Encryption in Social

Encryption is primarily used to safeguard the contents of a message so that only the intended recipient can read it. This is done by replacing the content of the message with unreadable data, which can only be understood by the intended recipient. Encryption is a widely used method to protect data from anyone who might want to steal it.

Encryption can be used in two situations:

- Encryption in Transit
- Encryption at Rest (EAR)

Encryption in Transit

Encryption in Transit refers to data that is encrypted when it is in transit, including from your browser to the web server and other third parties via integrations. Encrypting data in transit protects your data from man-in-the-middle-attacks.

Learn more about Encryption in Transit.

Encryption at Rest

Encryption at Rest refers to data that is encrypted when it is stored (not moving), which could be on a disc, in a database, or some other form of storage. When used alongside encrypting data during transit, encrypting data when it is stored on the servers provides an even higher level of security. EAR protects against any possible data leak due to server compromise or unauthorized access.

Encryption is performed at the application layer using the AES-256 algorithm, which is a symmetric encryption algorithm and uses 128-bit blocks and 256-bit keys. The key used to convert the data from plain text to cipher text is called the Data Encryption Key (DEK). The DEK is then further encrypted using the KEK (Key Encryption Key), providing yet another layer of security. The keys are generated and maintained by our in-house Key Management Service (KMS).

Learn more about our KMS.

What data do we encrypt in Social?

We encrypt all sensitive data such as AuthTokens and all fields that contain personal information at the application level.

Full-disk encryption

In addition to our standard application layer encryption, full disk encryption is available in the India (IN), Australia (AU) and Japan (JP) data centers.

Learn more about full-disk encryption.
Learn more about encryption and our KMS.