Tus wareables, cada vez más cerca

El uso de los wearables está tomando un curso relevante en el sector de la movilidad; dentro de mercados como la salud, el ocio y el deporte. Desde Intel explican cómo asegurar estos gadgets.

En la actualidad, usted puede utilizar wearables, la tecnología que rastrea, analiza y ayuda en las tareas diarias. Y esto es una tendencia popular: ABI Research estima que en el 2019, **el mundo tendrá 780 millones de dispositivos portátiles, desde los rastreadores fitness, relojes y lentes inteligentes e incluso monitores cardíacos incorporados en el cuerpo humano.** Pero estos dispositivos conllevan ciertos riesgos, el más destacado: la probabilidad de que los ciberdelincuentes tengan acceso a su información.

¿Pero cómo es que los ciberdelincuentes tendrán acceso a su información? El eslabón más débil en el espacio wearable es su teléfono móvil y no exactamente el propio dispositivo. Esto se debe a que es usual que se vinculen ambos equipos a través de una conexión wireless de corto alcance conocida como Bluetooth. Este espectro es utilizado para enviar y recibir datos entre su wearable y su teléfono móvil, lo que hace que éste último sea el objetivo clave para los hackers.

Generalmente, los hackers acceden a los datos en su dispositivo móvil a través de aplicaciones con malware. Estas aplicaciones son a menudo diseñadas para

parecerse a aplicaciones populares, pero con suficientes diferencias que ponen en duda su autenticidad.

Los hackers pueden usar estas aplicaciones maliciosas para hacer una variedad de cosas desde llamadas, envío y recepción de textos y extraer información personal, todo sin su conocimiento. También pueden saber cuál es su ubicación a través de GPS y registrar cualquier problema de salud que haya puesto en su wereable. La cuestión es: una vez que tengan acceso a su dispositivo móvil, ellos tendrán control y una gran cantidad de recursos a su alcance.

El hacker puede utilizar esta información para llevar a cabo diversas formas de fraude. ¿Necesita una receta especial de su médico que permita la compra de su medicamento?, los hackers también. ¿Sale a correr por la mañana? Información importante para un ladrón. Estos detalles personales son solo un vistazo a la información disponible en sus dispositivos móviles.

Sin embargo, estos tipos de amenazas no se limitan a wearables. Internet de las cosas, el fenómeno de los dispositivos conectados a Internet para el análisis y la optimización, abarca todo tipo de dispositivos electrónicos, tales como lavadoras y refrigeradores que también pueden poner en peligro sus datos.

A continuación algunos consejos para poner en práctica:

Use un PIN. Todos sus dispositivos móviles deben tener una clave de identificación personal (PIN). Este método básico de seguridad es una gran manera de disuadir a los hackers o ladrones casuales para evitar que roben sus datos.

Ponga límites a la información que comparta. La mayoría de los wearables no necesitan tener acceso a cada parte de la información acerca de usted. Se puede disminuir la probabilidad del intercambio de sus datos privados de su wearable introduciendo únicamente la información que su dispositivo requiere. Por otro lado, siempre vuelva a comprobar los permisos que la aplicación de los wearables está solicitando en su dispositivo móvil. ¿Realmente necesitan acceder a su ubicación, fotos y a su agenda? Si no es necesario, asegúrese de modificar estos ajustes apropiadamente.

Utilice la seguridad total. Por supuesto, asegurar el eslabón más débil en el entorno de sus wearables, su teléfono móvil, supone que usted recorrerá un largo camino para mantener sus datos seguros. McAfee LiveSafe, nuestra solución de seguridad integral ayudará a mantener su PC segura. También McAfee Mobile Security en su dispositivo Android o iOS de forma gratuita, ayudará en la protección.

Fuente: TyN Security 06.05.2015