México D.F., a 18 de julio de 2017
INAI/223/17

INAI EMITE RECOMENDACIONES PARA EVITAR SER VÍCTIMA DE *SPYWARE* O *SOFTWARE ESPÍA*

- **El Instituto destacó que, entre las implicaciones de ser afectado por *softwares espía,* es posible que terceros no autorizados puedan obtener contraseñas del usuario; conocer la ubicación geográfica de la persona en tiempo real; y acceder a las comunicaciones del titular del dispositivo, tales como mensajes de texto, llamadas y correo electrónico, entre otras**

El *spyware* es un software malicioso, también conocido como *software espía*, el cual, sin consentimiento ni conocimiento del usuario, se instala en un dispositivo móvil o equipo de cómputo y tiene como finalidad la obtención de información personal para efectuar actividades fraudulentas o con fines publicitarios, advirtió el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

El Instituto indicó que existen diversos softwares que permiten a los usuarios realizar un sinfín de actividades en sus dispositivos y equipos; sin embargo, hay quienes buscan beneficiarse de los avances tecnológicos, mediante la creación de programas maliciosos, denominados generalmente malware, de entre los cuales, es posible encontrar al *spyware*.

Señaló que el *spyware* es difícil de detectar, incluso una vez instalado, la mayoría de los usuarios ni siquiera se imagina que su equipo ha sido infestado por este software malicioso ya que su actividad se desarrolla en un segundo plano, por lo que le resulta fácil pasar desapercibido.

Actualmente, expuso el órgano garante, diversos *softwares espía* se encuentran implícitos en aplicaciones informáticas, aparentemente benignas, como en los sitios de descargas de intercambio de archivos de música, películas, series, imágenes, juegos, entre otros, o bien, pueden desprenderse de la navegación en páginas de internet inseguras y poco recomendables.

El INAI destacó que, entre las implicaciones de ser afectado por *softwares espía,* es posible que terceros no autorizados puedan obtener contraseñas del usuario; conocer la ubicación geográfica de la persona en tiempo real; y acceder a las comunicaciones del titular del dispositivo, tales como mensajes de texto, llamadas y correo electrónico, entre otras.

De igual forma, recopilar información sobre hábitos e historial de navegación en la red; obtener información financiera relacionada con operaciones bancarias realizadas por internet; y acceder a la lista de contactos del dispositivo, entre otras, lo que vulnera el derecho a la protección de los datos personales del titular.

El Instituto alertó sobre algunas señales que podrían ayudar a los usuarios a reconocer que su equipo ha sido afectado por un software espía, como el funcionamiento inadecuado y lentitud en el desempeño del dispositivo; creación de iconos nuevos o no identificados con anterioridad; y la emisión de mensajes de error al realizar operaciones en la unidad, que anteriormente funcionaban en forma correcta.

Asimismo, el enlazamiento a sitios web diferentes a los predeterminadamente utilizados; apertura automática de páginas emergentes o pop-ups con contenido comercial o pornográfico; y la generación de mensajes que indican supuestas infecciones al sistema, entre otras.

En este contexto, el INAI manifestó la importancia de que las personas tomen conciencia sobre el uso informado y responsable de los dispositivos móviles y equipos de cómputo, al tiempo que emitió algunas recomendaciones para evitar ser víctima del uso de *softwares espía*:

Primero. Navegar únicamente en sitios web seguros y confiables.

Segundo. Descargar archivos, programas informáticos, aplicaciones móviles, música, videos, etc., exclusivamente en sitios reconocidos o mercados de aplicaciones oficiales.

Tercero. Conocer los permisos que requieren las aplicaciones y programas informáticos antes de su instalación.

Cuarto. Eludir páginas emergentes, pop-ups y publicidad no deseada, evitando de cualquier forma, hacer clic en éstos.

Quinto. Revisar que el sistema operativo cuente con las actualizaciones y parches de seguridad más recientes.

Sexto. Descargar un antivirus de desarrolladores reconocidos que ofrezca protección *anti-spyware*.

Séptimo. Revisar los procesos que se realizan, en segundo plano, con la finalidad de detectar irregularidades.

Octavo. En los navegadores, habilitar la opción de “bloquear ventanas emergentes”, lo cual impedirá que se abran ventanas no deseadas.

Noveno. Realizar periódicamente un análisis completo del sistema.

Décimo. Cambiar contraseñas de manera regular.

-o0o-