GUIA RÁPIDA PARA PROTEGERSE EN LA RED

Aportaciones:

- "El pequeño libro rojo del pequeño activista en la red" de Marta Peirano (@minipetite)
- Víctor
- Xavi Domínguez (@xavidominguez)
- Xose Pérez (@xoseperez)

Información:

- Artículo de Marta Peirano: La Red no es neutral

General:

1. Utiliza un sistema operativo abierto (Linux, FreeBSD,...). Si quieres estar protegido y anónimo en un % muy alto te recomiendo que instales Tails https://tails.boum.org/ en una memoria USB.
2. Nunca compartas datos personales en una web de terceros, nada que te pueda identificar (DNI, dirección, lugares donde acostumbres a estar, imágenes donde se vean documentos personales,...)

Protege tu casa y espacios personales:
App desarrollada por Edward Snowden q puedes descargar desde aquí https://play.google.com/store/apps/details?id=org.havenapp.main . De momento sólo para Android. Más info aquí: http://m.eldiario.es/cultura/tecnologia/Edward-Snowden-Haven-app_0_722677980.html#click=https://t.co/MbEmfVRu7z

Navegar:

1. Navega siempre en modo incógnito. Chrome y Firefox lo permiten.
    a. Firefox: https://support.mozilla.org/es/kb/navegacion-privada-con-proteccion-contra-el-rastreo
2. Tapa tu webcam.
3. Utiliza TOR (https://www.torproject.org/) para navegar de manera anónima (nivel avanzado, puedes tener un proxy Tor en tu casa en una Raspberry Pi)

Ficheros:

- Encriptar tus ficheros en la nube:
    - https://cryptomator.org/

Buscador:

- https://duckduckgo.com/ (no track)

Contraseñas:

1. Aprende a hacer contraseñas seguras.

 **Attribution-NonCommercial 4.0 International (CC BY-NC 4.0)**

    - http://passwordsgenerator.net/
2. Aprende a memorizar contraseñas seguras.
3. Usa contraseñas distintas para cada cosa.
4. Cambia de contraseñas con frecuencia
5. No comportas tus contraseñas.
6. Opcionalmente (útil si tienes muchas contraseñas) utiliza un gestor de contraseñas (keypass, enpass...) Existen soluciones de llaves maestras basadas en hardware que aportan un nivel más de seguridad (mooltipass, signet,...)

Aplicaciones (correo, twitter, facebook…) :

- Activa siempre que puedas la verificación en 2 pasos.
- No utilices el mismo password para todos tus aplicaciones / servicios
- Desactiva las tareas automáticas de tu ordenador o móvil que impliquen romper alguna de las sugerencias anteriores (sincronización automática de fotos, por ejemplo)

Correos electrónicos:

1. OPC 1: Cuenta segura con información encriptada en servidor: **protonmail.com**
2. Activa la verificación en 2 pasos.
3. Instala en algun dispositivo aplicación de validación en 2 pasos tipo: Auth .
4. OPC 2: Instala un cliente de correo que utilize SSL/TSL junto con un protocolo de criptografía de clave pública.
    a. https://www.mozilla.org/es-ES/thunderbird/
5. Cifra el mensaje con PGP.
6. Envía correo a través de protocolos de transferencia segura cómo SSL o TSL.

- Si quieres enviar un correo anónimo....
    1) Envíalo desde un espacio público y no habitual para ti.
    2) Crea una cuenta de correo temporal (desaparecen a las pocas horas):
        a) https://www.guerrillamail.com
        b) http://www.mintemail.com/
        c) http://www.filzmail.com/
    3) Elimina cookies, historial… antes de irte.

Más seguro si lo envías desde tu propio SO en USB (no lo olvides !)

Pretty Good Privacy o **PGP** (*privacidad bastante buena*) :

- Criptografía de clave pública (cada usuario tiene una clave privada y otra pública)

1. Genera tu clave pública y privada.
2. Haz una copia en USB que llevarás contigo siempre y otra copia como medida de seguridad por si pierdes USB.
3. Instalar Thunderbird.
4. Instalar GPG. (Si instalas Enigmail pasa de este punto)

Attribution-NonCommercial 4.0 International (CC BY-NC 4.0)

5. Instalar extension de Thunderbird (Enigmail)
    - Enigmail te permite generar claves pública y privadas para encriptar y proteger tus correos.

Ayuda ?: https://ssd.eff.org/es/module/como-usar-pgp-para-linux

Data Detox Guide! https://datadetox.myshadow.org/detox

Attribution-NonCommercial 4.0 International (CC BY-NC 4.0)