

WhatsApp Implemented End-to-End Encryption by default for its 1 Billion Users

TechRounder PDF Edition

Live article:

<https://www.techrounder.com/whatsapp/whatsapp-implemented-end-end-encryption-default-1-billion-users/>

By Vipin PG | Published April 6, 2016 | Updated June 8, 2020 | Format: Article | 4 min read

In brief

This is the message most of the WhatsApp users seen when they send messages today. But no need to worry about this.

"Message you send to this chat and calls are now secured with end-to-end encryption. Tap for more info."

This is the message most of the WhatsApp users seen when they send messages today. But no need to worry about this. This is the new end-to-end encryption implemented for all its users for higher security. WhatsApp is updating its messaging app so that every text message and voice call will be encrypted. No need to worry about this, its just a notification saying that your message is more secure than the early one. This means, from now every message, image or voice call you made will be secured by end-to-end encryption so that only you and the person you're communicating with can read the content of the message, and nobody in between, not even WhatsApp. In other words, this also means that WhatsApp would not be able to comply with any court order that demands access to the content of any conversation happens over its service. Starting today, you will see a notification on your WhatsApp conversation screen as your messenger becomes end-to-end encrypted, as shown in the screenshot.

"This is because your messages are secured with a lock, and only the recipient and you have the special key needed to open and read them,"

Whatsapp says

.

Additionally, you will be able to see a small lock icon below the profile of the recipient that ensures your conversation is secured with encryption.

"All of this happens automatically: no need to turn on settings or set up special secret chats to secure your messages," the company adds.

How to verify if someone is trying to spy on your conversation?

Well, the latest version of WhatsApp mobile application offers you an option to verify the keys of the other users with whom you are communicating.. Whatsapp key verification can be done by scanning a QR code, or by comparing a 60-digit number, under newly introduced "verify security code" option in the WhatsApp.

"WhatsApp users can opt in to a preference which notifies them every time the security code for a contact changes."

Steps in Verifying

Please note, the following step is just to verify that end to end encryption is working fine, its not a mandatory thing to do the below step. Even if you are doing or not doing the step doesn't means that your encryption is on or off. The encryption is enabled to all users by default. No need to do enable or disable from user side.

1. If your private chat with any person, say James, shows the notification message saying "Message you send to this chat and calls are now secured with end-to-end encryption. Tap for more info." click on that message
2. It will open a popup showing verify. click on the verify button.
3. Next window will show you a QR code with some number as shown in the screenshot above. The window will have a Scan Now button at the bottom.
4. Click on the scan now button, it will open your camera to scan the QR code of your contacts phone ie here James's Phone, Do the same thing in James phone too to get the QR code, and scan the QR code using your phone from James phone, here the problem is that both phones should be near to each other.
5. In that case, we need to send the screenshot of QR code to James so that he can scan the QR code from distant place.
6. to do that, in the QR code page above click on the share Icon on the top (at the step 3) and send the QR code to James through any way, email, whatsapp, etc. The other person, say James will download the file and scan. when both person scan the QR code, the verification will complete.
7. Here also one limitation is there. to scan the QR code, you need to copy the file in another system like PC, TAB, or other phone, so that you can scan it using your phone.
8. Other than the above method you can verify simply by comparing the numbers show with other end user, each end user in your account will have separate number, that you can compare with the number shown in their phone too

Also please note that, if several users are sending texts in a group chat and one of the users is running an older version of WhatsApp that doesn't support encrypted messages, all the conversation going through that group chat will remain un-encrypted. So the new message and encryption will be available for only those with latest version of whatsapp.

References

1. whatsapp.com - security - <https://www.whatsapp.com/security/>