Publicado en Madrid el 06/02/2024

S2 Grupo advierte de que los smartwach o zapatillas que miden pasos pueden estar robando datos personales

Hoy martes 6 de febrero, se celebra el Día de la Internet Segura, iniciativa puesta en marcha para promover entre jóvenes y adultos el uso seguro y positivo de la tecnología. Desde S2 Grupo, especializada en ciberseguridad y gestión de sistemas críticos, se ha destacado que cada vez es mayor la presencia en los hogares de dispositivos IoT (Internet de las Cosas) y esto puede poner en riesgo la seguridad de los hogares y familias si no se utilizan adecuadamente

Algunos de los dispositivos IoT más comunes son los relojes inteligentes; las zapatillas que miden la distancia, recorrido y calorías consumidas; las aplicaciones para subir o bajar las persianas o graduar la luz en casa; hornos inteligentes que se encienden desde el móvil; collares para controlar el sueño de las mascotas o si tienen signos de alguna enfermedad; o cortacéspedes automáticos que realizan su mantenimiento de forma automática, entre otros.

"El problema de estos artículos conectados es que, como toda la tecnología, pueden ser hackeados. Si esto sucede, está dando muchísima información personal a los ciberdelincuentes. La más básica es informar en tiempo real de si estamos en casa o no, porque si usan la geolocalización como los smartwach, pueden saber cuándo estamos fuera y entrar, por ejemplo", ha reseñado José Rosell, socio-fundador y CEO de S2 Grupo.

"Hay numerosos informes que indican que 2024 estará marcado precisamente por los ciberriesgos y ciberamenazas a este tipo de dispositivos. Por ello, es importante que desde el punto de vista de la concienciación en ciberseguridad recordemos a todos los usuarios la necesidad de securizarlos correctamente", ha continuado Rosell.

Entre los ciberpeligros más comunes del IoT están el robo de datos personales, conocimiento de hábitos en el hogar, acceso a la geolocalización de los miembros de la familia, compras fraudulentas, robos físicos, suplantación de identidad, introducción de malware y comercio con imágenes o datos personales en mercados negros.

Recomendaciones para ciberproteger los dispositivos IoT

El equipo de expertos de S2 Grupo ha explicado que algunas recomendaciones básicas para protegerse de los ciberdelincuentes en el uso de dispositivos IoT son:

Configurar una red separada para estos dispositivos. Existen routers inteligentes que crean redes virtuales y, de esta forma, si se infectara algún equipo no podrían acceder a los dispositivos IoT ni a la inversa.

Configurar contraseñas robustas y diferentes para cada dispositivo. Además, es necesario cambiarlas periódicamente.
Deshabilitar el protocolo UPnP (Universal Plug and Play). Esto evitará que los dispositivos se encuentren entre sí de forma sencilla.
Instalar las últimas actualizaciones cuando estén disponibles. Suelen llevar asociados nuevos parches de seguridad.
Si se necesita app móvil, descargarla siempre de markets oficiales.
Revisar la configuración de seguridad del dispositivo y priorizarla siempre por encima de otras funcionalidades.
Desactivarlos cuando no se estén utilizando
Formación y concienciación en ciberseguridad para aquellos usuarios que utilizan dispositivos IoT.

Ciberpeligros de un smartwach

Desde S2 Grupo, con motivo del Día de la Internet Segura y poniendo énfasis en que el problema de ciberseguridad asociado a los dispositivos IoT puede poner en riesgo la seguridad de los hogares, ha explicado como ejemplo los problemas de ciberseguridad asociados a un reloj inteligente:

Los smartwatch se enfrentan, como el resto de dispositivos IoT, a una problemática común derivada de la inexistencia de estándares de ciberseguridad específicos para estos dispositivos.
Recogen muchísima información personal y crítica: desde la localización GPS hasta notificaciones de aplicaciones con las que haya sido conectado, datos biométricos o de salud, datos de entrenamiento, realización de pagos, etc.
Los smartwatch pueden ser hackeados: su diseño tiene muchas vulnerabilidades; su conectividad puede ser intervenida y esto implica incluso los pagos NFC; y el propio usuario puede debilitar su seguridad simplemente con contraseñas inadecuadas o no actualizar el sistema.
Algunos no permiten la instalación de antivirus.
No utilizan doble factor de autenticación: algunos smartwatch ya introducen el doble factor para hacer pagos, pero aún quedan muchos diseños que no lo han incorporado y los hacen más vulnerables.
Emparejamiento automático con otros dispositivos disponibles: es muy importante cancelar esta función para que sólo se conecte a los dispositivos que parezca oportuno y evitar conexiones inesperadas con wi-fi o Bluetooth públicos o inseguros.

Datos de contacto:
Luis Núñez
S2 Grupo
667574131

Nota de prensa publicada en: Madrid

Categorías: Nacional Software Ciberseguridad Dispositivos móviles Innovación Tecnológica