What is end-to-end (E2E) encryption and why should I use it?

Although most messaging apps encrypt messages sent to and from the service provider, unless end-to-end encryption is used, the service provider can still read those messages. E2E messaging apps keep your conversations private from everyone except you and the person you are talking to. They allow people to securely communicate sensitive information, protect against government surveillance, and provide an environment where people can speak freely with each other.

Which messaging apps provide E2E encryption?

Many messaging apps provide E2E encryption, including

- WhatsApp
- Signal
- Facebook Messenger Secret Conversations
- iMessage

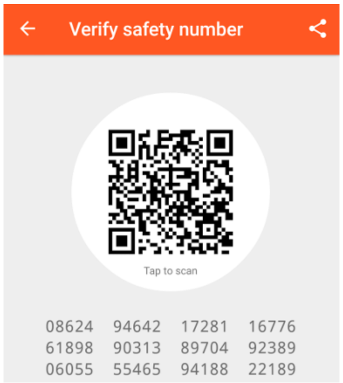
The Electronic Frontier Foundation provides tutorials on how to use Signal and WhatsApp to keep your messages secure: https://ssd.eff.org/

Is E2E encryption the default?

Not all apps E2E encrypt messages by default. If you choose to use an app that does not E2E encrypt by default, it is important to be aware of this before sending messages you would like to keep private. Alternatively, you can use an app that E2E encrypts all messages by default, e.g. WhatsApp.

What is key verification?

While E2E encryption ensures that messages sent between you and another person remain private between you and that person, it's still important that the person you are communicating with in the app is who they say they are. Apps such as WhatsApp and Signal allow users to verify this by either scanning a QR code shown on the other person's device or by comparing safety numbers (sometimes called security codes or fingerprints). Here is an example of Signal's key verification screen, found in the conversation settings menu:



```
08624   94642   17281   16776
61898   90313   89704   92389
06055   55465   94188   22189
```

Performing key verification by scanning QR codes is preferable to manually comparing safety numbers as it is less error prone. If you choose to manually compare numbers, it is important that all numbers match exactly; otherwise, an eavesdropper may attempt to avoid detection by using a key whose corresponding safety numbers are similar but not exactly the same (e.g. only matching in the beginning and ending numbers). For more information, see: https://ssd.eff.org/en/module/key-verification.