHONE NUMBER

Enter your mobile phone number and click "Verify This Device." In order to verify your phone number, you will be sent an SMS text with a six-digit code; enter the code in the space provided. If you are unable to receive SMS texts, you have the option of receiving a phone call to verify your phone number. Click "Submit Verification Code."

MAKING CALLS AND SENDING TEXT MESSAGES

In order to use Signal, the person that you are calling must have either Signal or TextSecure or RedPhone (for Android devices) installed. If you try to call or send a message to someone using the Signal app and they do not have any of the aforementioned apps installed, the app will ask if you would like to invite them via SMS, but it will not allow you to complete your call or send a message to them from inside the app.

To get started, click the "+" button. You'll see a list of your contacts that have already installed Signal, TextSecure, or RedPhone. You have the choice to either call them or send them a message.

To initiate an encrypted call to a contact, click on the phone icon next to the contact's name. Once a call is established, both parties to the call will be shown a random pair of words. This word pair will allow you to verify your identity and keys with the other user—also known as key verification.

The most trustworthy way to verify the identity of a caller is to use out-of-band verification to verify the word pair. You can also read the words aloud if you recognize the caller's voice. The word pair must be identical on both users' phones for you to be sure your message is not being intercepted.

In order to send an end-to-end encrypted text, picture, or video message, navigate to your contact list, click on the contact's name, and send your message. You can send an encrypted group message by navigating to your list of contacts, clicking on the group chat icon in the upper right-hand corner, and creating a new group.

access   EDRi   LIGA VOOR MENSENRECHTEN