# Los peligros que ocultan los relojes inteligentes

La popularidad de los relojes inteligentes ha crecido a ojos vistas los últimos años, pero algunos de los dispositivos a la venta en el mercado podrían poner en serio riesgo la seguridad de sus usuarios.

«Los relojes inteligentes baratos de marcas dudosas tienen un soporte de baja calidad y de corta duración para los dispositivos en términos de actualizaciones de seguridad», afirma Antón Kukánov, director del Centro de Experiencia Digital de Roskachestvo, la agencia estatal rusa de control de calidad.

En una entrevista con Rossiyskaya Gazeta, el especialista puso de relieve que en muchos de los relojes inteligentes más asequibles, de marcas menos conocidas, los datos de geolocalización y otra información personal no siempre están encriptados. Esto significa que **pueden ser interceptados**, lo que es especialmente preocupante en el caso de que los usuarios sean niños.

**Niños en riesgo**

Una investigación publicada a finales de 2019 en el Reino Unido reveló que algunos de los relojes utilizados por niños para que sus padres puedan localizarlos en cualquier momento, pueden ser fácilmente invadidos. El fallo permite que cualquiera tenga **acceso a la ubicación** de los pequeños usuarios de estos dispositivos.

Los investigadores encontraron, además, que los mensajes de voz intercambiados entre padres y niños a través de la función *walkie-talkie* de estos dispositivos se grababan y almacenaban en una nube digital insegura. El sistema de

almacenamiento permitía a cualquiera descargar y **escuchar los archivos de audio**, detalló TechCrunch.

Según los investigadores, los fallos fueron reportados a los desarrolladores de los dispositivos entre 2015 y 2017, lo que hizo que muchas marcas eliminaran la vulnerabilidad de sus sistemas. Sin embargo, muchas empresas simplemente ignoraron las advertencias, razón por la cual los investigadores decidieron hacer públicos sus hallazgos.

**Robo de información**

Otra investigación, llevada a cabo por Kaspersky, compañía rusa dedicada a la ciberseguridad, demostró que es posible recopilar datos obtenidos del sensor de aceleración de un reloj inteligente a través de un programa malicioso.

Los experimentos llevados a cabo por los expertos de la empresa mostraron que, con un *malware*, se puede obtener información valiosa sobre el usuario del dispositivo, como sus movimientos y sus hábitos. Aunque más complejo, es posible incluso identificar cosas escritas en una computadora, como la contraseña de la máquina portátil, por ejemplo.En el caso investigado por Kaspersky, evitar el problema mencionado es

más fácil y depende exclusivamente del usuario. Basta no instalar aplicaciones desconocidas y no dar demasiados permisos a las ‘apps’ que decidas tener en tu reloj inteligente.

**Hora de la medicación**

Otra investigación, realizada en el Reino Unido por la compañía PenTestPartners, mostró que un reloj inteligente, popular entre personas mayores y pacientes con demencia, podría ser **fácilmente invadido por *hackers***. Los investigadores descubrieron que era posible engañar al reloj inteligente para que enviara recordatorios falsos informando que era la hora de tomar ciertos medicamentos.

«Es poco probable que una persona que sufre de demencia recuerde que ya ha tomado su medicación. Podría resultar fácilmente una sobredosis», apuntó la compañía.

Los investigadores lograron, además, hacer llamadas y enviar mensajes de texto a partir de los dispositivos, así como acceder a la cámara de estos relojes inteligentes.Anton Kukánov, de Roskachestvo, consideró que no todos los fabricantes de relojes inteligentes se preocupan de la seguridad de los datos del usuario, en particular los de los dispositivos más baratos. Por esta razón, recomendó elegir *gadgets* de marcas más confiables, aunque sus precios sean más elevados. Además, subrayó la importancia de establecer estrictas configuraciones de privacidad en estos aparatos.

Fuente: elpais.