El fraude detrás de las aplicaciones que aseguran medir la presión arterial o tomar la fiebre

23/08/2023

Los **programas o aplicaciones** maliciosas no sólo se camuflan en juegos o utilidades. En algunas ocasiones, existen otras apps que **prometen y ofrecen servicios o funciones que no pueden cumplir**, como es el caso de aquellas que anuncian medir la presión arterial o tomar la fiebre.

A pesar de que sea casi una obviedad, **ni los celulares ni las tablets son capaces de revisar la presión arterial, revisar la temperatura corporal o diagnosticar algún tipo de enfermedad.** Sin embargo, tanto Google Play como App Store ofrecen, en su catálogo, dichas herramientas.

«Blood Presure Star» y «Monitor de Presión Arterial», son algunos de los resultados que figuran dentro de las primeras opciones. Sin embargo, y a pesar de que **tales aplicaciones no**

son herramientas válidas para un diagnóstico, cuentan con millones de descargas.

Tras los títulos engañosos se encuentran apps que, en realidad, sirven para llevar un registro de mediciones y brindan recomendaciones para hipertensos o hipotensos. En estos casos, **los usuarios se llevan una gran decepción al ver que, en efecto, no cumplen con lo que prometen.**

Listado de aplicaciones. Foto: Captura de pantalla.

Un software no es capaz de brindarle a un celular la habilidad para desarrollar estas tareas que dependen puramente de elementos físicos, es decir, de hardware. Esto significa que **los dispositivos electrónicos actuales no poseen los sensores necesarios para medir la presión arterial o tomar la fiebre.**

Sin embargo, **existen dispositivos que son capaces de llevar a cabo dichas tareas**. El teléfono Honor Play 4 y el Watch 8 de Apple cuentan con un **sensor infrarrojo especial** en sus pantallas que les permite llegar a un resultado aproximado.

¿Con qué fin los desarrolladores lanzan estas apps al mercado?

- Mayoritariamente, buscan un gran volúmen de descargas en poco tiempo.
- En caso de que su app sea descargada por varias personas, se posicionará dentro de un listado que les dará visibilidad.
- Con dicha visibilidad, tienen la capacidad de monetizar sus aplicaciones, generando ingresos de forma rápida e inmediata.
- Existe la posibilidad de que las apps vengan acompañadas de malwares o virus que, una vez descargada, se inyectan

directamente en los dispositivos afectando datos sensibles y vulnerando contraseñas.

Hay otros comportamientos que preocupan en muchas de esas aplicaciones. En algunos casos, al revisar su **política de privacidad** se encuentra que **recopilan datos como números telefónicos, direcciones de email, género y nombre del usuario.** Además, si se vinculan cuentas de otros servicios (por ejemplo Google o Facebook) dicen que podrían acceder a los contactos de esos entornos.

Hackers, ciberataque. Foto: Unsplash.

Si bien en muchos casos tienen puntajes altos, al leer las reseñas se puede descubrir el engaño. Muchas de las positivas están escritas con un lenguaje raro e incomprensible, **producto de la acción de un bot**. "Nunca había tenido un ánimo tan alto de mi enfermedad", se lee en una review con cinco estrellas.

En estos casos, que son demasiado habituales, **los developers compran paquetes de reseñas positivas para generar confianza en los usuarios.**

Resulta fundamental **corroborar reseñas y evitar descargar aplicaciones que, a simple vista, no resultan confiables o prometen cosas imposibles.** Sin embargo, esto podría significar un avance significativo para las empresas tecnológicas, que podrían desarrollar herramientas acordes y acabarían con las aplicaciones maliciosas.

Fuente – Canal 26