¿Qué es el bluesnarfing?

Toda innovación viene acompañada de quienes quieren aprovecharla en su beneficio. En ocasiones, con métodos que rozan la ilegalidad. Llamadas fraudulentas, mensajes engañosos, enlaces dañinos… La lista es interminable, y tampoco ayuda que desde los países anglosajones se les bautice con nombres como phishing, vishing o smishing. Y mientras que muchos métodos implican el uso de la ingeniería social, otros directamente emplean técnicas de hackeo que aprovechan vulnerabilidades de nuestros dispositivos y aparatos conectados. Es el caso del bluesnarfing, que como indica su nombre, tiene que ver con una tecnología tan popular como es el Bluetooth.

El bluesnarfing es, citando la Wikipedia, “el acceso no autorizado a información de un dispositivo móvil por medio de una conexión Bluetooth, normalmente entre teléfonos, ordenadores de sobremesa o portátiles y PDAs”. ¿Qué clase de información? “Calendarios, lista de contactos, correos electrónicos y mensajes de texto”. “En algunos teléfonos móviles, los usuarios pueden incluso copiar fotos o vídeos privados”.

Tal es su popularidad que hasta la Policía Nacional le dedica un video en TikTok. También habla de ello la OCU, es decir, la Organización de Consumidores y Usuarios, y hasta algunos bancos lo mencionan en sus blogs. ¿Qué dice la Policía Nacional? “Basta con que el ciberdelincuente se encuentre a 10 o 15 metros de distancia y tú tengas el Bluetooth activado para que puedan acceder a tu teléfono”. El objetivo de esta amenaza es “robar datos”. En concreto, “contactos, correos electrónicos, mensajes e incluso archivos almacenados en el móvil”. Con esos datos se pueden cometer estafas o extorsiones. O aparecer en la Dark Web. ¿Qué hay de cierto en esto y hasta qué punto supone el bluesnarfing una amenaza real?

La tecnología Bluetooth es muy popular porque ha sustituido las conexiones por cable. Auriculares, pulseras y relojes inteligentes, televisores, mandos de juego y toda clase de dispositivos se pueden conectar a tu teléfono móvil o a tu ordenador con una tecnología inalámbrica emparentada con el WiFi y que está presente en millones de aparatos. Y cuando una tecnología se vuelve tan popular, es normal que se convierta en objetivo de los ciberdelincuentes.

No hace falta buscar mucho para encontrar casos en los que el Bluetooth es el protagonista debido a fallos, errores y vulnerabilidades encontradas en esta tecnología. A finales del

año pasado, unos investigadores encontraron una vulnerabilidad en Bluetooth que afectaba a las versiones de Bluetooth 4.2 a 5.3. Es decir, un abanico que abarca prácticamente cualquier aparato fabricado en los últimos años. Bluetooth 5.4 se publicó en febrero de 2023 y su actualización Bluetooth 6.0 se anunció este verano. Pero tardará en llegar a las tiendas.

También se encontraron otras vulnerabilidades a finales de 2021, a finales de 2020 y en el verano de 2019. Popularidad y agujeros de seguridad. La combinación perfecta. Además, tengamos en cuenta que el rango de alcance del Bluetooth puede llegar tranquilamente a los 10 metros. Y con la tecnología adecuada, ampliar el rango a 100 metros. Sin embargo, no es tan simple como pueda parecer.

Qué hay de cierto en el bluesnarfing

El bluesnarfing es una realidad. Se conoce desde 2003. Ese año se descubrió la primera de muchas vulnerabilidades del protocolo Bluetooth. Que si bien es relativamente seguro, prima más la facilidad de uso. Y aunque cada nueva versión es más segura que la anterior, todavía hay mucho por mejorar. En esa primera vulnerabilidad, “los datos podrían obtenerse de forma anónima sin el conocimiento o consentimiento del propietario y los dispositivos previamente emparejados podrían acceder al contenido completo de la memoria de algunos dispositivos (incluso después de que los dispositivos se eliminen de la lista de dispositivos emparejados con el dispositivo original)”.

Para que este hackeo sea efectivo, se tienen que unir varios elementos. Primero, la víctima tiene el Bluetooth activo en su dispositivo, normalmente el teléfono móvil. Aunque también podría ser una tableta o un ordenador portátil. Segundo, además de tener el Bluetooth activado, debe estar configurado para ser visible por otros dispositivos que se encuentren cerca. Así, los cibercriminales buscan este tipo de aparatos susceptibles de ser interceptados en lugares de mucha concurrencia, como estaciones de tren o centros comerciales. Para ello, pueden emplear métodos propios o hacerse con programas y aplicaciones especializados que pueden descargar o comprar en la Dark Web.

Sin embargo, que la conexión o enlace sea posible, es una cosa. Que tenga acceso a tus datos es algo distinto. El objetivo es obtener cuantos más datos mejor. Correos, mensajes, contactos, archivos, fotos, videos… Todo lo que pueda usarse para extorsionarte o engañarte para, finalmente, obtener datos más jugosos como tu cuenta bancaria o tu tarjeta de crédito. En el

peor de los casos, hasta se podría aprovechar este hackeo para instalar malware que recopile datos.

Consejos para protegerte del bluesnarfing

Ahora ya sabemos que el bluesnarfing es posible. También sabemos que no es tan fácil como encender tu teléfono y probar suerte como quien busca un punto WiFi abierto. Pero no podemos descartar del todo que nos topemos con alguien con los conocimientos necesarios o la aplicación capaz de hacer ese trabajo tan desagradable. En especial si estás en un sitio con mucha gente, como una plaza, un centro comercial, un aeropuerto o lugares turísticos.

Además, hay muchas maneras de ponérselo difícil a los ciberdelincuentes. Acciones que a buen seguro ya realices con frecuencia para evitar toda clase de fraudes y peligros que puedes encontrarte en internet. Solo hay que tomar ciertas precauciones y seguir disfrutando de las ventajas y comodidad que ofrece el Bluetooth para conectar teléfonos, auriculares y demás aparatos sin cables.

Para empezar, los teléfonos móviles actuales incorporan de serie medidas de seguridad para evitar este tipo de problema. La visibilidad del Bluetooth depende de nosotros, pero las conexiones automáticas ya no son posibles. Debes ser tú quien acepte la conexión. Así que aquí van varios consejos para evitar el bluesnarfing. Por otro lado, los terminales más recientes utilizan Bluetooth de baja energía o BLE, que es más seguro y eficiente.

Mantén actualizado el software de tu teléfono.

Procura actualizar las aplicaciones que tienes instaladas.

Revisa periódicamente los permisos de las apps instaladas.

En nuestro caso particular, los permisos de acceso al Bluetooth.

No aceptes notificaciones sin revisarlas.

Desactiva el Bluetooth si no lo vas a utilizar.

Si es posible, desactiva la visibilidad Bluetooth del dispositivo.

Y en dispositivos antiguos, desactiva el emparejamiento automático.

Elimina dispositivos vinculados anteriores si ya no los

utilizas.

Con información de Hipertextual