A GUIDE TO COMMUNICATING WITH OTHERS: MESSAGING APPS

Messaging apps have become a key part of the way we communicate with each other in all aspects of our lives, from keeping in touch with our distant relatives to organising mass movements. Yet, there are so many out there, it is hard to know which ones are the most secure.

Take a look at our guide below to learn more:

What are the key factors you should consider when using a messaging app?

There are two main aspects to consider when deciding on the messaging app you want to use:

1. Whether it offers end to end encryption that protects the content of your communication; and

2. Whether it collects any information beyond the content of the message, such as location, who you communicate with and other details referred to as 'metadata'.

Why is encrypted messaging important?

Encryption is the process of scrambling information so that it cannot be read by anyone apart from the sender and the intended recipient(s). The use of cryptography in order to communicate secretly goes back to ancient Egypt and continues right up to present day.

End-to-End Encryption ("E2EE") describes the process of sending encrypted content from one recipient ("end") to another in such a way as its content cannot be read or modified by third parties while in transit. E2EE continuously protects the confidentiality and integrity of transmitted information by encrypting it at the origin and decrypting it at its destination. When E2EE is deployed, service providers cannot intercept the content or read the messages as they remain encrypted even as passing through the service providers' servers. In fact, anyone trying to intercept the message in transit before it reaches the receiver's device will not be able to read or modify its contents.

E2EE is made more sure through the use of digital signatures, in which messages are signed to prove who wrote them.

It's important to note that in almost all messaging apps, when messages are received your phone will decrypt them, save them & show them to you, decrypted, in the app. As a result, encrypted messaging doesn't necessarily protect you against someone getting access to your phone in order to read your messages.

Because of this, for sensitive conversations, it may be sensible to use disappearing/timed/vanishing messages if offered by your app as one method to stop the long-term storage of messages. It's also important to note, however, that any recipient in a conversation can take a screenshot or otherwise retain the message. Also, the app will display a notice that message deletion is taking place, and shows placeholders for manually deleted messages.

Please note that Mobile Phone Extraction (MPE) - which is used by some police forces and border guards - has been shown able to retrieve deleted messages from e.g. WhatsApp. It is unclear whether self-destructing messages are also recoverable by mobile phone extraction technology.

The use of E2EE for messaging should always be preferred over text messages/SMS. SMS messages are completely unencrypted meaning they can be easily read, manipulated in transit, or spoofed. They may also be stored by your telecommunications provider, which may be subject to access requests from governments and law enforcement.

Does your app encrypt both content and communications data?

Another consideration in choosing an app is the generation of metadata - this is data about what you're sending, to whom, and when rather than the contents of your messages.

Signal uses E2EE not only to encrypt the contents of messages, but also to obscure all metadata even from itself, storing only when an account was created & when it last connected to the service.

In contrast, both WhatsApp and Telegram store, and can access, far more metadata, including IP addresses, profile photos, "social graphs", and more.

In Telegram's case, Telegram does not use E2EE by default but instead stores all messages with keys that they have full control over. As a result, Telegram can provide access to messages at any moment. Both WhatsApp - through their Law Enforcement Online Requests System - and Telegram are known to have responded to police demands for information.

WhatsApp further collects information such as how you interact with others, as well as features you use such as groups or calling, but like Signal they don't retain encrypted messages on their servers once they have been delivered, and will delete undelivered messages after 30 days.

Your app requires your phone number to use it

To reduce the number of steps during sign up, most messaging apps rely on a phone number. While this is useful for more widespread pickup, this may be less than ideal for people not wanting to give out their personal number.

There are ways to avoid this, such as registering for the messaging app using the number of an alternative SIM card you possess.

App*	Offers E2EE	E2EE By Default	Requires phone number
iMessage	Yes	When not stored in the cloud	Yes
WhatsApp	Yes	Yes	Yes
Signal	Yes	Yes	Yes
Viber	Yes	Yes	Yes
Telegram	Kinda	No	Yes
Skype	Yes	No	No
Wickr	Yes	Yes	No
Matrix Client	Client Based	When offered by the client	No
Facebook Messanger	Yes	No	Increasingly
Google Messages	Yes	Yes	No
Instagram DMs	Yes	No	No
Twitter DMs	No	No	Increasingly
Discord	No	No	No

*This table was last updated in August 2022.