

---

¿Espionaje? También hay que cuidarse de los dispositivos inteligentes

02/01/2020



Es fácil olvidar, pero todo tipo de aparatos inteligentes \_desde altavoces conectadas a internet con asistente de voz, como Alexa de Amazon, hasta televisores con Netflix integrado\_ pueden estar escuchando a los usuarios y, a veces, incluso viéndolos. Como con la mayoría de la nueva tecnología, instalar dichos dispositivos significa sopesar por un lado los riesgos de invasión a la intimidad y por el otro la practicidad que ofrecen.

La firma de investigación IDC calcula que se compraron a nivel mundial 815 millones de altavoces inteligentes, cámaras de seguridad y otros dispositivos en 2019, 23% más que en 2018. Muchas de las ventas fueron para hacer regalos.

Puedes evitar todo riesgo si devuelves de inmediato los dispositivos, pero si decides quedártelos \_y la inteligencia artificial que los acompaña\_ hay algunas cosas que puedes hacer para minimizar su posible espionaje:

#### LOS ALTAVOCES ESCUCHAN... Y ALGUNOS OBSERVAN

Lps altavoces inteligentes como Echo de Amazon y Google Home te permiten revisar el estado del tiempo y hacer citas con comandos sencillos de voz. Las versiones más equipadas incluyen cámaras y pantallas.

Muchos de estos dispositivos escuchan constantemente, a la espera de recibir comandos, y se conectan a servidores corporativos para su ejecución. Comúnmente, ignoran conversaciones privadas y transmitirán grabaciones de sonido sólo cuando el usuario activa el dispositivo. Algunos tienen un botón de silencio para deshabilitar por completo los micrófonos, pero no hay forma fácil para verificar esas protecciones.

Y otra cosa: los comandos de voz enviados por internet suelen almacenarse por tiempo indefinido e incluyen las conversaciones que los usuarios hacen en el fondo. Puede accederse a ellas para demandas e investigaciones.

En cuanto a los modelos con pantallas, muchos también tienen cámaras para videochats. Considera la posibilidad de apagar o voltear al dispositivo hacia la pared cuando no lo usas.

## SEGURIDAD CON VIDEO DE SEGURIDAD

Las cámaras de seguridad en línea te permiten ver a tus mascotas o hijos cuando no estás en casa. ¿Lo malo? Si tú puedes ver el video en una aplicación, es posible que un hacker habilidoso también lo pueda hacer.

Si usas la misma contraseña para varios servicios, un hacker que logre robar tu contraseña también podrá utilizarla para el servicio de cámara. Así que no utilices la misma contraseña.

## ¿LAS CERRADURAS INTELIGENTES SON TAN INTELIGENTES?

Las cerraduras inteligentes te permiten abrir las puertas con una app para que permitas la entrada a invitados si no estás en casa. Los ladrones podrían intentar hackear el sistema, aunque es más fácil para ellos romper una ventana.

Como precaución, deshabilita cualquier capacidad para abrir puertas con un comando en un altavoz inteligente, sobre todo si tienes hijos traviosos o adolescentes que quieran meter a alguien a escondidas.

## EN CUANTO A LOS TELEVISORES

Muchos televisores inteligentes o dispositivos para que permiten recibir streaming tienen micrófonos para controles activados por voz y búsqueda de videos. Eso significa que hay fragmentos de audio que son transmitidos por internet. Las mismas advertencias para los altavoces inteligentes se aplican aquí.

## JUGUETES QUE HABLAN

Los niños podrán estar encantados con muñecas u otros juguetes que responden a la voz, pero si el juguete está conectado a internet, pon atención en cuánto control da a los padres y si permite que los niños se conecten con el mundo externo.

---