

PRIVACIDAD 101: MENSAJERÍA MÁS SEGURA

¿QUÉ TAN SEGURA ES MI APP DE MENSAJES?

Usamos aplicaciones de mensajes para todo tipo de cosas. Pero, ¿qué tan seguras son realmente? Aquí tienes un breve resumen:

 **SIGNAL**
Propietario: Signal Messenger

La mejor y más segura app para mensajes y llamadas. No solo los mensajes y llamadas en Signal están cifrados de extremo a extremo (E2EE), sino que también protege tu metadata (la información sobre con quién te comunicas).

 **MENSAJERÍA EN IOS**
Propietario: Apple Inc

Los mensajes entre iPhone (iMessage) están cifrados de extremo a extremo, pero las copias de seguridad en iCloud pueden incluir mensajes almacenados (usa una contraseña para iCloud para cifrarlos).

 **MENSAJERÍA EN ANDROID**
Propietario: Open Handset / Google

Google Messages tiene E2EE para mensajes entre dispositivos Android, pero Google puede ver con quién te comunicas y cuándo.

   **WHATSAPP / MENSAJERÍA DE META**
Propietario: Meta Platforms

Usa cifrado de extremo a extremo, pero Meta puede ver con quién te comunicas y cuándo.

¿QUÉ ES CIFRADO DE EXTREMO A EXTREMO (E2EE)?

El dispositivo del remitente cifra los mensajes y solo pueden ser descifrados por el dispositivo del destinatario.

TIPS DE SEGURIDAD

- Usa una contraseña en tu teléfono
- No envíes mensajes en situaciones de alto riesgo
- Activa los mensajes que desaparecen (Disponible en Signal y WhatsApp)

LO MÁS IMPORTANTE

Muchos problemas con la mensajería segura provienen de errores humanos. Asegúrate que contactos sean confiables, usa contraseñas, evitar capturas de pantalla y ten cuidado con quién agregas al chat.

 libraryfreedom.org  info@libraryfreedom.org

 Mellon Foundation

PRIVACIDAD 101: MENSAJERÍA MÁS SEGURA

¿QUÉ TAN SEGURA ES MI APP DE MENSAJES?

Usamos aplicaciones de mensajes para todo tipo de cosas. Pero, ¿qué tan seguras son realmente? Aquí tienes un breve resumen:

 **SIGNAL**
Propietario: Signal Messenger

La mejor y más segura app para mensajes y llamadas. No solo los mensajes y llamadas en Signal están cifrados de extremo a extremo (E2EE), sino que también protege tu metadata (la información sobre con quién te comunicas).

 **MENSAJERÍA EN IOS**
Propietario: Apple Inc

Los mensajes entre iPhone (iMessage) están cifrados de extremo a extremo, pero las copias de seguridad en iCloud pueden incluir mensajes almacenados (usa una contraseña para iCloud para cifrarlos).

 **MENSAJERÍA EN ANDROID**
Propietario: Open Handset / Google

Google Messages tiene E2EE para mensajes entre dispositivos Android, pero Google puede ver con quién te comunicas y cuándo.

   **WHATSAPP / MENSAJERÍA DE META**
Propietario: Meta Platforms

Usa cifrado de extremo a extremo, pero Meta puede ver con quién te comunicas y cuándo.

¿QUÉ ES CIFRADO DE EXTREMO A EXTREMO (E2EE)?

El dispositivo del remitente cifra los mensajes y solo pueden ser descifrados por el dispositivo del destinatario.

TIPS DE SEGURIDAD

- Usa una contraseña en tu teléfono
- No envíes mensajes en situaciones de alto riesgo
- Activa los mensajes que desaparecen (Disponible en Signal y WhatsApp)

LO MÁS IMPORTANTE

Muchos problemas con la mensajería segura provienen de errores humanos. Asegúrate que contactos sean confiables, usa contraseñas, evitar capturas de pantalla y ten cuidado con quién agregas al chat.

 libraryfreedom.org  info@libraryfreedom.org

 Mellon Foundation