**Whatsapp Security and Encryption**

WhatsApp has introduced end-to-end encryption, and changes to its terms and conditions mean you're sharing your data with its parent company Facebook.

WhatsApp is an extremely popular mobile messaging service with over 1 billion daily users. That's an amazing figure, and the company prides itself in the apparent security it affords all of those users (provided they are running the latest version of the app).

Below is our guide on how to ensure your WhatsApp messages are fully end-to-end encrypted. However it's also good to be aware that not everyone trusts the company's word, in part because of privacy issues surrounding its parent company Facebook and also its implementation of encryption.

WhatsApp uses part of a security protocol developed by Open Whisper Systems, a company that has its own fully secure messaging app Signal (for iOS and Android). It's very good. It may not be as obsessed with multimedia sharing as WhatsApp but its basic functions are the same - and fully end-to-end encrypted.

**How does WhatsApp end-to-end encryption work?**

WhatsApp encrypting messages ‘end-to-end’ is a big deal because it means that the company itself has decided to run a system in which even it cannot intercept and read messages sent on its own platform.

When you send a message, it can only be ‘unlocked’ by the intended recipient, thanks to a very complex code that took WhatsApp several years to develop. It’s no mean feat to achieve, particularly given that 1 billion people use the service.

This differs to many messaging apps, which only encrypt messages between you and them. This means that your messages are stored on the services servers, usually not permanently, so hypothetically could be accessed and read.

**Why has WhatsApp introduced end-to-end encryption?**

Now that WhatsApp has end-to-end encryption, it means that they and no party – governments, police, hackers, other users – can intercept and read your messages.

WhatsApp has done this because as a company they believe in your right to have private conversations when you use their service. Also see: How to avoid WhatsApp scams

**Why is end-to-end encryption important?**

The reason the decision is getting a lot of attention is because of high profile cases in which communications service providers like Facebook are put upon by authorities to release sensitive personal data.

A high profile case is the FBI asking Apple to unlock an iPhone 5C that was used by one of the San Bernardino shooters, a move which Apple refused, underlining the integral values many large communications companies hold when it comes to personal data, security and encryption.