8 OCHO TIPS

Para protegerse del perfilamiento con inteligencia de fuentes abiertas OSINT

Desde Karisma queremos compartir unas recomendaciones para que quienes utilizan internet puedan proteger sus derechos frente al posible uso inadecuado de las tecnologías OSINT que posee el Estado. En especial, para aquellas personas cuyo trabajo de investigación, periodismo o de activismo pueda ponerlas en una posición de riesgo respecto al abuso de la vigilancia por parte de las fuerzas de seguridad.

1 Evalúe la sensibilidad de sus publicaciones en redes sociales.

La información compartida y los datos asociados a esta como ubicación, tipo de dispositivo, nombre de usuario, fecha y hora de publicación, entre otros, pueden ser recogidos para su uso por el Estado, empresas privadas e, incluso, organizaciones criminales. ¡No olvide que con herramientas OSINT se puede cruzar información de distintas redes sociales y bases de datos!

2 Resguarde su privacidad cuando navega en internet.

Use Tor[1] o una VPN (red privada virtual), como Riseup VPN[2] o Psiphon[3]. Esto minimizará la información de localización e identidad registrada por los proveedores de internet y que puede ser usada por sistemas OSINT.

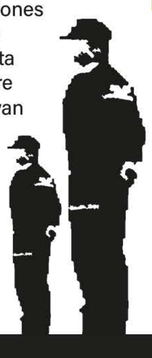
1. https://www.torproject.org/es/download/
2. https://riseup.net/es/vpn
3. https://psiphon.ca/es/download.html

3 Cuide su anonimato.

El anonimato en internet está especialmente protegido cuando se utiliza con fines relacionados a los derechos a la libertad de expresión, la participación, reunión y la protesta. Utilice perfiles anónimos no relacionados con usted (deben estar desconectados de su correo personal, cuentas con su nombre o número de celular) si considera que su publicación puede generar un riesgo a su integridad o la de sus conocidos. Cuando utilice un perfil anónimo es recomendable usarlo solamente a través de una VPN o Tor.

4 Proteja la información de los lugares que frecuenta.

Tenga en cuenta que señalar su ubicación, así como la publicación de imágenes y videos con direcciones o en lugares identificables (sitios históricos o estaciones de transporte público, por ejemplo) facilita que se conozca su localización o los lugares que frecuenta mediante OSINT. Además considere publicar sobre actividades en las que participó cuando estas hayan concluido y sólo si no frecuenta el lugar donde suceden, para no ayudar a otros a determinar su ubicación o hábitos.



5 No hable con extraños.

Los software de OSINT suelen usar cuentas falsas para infiltrar grupos en redes sociales o para acceder a información cuando se encuentra restringida en perfiles privados. Antes de agregar un perfil desconocido o de incluirlo en un grupo, verifique si es confiable e intente cerciorarse de la autenticidad del perfil. Si no es posible establecer que el perfil pertenece a alguien que conoce, lo mejor es no aceptarlo.

6 Comuníquese de forma cifrada.

El cifrado es un método de protección de la información que la transforma volviéndola ilegible sin el programa y la llave utilizada en el proceso. Instale aplicaciones de mensajería cifrada e invite a otras personas a hacerlo (WhatsApp o Signal[4]). Además, si desea llamar o enviar un mensaje de texto, estas aplicaciones son la mejor opción para hacerlo de forma privada, no utilice la red celular ni mensajes de texto (SMS). Evite usar chats abiertos (grupos masivos en WhatsApp o Telegram), pues estos pueden ser infiltrados y vigilados por las herramientas OSINT.

4. https://signal.org/es/

7 Proteja la imagen e identidad de otros.

Cuando capture y publique imágenes o videos evite que otras personas a su alrededor puedan ser identificadas. Aplicaciones como ObscuraCam[5] o Signal permiten anonimizar a terceros difuminando rasgos distintivos.

5. https://guardianproject.info/es/apps/org.witness.sscphase1/

8 Modifique o elimine los metadatos de las fotos antes de publicarlas.

Los metadatos son información adicional (la ubicación, fecha y hora de creación, tipo de cámara, propietario, etc). Puede hacer una captura de pantalla y compartirla en lugar de la imagen original. También puede enviarla primero por WhatsApp (esto elimina los metadatos) y luego sí publicarla. Para gestionar los metadatos de sus fotografías también puede usar herramientas como Scrambled EXIF y Exif Cleaner[6].

6. https://exifcleaner.com/

El Ejército y la Policía Nacional de Colombia tienen en su poder potentes herramientas OSINT (Open Source INTelligence o Inteligencia de Fuentes Abiertas) con la capacidad de vigilar de forma masiva internet y perfilar personas. Hablamos de software que permite encontrar, descargar y procesar grandes cantidades de información en fuentes abiertas de internet como foros, blogs, redes sociales, medios de comunicación o chat abiertos. No existe información pública respecto a cómo se están usando estas tecnologías, con qué garantía y controles, por orden de quién y a quiénes afecta.

En Colombia hay varios antecedentes inquietantes que involucran vigilancia individualizada a personas percibidas como opositoras políticas, activistas de derechos humanos, periodistas e incluso funcionarios y funcionarias públicas. Los casos de las chuzadas del DAS o las Carpetas Secretas del Ejército Nacional son algunos ejemplos de abuso de sistemas de vigilancia.

Si le interesa conocer más herramientas y prácticas para proteger su seguridad digital le recomendamos revisar los cursos cortos de Entrenamiento de seguridad digital para activistas y periodistas del proyecto Totem y las Guías de configuración y uso seguro de herramientas de la Fundación Conexo

https://conexo.org/project/guias-de-herramientas/
https://totem-project.org/es/

Encuentre nuestro informe Cuando el Estado vigila, Ciberpatrullaje y OSINT en Colombia en:

https://bit.ly/InformeCiberpatrullaj

20 años Fundación Karisma