How to use TextSecure on Android

TextSecure is a messaging app that allows users to send secure messages with their mobile phone using end-to-end encryption. The app works over a Wi-Fi or data connection (3G/LTE), but can also be used to send traditional SMS to non-TextSecure users, however, traditional SMS will not be encrypted in transit. Messages in blue are encrypted and sent over a data connection, while those in green have been sent over SMS. Both sides have to be using TextSecure (on Android) or Signal (on iPhone) for the messages to be secure while they travel over the Internet. In addition, you can set up a password to encrypt all conversations when they are stored on your phone. This means that they are better protected against being read if your phone is seized or compromised.

DOWNLOAD AND INSTALL TEXTSECURE

On your Android phone, enter the Google Play store and search for "TextSecure." Select the app, "TextSecure Private Messenger." Select "Install" and accept the Terms of Service by selecting "Accept." The app will download and install automatically.

CREATE A PASSWORD AND IMPORT EXISTING SMS

Open the app. You will be prompted to create a password in order to locally encrypt your data. This means that your data will not only be encrypted in transit but also locally on your phone. If you choose to skip this step, your messages will still be encrypted in transit, but will not be protected on your device. As always, choose a strong password.

You will then be asked if you would like to import your existing text messages into TextSecure's encrypted database. This is up to you: It allows you to send and receive also all your traditional SMS with TextSecure and replaces your built-in SMS app anymore. With TextSecure you have one app for both: secure messages and traditional SMS.

LET OTHERS KNOW YOU USE TEXTSECURE

The next screen will prompt you to "Connect with TextSecure" by registering your mobile phone number with TextSecure. This will allow other TextSecure users to know that you use TextSecure, too, and to send you secure messages. This is an optional step. Once you have registered your phone, TextSecure will automatically verify your number using a text message.

VERIFYING KEYS

TextSecure uses end-to-end encryption. When you first send a message to another TextSecure user, the app will automatically do the key exchange for you. In addition, however, you should verify keys with the other user to ensure that no one has tampered with the keys during key exchange (this is just like verifying someones PGP fingerprint).

To view the keys, click on the padlock icon in the top right of the screen and select "Verify Identity." You will be shown two sets of keys: one belonging to you and one belonging to the other user. TextSecure supports manual verification or verification by scanning the other user's barcode. If you are in the same room as the other person, you can easily scan the barcode on their phone (reachable by clicking on the lock icon on the menu bar at the top of your conversation, selecting "verify identity" and then clicking on the barcode icon) or read your keys aloud to one another. If you are not in the same room, you can read your keys aloud to one another on the phone if you recognize one another's voices or send them using another verified method of communication such as PGP or OTR.