

Ciudad de México, a 22 de julio de 2017
INAI/229/17

ADVIERTE INAI RIESGOS DE SINCRONIZAR APP'S CON REDES SOCIALES Y LA FORMA DE PREVENIRLOS

- **El intercambio de información puede llegar a países donde no existen leyes que protejan los datos personales**

Con el propósito de proteger a los usuarios de internet, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) advierte sobre los riesgos que implica sincronizar las aplicaciones (app's) con las redes sociales.

La sincronización consiste en la vinculación de información personal de las cuentas de redes sociales para que la aplicación suministre algún servicio como juegos, música, citas, edición de imágenes, servicios de transporte privado, entre otros.

Al consentir este vínculo los usuarios podrían permitir el acceso a datos personales contenidos en el perfil de la cuenta, entre ellos: domicilio, intereses, hábitos, fecha de nacimiento, centro de trabajo, academia de estudios, sitios visitados, opiniones personales, fotografías, videograbaciones y comunicaciones privadas.

Además, las funciones de algunas app's posibilitan obtener información adicional de los usuarios, como el acceso a las cuentas asociadas a los dispositivos, a la agenda del móvil, los contactos registrados en el directorio y la ubicación en tiempo real del individuo a través de la red o el sistema GPS, entre otros.

De manera que el vínculo que se genera al sincronizar las app's con redes sociales podría resultar riesgoso para la protección de datos personales, ya que el intercambio de información puede llegar a países donde no existen leyes que vigilen este derecho humano.

Los datos personales podrían utilizarse con finalidades de prospección comercial, por ejemplo, mediante la identificación de pautas de comportamiento de los usuarios con el fin de personalizar la publicidad dirigida a los consumidores.

Por ello, la Secretaría de Protección de Datos Personales del INAI hace las siguientes sugerencias a quienes deseen sincronizar alguna aplicación con sus redes sociales:

- Estar consciente que al menos una parte de sus datos provenientes de una red social serán compartidos con la app.

- Conocer la política y/o aviso de privacidad, tanto de las aplicaciones como de las redes sociales, para saber si es acorde con sus necesidades. Es necesario verificar si la configuración del perfil de privacidad permite un control adecuado y suficiente de los datos personales.
- Corroborar la existencia de cláusulas que aludan a la posibilidad de que los proveedores de la aplicación se atribuyan “la propiedad” de sus datos personales por el uso de la aplicación, y con ello se pueda estar privando de la posibilidad de disponer libremente de esos datos en el futuro.
- Saber si sus datos serán protegidos confidencialmente.
- Descargar las aplicaciones sólo en tiendas autorizadas como App Store o Google Store.
- Examinar los comentarios formulados respecto de las apps en las tiendas de venta para conocer la calificación de la misma y tener con ello algún parámetro fácil de consulta sobre su funcionalidad y confiabilidad.
- Revisar en la red social (Facebook, Google+, Twitter) las opciones para gestionar los permisos con la red social.
- Estar consciente de que los usuarios no se encuentran obligados a sincronizar sus apps con redes sociales, pero la decisión final radicará en la voluntad de cada individuo y atenderá a los intereses particulares de éstos.
- Por lo tanto, se sugiere no realizar alguna sincronización si ésta no resulta realmente indispensable.
- Antes de borrar una app de un dispositivo móvil, asegurarse de haberla desvinculado de la red social.

En caso de que algún particular detecte el mal uso de sus datos personales, el INAI recomienda llamar al Centro de Atención a la Sociedad (CAS) al 01800 8354324 o acudir a las oficinas ubicadas en la Avenida Insurgentes Sur 3211, colonia Insurgentes Cuicuilco, delegación Coyoacán.

-o0o-