Comunicación, seguridad y privacidad: correo electrónico y mensajería instantánea

Práctica 4

En la práctica anterior trabajasteis con software libre para tareas cotidianas de ofimática y navegación. Un siguiente paso sería hablar de comunicaciones en lo que respecta a aplicaciones de escritorio (propias de escritorio o web a través del navegador) y aplicaciones móviles.

En esta práctica te proponemos que tomes consciencia de la cuestión de la libertad y privacidad en el uso de comunicaciones que usas a diario, fundamentalmente el correo electrónico y la mensajería instantánea de móviles (WhatsApp, Telegram...).

Comienza leyendo los siguientes textos:

1. Artículo "Mensajería instantánea libre y responsable", por Óscar Martín, de Ingeniería sin Fronteras Andalucía.
2. Acerca de riseup.net y Political Principles
3. ¿Qué hace especial al correo de riseup.net?

Una vez leído, puedes realizar las siguientes actividades:

1. Instala en tu móvil las aplicaciones de mensajería instantánea sugeridas en el artículo 1. Reflexiona sobre puntos fuertes y débiles de cada una, y en qué se puede basar la popularidad de cada una.
2. Responde a la pregunta ¿es Telegram totalmente libre?
3. Investiga sobre el protocolo OTR (*Off the record messaging*), ¿podrías utilizar este cifrado en alguna de las redes de mensajería instantánea que usas?
4. Investiga sobre GNU Privacy Guard (GnuPG o GPG). Estudia cómo podrías usarlo en tu correo electrónico (existen implementaciones a nivel de navegador y a nivel de cliente de correo).

Otros textos de interés:

- Defensa personal del correo electrónico, infografía de la FSF (Free Software Foundation)
- Defensa personal del correo electrónico, guía de la FSF (Free Software Foundation)
- Tor and HTTPS, de la EFF (Electronic Frontier Foundation)
- NSA Spying on Americans, de la EFF