Publicado en Ceuta el 08/07/2019

Jose Fernández de todosmartwatch habla sobre la seguridad y protección de datos de los relojes inteligentes

Hoy en día, el reloj inteligente no es un gadget más sino una necesidad para el usuario y eso conlleva a que hay que protegerse de los ciber ataques

Los ingenieros especializados en ciberseguridad han descubierto que uno de los dispositivos más sensibles del mercado son los smartwatches o relojes inteligentes.

Cualquier usuario moderno se preocupa por mantener cargados y actualizados sus programas antivirus y antispyware en su PC, ya sea en la versión de escritorio como en las notebooks, pero pocos reparan en que otros dispositivos inteligentes no cuentan con las mismas protecciones.

Esto último es particularmente cierto para los teléfonos móviles y para el smartwatch, los cuales –además- están frecuentemente conectados por el usuario a través de Blue Tooth.

Los sensores del smartwatch se encuentran permanentemente relevando datos del usuario que podrían ser información sensible si cayesen en las manos inapropiadas. Por ejemplo, el podómetro, que el poseedor del reloj aficionado al fitness activa cada vez que emprende sus caminatas, parecería estar trabajando con datos de menor importancia.

Estos datos ingresan al dispositivo en forma de señales eléctricas que se registran y almacenan en la memoria y pueden pasar al teléfono móvil cuando se encuentra activada la interconexión entre ambos.

En principio, se trata de datos rutinarios e irrelevantes, pero a un hacker malicioso le permitirían establecer patrones de conducta del usuario del dispositivo, conocer horarios y lugares por donde se desplaza, a través del localizador GPS y la periodicidad con la cual se producen sus desplazamientos.

Toda esta información puede servir para ir armando un perfil del propietario del Smart watch que lleve a determinar su identidad, junto con otros datos sensibles a los que podría accederse, como resultaría ser una dirección de correo electrónico al momento de registrar una aplicación o cuando se activa el acceso a las credenciales de la cuenta en Android.

La forma en que esta captura de datos pudiera terminar siendo perjudicial para el usuario del dispositivo inteligente queda un poco librada a la imaginación, pero el conocimiento de su identidad y algunas rutinas diarias por parte de terceros desconocidos ya supone un riesgo.

Por lo pronto, en el mercado ilegal de bases de datos de usuarios ya podría cotizarse esta información personal, en el mejor de los casos para establecer un patrón de consumo y bombardearlo con spam publicitario.

En el peor de los casos, en poder de ciberdelincuentes, los datos podrían permitirles aplicar algoritmos especializados para desentrañar información cifrada de contraseñas o incluso instalar remotamente un software malicioso en alguno de sus dispositivos para llegar a información bancaria y de cajeros automáticos.

Lejos de constituir una presentación alarmista, esta nota pretende concientizar sobre la importancia de valorar toda la información personal y protegerla mientras se disfruta de las innovaciones tecnológicas disponibles.

Algunas simples medidas de prevención pueden resultar suficientes para evitar futuras complicaciones, a saber:

Prestar atención a los cambios en el funcionamiento del smartwatch, en especial si sus funciones se ponen más lentas repentinamente o aumenta el consumo de la batería sin causa aparente, esto podría estar indicando el ingreso de algún programa troyano en el software del equipo.
No utilizar para el inicio de sesión una dirección de correo electrónico laboral o corporativa.
Hacer caso omiso si alguna aplicación solicita datos de geolocalización.

Si una aplicación solicita recuperar información de la cuenta del usuario hay que desoír esta solicitud.
Desconfiar de cualquier pedido de otorgamiento de permisos o licencias adicionales solicitadas desde aplicaciones poco conocidas.

Datos de contacto:
Jose Fernández
8098808232

Nota de prensa publicada en: Ceuta

Categorías: Ciberseguridad Dispositivos móviles