What is an encrypted messaging app? Are they really safe?

Encryption is a hot topic in the world of instant messaging apps. Some apps take a more serious approach to the security aspect - like Telegram and WhatsApp - while others still lack features in this respect.

Even Facebook's Messenger, which was once considered a less secure option, has implemented encryption, and the app's developers have shown greater attention to security.

All users benefit from using encrypted messaging. So you should have a clear understanding of the basic concepts and how all of this will impact you personally.

How encrypted messages work

Many people have become interested in coding. There are various factors cited as reasons for this growing interest, but it is important to understand how these apps work and what they bring to the users.

Traditionally, instant messaging applications work by passing messages between users through the use of a server as an intermediary. Meaning, when you send a message to one of your contacts, the message is actually sent to one of the company's servers, which is then forwarded to the intended recipient.

One obvious problem with this setup is that anyone with access to those servers has the ability to intercept communications and even modify them on the fly.

Also, the real intruder doesn't need to access the company's servers on their own. As long as hackers can 'insert' themselves at any point in the communication chain, they can get the same level of access.

This means that a compromised WiFi network can expose the contents of your messages and forward them to third parties, if you are using an unencrypted app.

Encrypted messaging apps solve this problem by encrypting user messages end-to-end. That means the application encrypts (i.e. scrambles) messages before sending them to the server, and the receiver decrypts them on their side locally. Not even the operators of the company can access any of your communications, as long as the encryption keys have not been changed.

Why are instant messaging apps so popular?

A decade ago, encryption wasn't much of a concern (at least for most users), but things are changing rapidly. Nowadays, people trust a third party less in keeping their data safe.

Serious cases like the Snowden leaks seem to reinforce that notion even further. Users prefer to use encrypted messages by default, because they understand that it is a higher level of security option than all other forms of communication, in case someone else is watching.

There are also concerns such as law enforcement seizing personal devices during investigations, airports requiring access to the device for international travel, and many other incidents that have made more and more Many people explore options in the encrypted messaging market.

And as expected, this market has also grown a lot. Many people have begun to expect encryption capabilities to be provided by default at this point, and things will likely continue to evolve in that direction.

Why should you care about encryption?

This leads to the question of whether you should care about encrypted messaging apps. In general, you can assume that as long as you don't send any inappropriate or illegal content, it doesn't matter whether or not you use encrypted messages.

But the truth is not so. Encrypted messaging means hackers can't intercept your communications and extract details like payment information or personal data that could be used to access your account.

Considering the fact that most of the popular messaging apps these days have encryption capabilities, it makes no sense to avoid them at this point. All the heavy lifting happens in the background and you don't have to do anything yourself, even during the initial setup.

There may be some hurdles to overcome if you want to take advantage of more advanced encryption features, but for most people's needs, it's not necessary.

Are encrypted messaging apps really secure?

Can these apps really keep your communications secure? It is not possible to give a definite yes or no answer. It is important to understand that encryption, like all other technologies, has its limitations and drawbacks.

For example, if encryption keys were ever compromised, an attacker could easily access your communications. It's important to remember that you have no real control over that actual encryption implementation.

This means that an app may be lying about encrypting your communications, and it is difficult to find out the truth. You could do some analysis on the net to figure out what kind of data is being transferred, but that might not tell you anything useful.

For example, if the app has a backdoor that provides access to the encryption key to developers, this will frustrate any efforts at keeping your communications secure.

In the end, if you don't care about encryption, that's usually fine. Just keep in mind that there can be some consequences to using outdated apps with security exploits that you might not immediately anticipate. On the other hand, putting too much trust in cryptographic platforms is also not necessarily a good thing, as it puts you at serious risk of letting your guard down in conversations.

It's best to stay neutral, taking advantage of what these apps have to offer, but don't over-trust anything you don't want to see public online.