What is end-to-end encryption? How does it work?

Online privacy is the need of the times. Especially when there is a continuous increase in the number of techniques to steal user data.

Aware of this need, the major online messaging services use a technique known as end-to-end encryption, to secure and protect users' chats.

But what does end-to-end encryption mean and how does it actually work? Let's find the answer through the following article!

What is end-to-end encryption?

You encrypt the message/image to be sent and it travels over the Internet as a 'secret' code. Only the receiver can then decrypt this 'secret' code. This process is called end-to-end encryption.

Picture 1 of What is end-to-end encryption? How does it work?

In the simplest terms, end-to-end encryption ensures confidential communication between the sender and receiver, preventing third parties from accessing this information. The tools and technologies that help with this process are designed into messaging apps and other software that users (may) use.

How does end-to-end encryption work?

The goal of end-to-end encryption is to prevent any intruder from stealing information between the sender and receiver. Back to the situation mentioned earlier: You are sending someone else a message.

When using an end-to-end encryption service, you are provided with a public and private key pair. These keys help you encrypt and decrypt. Along with that, the messaging app has an algorithm, consisting of mathematical functions used to encrypt or decrypt data.

When you're sending someone a message, you'll be provided with a public key that maps to that person's chat box. The public key is used to encrypt the message, using an algorithm found in the messaging app. This public key helps you recognize the recipient's device and the fact that he or she will receive the message.

Picture 2 of What is end-to-end encryption? How does it work?

Now, the recipient will use the private key, which helps to decrypt the message and interpret the information in the message sent by you. This private key is only available and exclusive to the recipient's device. Therefore, no one else can decrypt the message - at this point, the end-to-end encryption has succeeded.

This is the basic operating principle of end-to-end encryption. However, not all services use end-to-end encryption. Some tools often use transport layer encryption instead. So what is the difference between these 2 techniques.

What is the difference between end-to-end encryption and transport layer encryption?

As mentioned earlier, not all services are end-to-end encrypted. But, that doesn't mean they don't have any means of encryption. The most common form of encryption for websites is TLS - Transport Layer Security encryption.

The only difference between this type of encryption and end-to-end encryption is that in TLS the encryption takes place in the sender's device and is decrypted at the server. Therefore, it is not really end-to-end encrypted but provides a good level of security and is capable of protecting the user's information.

Picture 3 of What is end-to-end encryption? How does it work?

It is also known as encryption in transit. This means that the service provider can access all your messages through their servers. That's why you can easily see your old Instagram messages when you reload the app, but not on WhatsApp. You can only restore messages by downloading the backup file and decrypting it on your device.

Advantages and disadvantages of end-to-end encryption

Here are some advantages of end-to-end encryption.

1. Every step is fully protected.
2. Servers of messaging services cannot access messages and related information.
3. Information cannot be accessed by unauthorized persons online.
4. You cannot restore messages through a new login - unless there is an encrypted backup. Consider the Instagram and WhatsApp Messenger messenger example explained above.

Some disadvantages of end-to-end encryption include:

1. Metadata such as date, time, and participant names are not encrypted.
2. If the endpoints (sender or receiver) are vulnerable, end-to-end encryption doesn't do much.
3. In some cases, it can happen despite end-to-end encryption. Therefore, if someone chooses to physically impersonate the sender or receiver, the messages and information can be read by unauthorized people.

Above are all the pros and cons of end-to-end encryption. If you're still wondering whether to enable end-to-end encryption even if you're not sending secret messages, the answer is yes. Why allow others to access your data?

Here's everything you need to know about end-to-end encryption. Hope you found this article useful!

You finished reading the article "**What is end-to-end encryption? How does it work?**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com