

Chiffrement de bout en bout

Aussi appelé `end-to-end encryption` ou `E2E`, il s'agit d'un système de communication où **seules les personnes qui communiquent peuvent lire le contenu échangé.**

Aucun autre acteur ne peut lire le message : ton FAI ou le serveur qui transporte le message ne voient qu'un contenu chiffré.

C'est une garantie bien plus forte que l'`HTTPS` qui crée un tunnel chiffré entre ton appareil et le serveur, donc le serveur sait parfaitement à quelles données tu accèdes contrairement à ton FAI.

— Services qui implémentent l'E2E

Messageries instantanées

✓ Chiffrement de bout en bout

- Signal (et ses forks, comme Molly) : [Configurer Signal](#)
- WhatsApp
- GPG pour les mails (ProtonMail entre 2 comptes Proton) ; ⚠ de nombreuses métadonnées restent en clair

⚠ Les données sont visibles en clair par le serveur

- Instagram (suppression pour les DMs depuis le 2026-05-08¹)
- Messenger
- TickTock
- ...

Services en ligne

✓ Chiffrement de bout en bout

- Cryptpad, cryptdrive



Les données sont visibles en clair par le serveur

- Google Drive
- Frama-quelquechose
- Jitsi
- ...

Les dangers du chiffrement de bout en bout, en anglais (2025-04-01)

2026-10-252026-10-25

Page citée par

-  Anonymat de la connexion et des échanges
-  Configurer Signal — Installer, sécuriser et relier Signal sur téléphone et ordinateur
-  Contenus d'un service en ligne — Les messages et documents stockés chez un service
-  Faire une visio — Se réunir en visio sans dévoiler d'informations personnelles
-  N'importe qui sur Internet — Escrocs, harceleurs, pirates : aucun cadre et aucune autorisation

1. <https://cybersecuritynews.com/instagram-end-to-end-encryption/> 