colectivo disonancia

APLICACIONES Y PRECAUCIONES BÁSICAS PARA AUTODEFENSA DIGITAL EN LA PROTESTA

MENSAJERÍA

SIGNAL

Para una mensajería segura y fácil de usar, es recomendable Signal. Posee cifrado completo, de extremo a extremo, y posibilidad de autodestruir todos sus mensajes.

Existen otras opciones aún mejor, como Matrix o XMPP, pero requieren de algunos conocimientos para su adecuada configuración.

FOTOS EN CELULAR

Scrambled Exif

Antes de compartir una fotografía, es necesario borrar sus metadatos (GPS, modelo de celular, etc) para que no sea identificado quién la comparte.

Para usarla, una vez instalada, hay que compartir la foto a esta aplicación, que limpiará los metadatos y luego permitirá volver a compartirla.

FOTOS EN CELULAR

ObscuraCam

Para no revelar la identidad de los manifestantes, es necesario pixelar rostros o vestimentas, para eso sirve ObscuraCam.

Puede tomar fotografías y editarlas o editar fotos o imágenes que ya has sacado y tienes en tu memoria. Proteger la identidad de los manifestantes es proteger la protesta social.

VPN

R I S E U P VPN

Una VPN es una conexión de internet que permite mantener segura y privada tu comunicación al navegar por internet desde un servidor distante, en este caso del colectivo Riseup.

Para usar la app solo hay que descargarla y activarla, haciendo que toda tu conexión a internet esté cifrada y anónima para las empresas de telecomunicaciones.

SIN INTERNET

BRIAR

En el caso de que el internet sea cortado, Briar es una opción de mensajería necesaria. No depende de ningún servidor (P2P).

Puede utilizarse con Bluetooth o con Routers encendidos sin internet, permitiendo comunicarse en zonas cercanas, entre vecinos o grupos cercanos.

SIN INTERNET

SILENCE

Al usar SMS, deben estar cifrados, ya que de lo contrario pueden ser leídos por las empresas de telecomunicaciones. Silence soluciona ese problema.

Cuando 2 o más usuarios usan Silence para usar SMS, tienen la opción de cifrar sus mensajes y proteger su comunicación. SIGNAL también ofrece esta opción

PRECAUCIONES

- Bloquea tu celular con contraseña y cuida que las cámaras no vean tu clave.
- Todas las cámaras pueden potecialmente analizar los rostros con reconocimiento facial. Cubre tu rostro si es necesario.
- Ten en cuenta que mientras estés con un celular, tu ubicación es rastreable por las antenas de telefonía, información que las empresas guardan.

colectivo disonancia