Publicado en España el 13/05/2021

Los juguetes sexuales conectados son el nuevo objetivo de los ciberdelincuentes

La empresa especializada en ciberseguridad S2 Grupo, advierte de que en el último año el sector de la llamada "sexnología" (sexo+tecnología), juguetes sexuales conectados a Internet, ha experimentado un incremento notable que ha ido acompañado de un aumento de sus ciberriesgos y se ha convertido en uno de los nuevos objetivos de los ciberdelincuentes

Según detalla S2 grupo en un comunicado de prensa “como toda tecnología, la 'sexnología' también se ha convertido en nuevo blanco de los delincuentes en la red". En este sentido, es muy importante utilizarla de una forma cibersegura, porque si no se gestiona adecuadamente, las consecuencias pueden llegar a ser muy graves. En este caso, los ciberdelincuentes "manejan información muy sensible, muy íntima, que puede ser de gran impacto para la vida personal o profesional de la víctima”, ha declarado José Rosell, socio-director de S2 Grupo.

“Ya hemos conocido varios casos de ciberataques a este tipo de juguetes. Uno de los más conocidos fue el hackeo de un dispositivo conectado tipo cinturón de castidad en el que el atacante bloqueó el sistema de apertura y pidió un rescate a las vícctimas en forma de bitcoins. Cualquier aparato que se conecta a Internet conlleva un riesgo, pero en el caso de la sexnología el riesgo es extremo”, ha explicado Miguel A. Juan, socio-director de S2 Grupo.

Principales ciberpeligros de la sexnología

De este modo, el equipo de expertos de S2 Grupo señala que algunos de los principales ciberpeligros de los juguetes sexnológicos son:

Sus fabricantes no tienen en cuenta la seguridad informática del aparato en su proceso de creación. Únicamente se atiende a la funcionalidad, aspecto y coste reducido. Es común su fabricación masiva en China sin atender normas de seguridad o privacidad para proteger el aparato y la información que almacene.

Proporciona información a los ciberdelincuentes muy sensible como pueden ser hábitos sexuales, lugares, horarios, imágenes, conversaciones o, incluso, si se detecta infidelidad, por ejemplo.

Los usuarios lo ven como un juguete inofensivo, lo que hace que no tomen las mismas precauciones de ciberseguridad que con un ordenador. Errores comunes son el uso de contraseñas blandas o no actualizar el sistema.

“Los ciberdelincuentes saben que es un camino más para lucrarse y lo están utilizando. Por eso, intentarán sacarle el mayor partido a cualquier tipo de vulnerabilidad en el aparato, en la cuenta de la persona, en los servidores o en la aplicación que lo gestione”, ha afirmado Miguel A. Juan.

“Lograr acceder al tipo de información que registra la sexnología, los hace pasar al chantaje

rápidamente porque saben que muchas víctimas van a preferir pagar que verse expuestos públicamente", ha enfatizado José Rosell.

Recomendaciones para un uso seguro de la sexnología

Desde S2 Grupo se recomienda seguir los consejos básicos de ciberseguridad que se utilizan en cualquier dispositivo conectado: uso de contraseñas únicas y robustas, proteger el acceso a la red Wifi de casa con una buena contraseña y confirmar que no haya nadie más utilizándola, nunca utilizar estos dispositivos con redes Wifi públicas. Además, el comunicado de la compañía recuerda la importancia de "informarse de la seriedad del fabricante y de su compromiso con la fabricación de cibersegura de sus productos, actualizar periódicamente el dispositivo y, por supuesto, sentido común y no compartir nada que pudiera hacer daño a una persona si se expusiera públicamente".

Datos de contacto:
Luis Núñez
667574131

Nota de prensa publicada en: España

Categorías: Nacional Sociedad Entretenimiento E-Commerce Ciberseguridad