Guía antirrepresiva para la acción: Seguridad informática

MOVIMIENTO ANTIRREPRESIVO DE MADRID :: 09/06/2020

Artículo extraído de la revista "Amnistía" número 3 del Movimiento Antirrepresivo de Madrid.

El desarrollo en tecnologías de la comunicación y el acceso general a internet ha abierto nuevas formas de expresión, difusión y organización. Gracias a ello, las comunicaciones y la información pueden ser consultadas de manera prácticamente instantánea, pudiendo incluso transmitirse en tiempo real.

Sin embargo, el uso indiscriminado de la tecnología la convierte en un arma de doble filo, dotando a agentes externos de información sensible que pone en riesgo tanto a la propia persona como a los de su alrededor.

Por ello, en este capítulo de la guía antirrepresiva hablaremos de cómo utilizar la tecnología de tal forma que minimice los riesgos a los que podemos exponernos como activistas.

El teléfono móvil se ha convertido, para muchas personas, en una herramienta imprescindible, tanto es así que ha superado incluso a los ordenadores como dispositivo para acceder a internet.

Además, en el móvil almacenamos todo tipo de información, indistintamente de que esta información sea intrascendente o no, siempre es útil para realizar perfiles de quiénes somos, con quién nos relacionamos o las actividades que realizamos. Por lo que asegurar nuestros datos es de vital importancia. Para ello, se puede realizar un cifrado de la memoria interna tanto de móviles como de tablets. Este proceso hace ilegible cualquier tipo de información (mensajes de texto, imágenes, etc.) si no se conoce la contraseña. En Android, en el primer encendido durante el proceso de configuración inicial, te preguntará si quieres realizar el cifrado de la memoria interna. Esto puedes hacerlo también en cualquier momento en el apartado de seguridad en la pestaña de “opciones”. En los dispositivos con iOS, el contenido está cifrado por defecto, solo hay que asegurarse de que el bloqueo es por contraseña.

En lo que se refiere a nuestras comunicaciones, recomendamos usar aplicaciones de mensajería instantánea de licencia libre, como es Signal. Que una aplicación sea de licencia libre significa que el comportamiento interno de la aplicación es accesible para poder estudiarlo, e incluso contribuir a su desarrollo, lo que permite verificar si nuestras conversaciones están siendo leídas, o no, por terceros o si están siendo almacenadas en algún servidor. En principio, Signal no almacena nuestras conversaciones en ningún servidor, lo cual significa que desaparecen al ser borradas de nuestros respectivos dispositivos. Al no almacenar las conversaciones, Signal no puede acceder a los mensajes ni ceder estas conversaciones a ninguna otra compañía ni Gobierno que las reclame.

En ocasiones son las mismas aplicaciones, como ocurre con Gmail o con las aplicaciones de banca electrónica, las que nos ofrecen determinadas medidas de seguridad que consisten en

la verificación de nuestra identidad por distintos métodos. Estos métodos de autenticación de la identidad pueden ser de lo más inofensivos, como por ejemplo introducir un pin o clave que te ha llegado por SMS al teléfono móvil. Otros métodos, aunque pueden parecer más cómodos para el uso diario, pueden volverse en nuestra contra, en tanto que pueden suministrar datos sensibles sobre nosotros. Entre estos métodos destacamos el reconocimiento facial y la huella dactilar.

Los métodos biométricos presentan dos inconvenientes principalmente. El primero es que una vez introducida tu huella o imagen, éstas no pueden ser cambiadas y quedan vinculadas a tu identidad de forma permanente, lo que conlleva a una fácil identificación de qué personas acuden a manifestaciones o eventos y cayendo en el riesgo de poder convertirte en un objetivo. Y el segundo es que estos métodos son especialmente vulnerables en un contexto de conflicto cómo puede ser una manifestación, en el cual pueden sustraerte el móvil y forzarte a desbloquearlo. Es por todo esto que recomendamos desactivar los métodos de autenticación biométricos de los dispositivos y aplicaciones y usar contraseñas seguras en su lugar.

Por último, es importante mencionar que, aunque estos métodos dificultan el acceso a nuestra información por agentes externos, cualquier dispositivo informático, esté encendido o no, es susceptible de ser rastreado e incluso utilizado como micrófono y geolocalizador mediante distintos mecanismos que son accesibles por equipos especializados del Estado y que no pueden ser previstos ni mitigados y que la única opción de defenderse ante ello es concienciar de la importancia de utilizar los dispositivos electrónicos cuando sean verdaderamente necesarios como, por ejemplo, el trabajo de agitación en redes, y empezar a prescindir totalmente de ellos cuando tratemos temas cuya información pueda ponernos a nosotros o nuestros colectivos en riesgo.

Debemos tomar conciencia de la importancia de qué tipo de uso damos a nuestros dispositivos y cuándo estos nos están ayudando y cuándo nos perjudican individual y colectivamente. Podemos sintetizar todo esto en las siguientes medidas de seguridad:

- Evitar llevar cualquier dispositivo informático en las reuniones.
- Utiliza un ordenador que no haya sido conectado nunca a internet para el trabajo de militancia.
- No activar el reconocimiento facial ni dactilar en ningún dispositivo.
- Al asistir a manifestaciones, deja el móvil en casa.

---

https://www.lahaine.org/est_espanol.php/guia-antirrepresiva-para-la-accion