LITORALPRESS

Fecha: 17-05-2023 **Visitas:** 697.475 **Favorabilidad:** ☐ No Definida
Fuente: La Tercera Online
Título: **¿Tienes el Bluetooth siempre encendido en tu celular? Estos son los potenciales riesgos a los que te expones**

Link: https://www.latercera.com/tendencias/noticia/tienes-el-bluetooth-siempre-encendido-en-tu-celular-estos-son-los-potenciales-riesgos-a-los-que-te-expones/I6DPUV3U3ZFDDJ7ZFQTMFIKKR4/

Desde robar tus datos hasta acceder a fotos y videos. Acá, expertos en ciberseguridad explican los posibles riesgos y entregan sus recomendaciones al respecto. Conectar dispositivos electrónicos a través de Bluetooth puede ser cómodo y útil durante la rutina. Esta tecnología permite que puedas utilizar artefactos como audífonos o parlantes, sin la necesidad de usar cables y en espacios como el transporte público o mientras estás en movimiento. Pero, ¿eres una de las personas que siempre deja esta función activada en el teléfono celular? Bueno, hay ciertos riesgos que podrían afectar a tu seguridad. En 2017, la empresa de ciberseguridad Armis descubrió un conjunto de vulnerabilidades (fallas) para hackear a través de Bluetooth, que pusieron en un potencial riesgo a cerca de 8.000 millones de dispositivos. Mediante estas ""las cuales fueron agrupadas con el nombre BlueBorne"" los delincuentes digitales encontraron formas de interceptar a sus objetivos, los cuales podían ir desde teléfonos celulares hasta computadores y otros objetos electrónicos con Bluetooth.

Qué es el Phishing y cómo denunciarlo: las estafas digitales que amenazan a los chilenos "BlueBorne permite a los atacantes tomar el control de dispositivos, acceder a datos y redes corporativas, penetrar en redes seguras "˜air-gapped' (es decir, deshabilitar la conexión) y propagar malware (un programa malicioso) lateralmente a dispositivos adyacentes", aseguraron desde la compañía. En otras palabras, este conjunto de fallas "se puede utilizar para una amplia gama de delitos", que incluyen desde acceder a tu información personal hasta obtener fotos y videos desde el aparato que es interceptado.

Si bien, después de aquella advertencia en 2017 distintos sistemas operativos implementaron nuevas medidas de seguridad para proteger a sus usuarios, desde Armis enfatizaron: "Creemos que muchas más vulnerabilidades esperan ser descubiertas en las diversas plataformas que utilizan Bluetooth". Frente a este escenario, expertos en ciberseguridad conversaron con La Tercera para descifrar cuáles son los posibles riesgos a los que podrías estar exponiéndote en la actualidad. ¿Tienes el Bluetooth siempre encendido en tu celular? Estos son los potenciales riesgos a los que te expones. Foto: referencial.

Por este último punto, añade que "por la vía convencional, se le puede hacer difícil a un hacker vincularse con un dispositivo si es que no ha tenido una conexión previa", debido a que sistemas como Android e iOS han tomado resguardos para prevenir estas situaciones.

Los ataques "más graves y efectivos", dice Álvarez, aparecen cuando los ciberdelincuentes encuentran "vulnerabilidades de día cero", las cuales se caracterizan ""en términos sencillos"" porque los desarrolladores no saben de su existencia y los atacantes se aprovechan de ellas tras identificarlas primero. Dentro de esa categoría, entran las que hallaron los especialistas de Armis en 2017, mientras que su aparición incita a los responsables en este ámbito a tomar medidas rápidas para evitar interceptaciones de gran magnitud.

"Así, los atacantes pueden realmente perpetrar una acción masiva, de robar información y de tomar control de los aparatos incluso para otro tipo de ilícitos ", explica el académico. ¿Tienes el Bluetooth siempre encendido en tu celular? Estos son los potenciales riesgos a los que te expones. Foto: referencial.


¿Tienes el Bluetooth siempre encendido en tu celular? Estos son los potenciales riesgos a los que te expones

Álvarez cuenta que también existen métodos poco recurrentes mediante los cuales los cibercriminales podrían saber si el dispositivo de una persona (un teléfono celular, reloj inteligente u otro con Bluetooth de baja energía) está presente en un lugar o no. "Otros ataques un poco más comunes podrían ser los de plantar un dispositivo malicioso, como un parlante con Bluetooth, para que tú te conectes. Puede ser en un hostal, en un hotel, por ejemplo, anda a saber tú.

Este aparato podría tener dentro un firmware, un software modificado para que en este caso cuando vincules tu dispositivo por Bluetooth, este te instale un malware (un programa malicioso) o sustraiga datos de tu teléfono". "Esa también puede ser una posibilidad", añade Álvarez, "la enseñanza que se podría sacar de un caso como ese, es que uno tiene que ser bastante suspicaz respecto al dispositivo al que te estás conectando y si te genera confianza o no". ¿Tienes el Bluetooth siempre encendido en tu celular? Estos son los potenciales riesgos a los que te expones. Foto: referencial.

En esos casos, en donde se descarga una aplicación de fuente no confiable que podría contener amenazas, los usuarios se enfrentan a que "te pueden dejar abierto el Bluetooth, la geolocalización, el micrófono o la cámara de video, sin que tú te des cuenta". Si pensamos en un caso hipotético en el que buscas una aplicación gratuita para escuchar música en alta fidelidad y encuentras una que promete un extenso catálogo en un foro no especializado o que no está verificado por una tienda oficial como la App Store, podría ocurrir lo siguiente, según el experto en ciberseguridad de la UAI. "Ahí podrían aparecer distintos tipos de exfiltración de datos. Por ejemplo, si el Bluetooth de tu teléfono celular se conecta a una red de internet, sin que lo notes podrían estar mandando

datos, que pueden ser información confidencial, fotos o videos, entre otros. Podrían estar enviando eso para otro lado, para el sitio del atacante en este caso.

Ese es un alto riesgo". En este sentido, Seguel añade que un escenario similar podría ocurrir si los cibercriminales logran acceder a la cámara o el micrófono de tu dispositivo, con lo que eventualmente podrían revisar "todo lo que puedas estar hablando, filmando o fotografiando". ¿Tienes el Bluetooth siempre encendido en tu celular? Estos son los potenciales riesgos a los que te expones. Foto: referencial.

"Después, el problema es que te pueden extorsionar ". Aún así, subraya que estos casos no son tan frecuentes en la población general, lo que no quita que haya que tener ciertos cuidados a la hora de descargar contenidos en la internet. ¿Tu aplicación de WhatsApp es real? Los peligros de los "clones" que podrían filtrar tu información privada Es por esto que Claudio Álvarez, el especialista de la Universidad de los Andes, enumera tres recomendaciones esenciales para los usuarios: "La primera es mantener siempre apagado lo que es el modo de descubrimiento o de apareamiento de Bluetooth. La segunda es que realmente no te conectes a un aparato que no conoces y sobre el cual no tienes mayores referencias. Y la tercera, yo diría que usar Bluetooth quizás lo justo y necesario, cuando estás con los audífonos puestos, por ejemplo. Tratar de mantenerlo apagado cuando no lo estés usando te ahorrará nivel de batería y también disminuirá la posibilidad de que tu teléfono pudiera ser comprometido con alguna vulnerabilidad de día cero".