Publicado en Ciudad de México el 13/12/2018

# [Avast comparte consejos de seguridad para la compra de dispositivos IoT en estas fiestas](http://www.notasdeprensa.es)

## Es recomendable hacer una investigación adecuada antes de regalar un dispositivo de IoT en esta temporada, para evitar ponerse a sí mismo o a los seres queridos en riesgo de robo de datos personales, pérdidas financieras y tecnología que comprometa la privacidad

 Es época de agasajar con regalos y para ello es importante elegir con tiempo y tener en cuenta varios aspectos, especialmente si se tiene en mente un producto tecnológico para obsequiar. Martin Hron, Investigador Senior de Seguridad de Avast (LSE: AVST), el líder mundial en productos de ciberseguridad, comparte 7 consejos de seguridad para los usuarios interesados en comprar dispositivos de Internet de las Cosas en esta temporada navideña. Comparar el precio. Es recomendable verificar el precio del dispositivo con otros productos similares. Si está en el mismo rango, es una buena señal. Si es drásticamente más bajo que sus competidores, es momento de considerar por qué y profundizar más sobre la calidad del producto. Mirar la marca. Si no es una marca conocida, consulte qué vendedores la ofrecen. Luego, aconsejan verificar cuánta información sobre el dispositivo está disponible en el sitio web del proveedor. Es importante buscar detalles, incluidas las especificaciones técnicas, los programas para futuras actualizaciones de software/firmware, la última vez que se emitió una actualización de software/firmware y el nivel de soporte del dispositivo proporcionado por el fabricante. Revisar cuidadosamente el diseño del sitio web. ¿La empresa en cuestión utiliza HTTP o HTTPS en su URL? Las empresas preocupadas por la seguridad definitivamente utilizarán HTTPS, el protocolo de Internet que encripta la conexión entre el usuario final y el sitio web. Si bien esto está relacionado con la seguridad del sitio web del producto y no con el producto en sí, puede ser un buen indicador de cuánto valora la compañía la seguridad. Además, si el producto a comprar tiene páginas de administración o un portal en Internet y la página de inicio de sesión usa HTTP, se debería considerar otro producto con una página de inicio de sesión que use HTTPS. Revisar las capacidades. ¿Qué información recopila el dispositivo? ¿Utiliza un micrófono o una cámara? Recomiendan evaluar los datos que podría recopilar el dispositivo y evaluar qué pasaría si esa información, que podría incluir datos personales, cayera en las manos equivocadas. Más importante aún, es cuestionar la integridad de la recolección de datos en sí. ¿Es correcto que el dispositivo tenga acceso a esta información? Si la respuesta es and #39;no and #39;, vale la pena pensarlo dos veces antes de comprar el producto. Verificar los detalles de CVE. CVE significa vulnerabilidades y exposiciones comunes, y hay un sitio disponible al público que enumera a los proveedores y todas las vulnerabilidades conocidas asociadas con ellos. Recomiendan hacer una búsqueda del fabricante del dispositivo que se está considerando en la página del proveedor de CVE y comprobar si hay informes de vulnerabilidades de alta seguridad y busque versiones de productos específicos. Como paso adicional, comparar la fecha en que se detectó la vulnerabilidad en la página del proveedor de CVE con la fecha en que el proveedor o fabricante actualizó el software/ firmware. Esto puede ser un buen indicador de la rapidez con que el proveedor o el fabricante corrige las vulnerabilidades conocidas. Buscar comentarios de usuarios. Si están disponibles, es recomendable leer los comentarios de usuarios sobre el producto. Verifique la calificación y el número de descargas para tener una idea de si otros usuarios lo elogian o han tenido problemas con él. Mire las reseñas tanto positivas como negativas y considere si son revisiones reales con suficiente detalle que tengan sentido, o solo reseñas de una palabra que lo califican con 4 o 5 estrellas, posible indicador de que pueden ser falsas. Considerar el proceso de configuración. Investigar el proceso de configuración del producto y verificar si menciona la seguridad es muy importante, especialmente el verificar si la configuración requiere que los usuarios cambien la contraseña predeterminada por una más compleja. Si el proceso de configuración es simplemente encender el dispositivo y eso es todo, sin ninguna mención de seguridad y protección, podría ser una bandera roja. Los dispositivos IoT pueden ser extremadamente cómodos y divertidos, pero lo que muchas personas no se dan cuenta es cuán vulnerables pueden ser. Un hacker solo necesita un dispositivo vulnerable para acceder a toda la red doméstica. Por lo tanto, es recomendable hacer una investigación adecuada antes de regalar un dispositivo de IoT en esta temporada, para evitar ponerse a sí mismo o a los seres queridos en riesgo de robo de datos personales, pérdidas financieras y tecnología que comprometa la privacidad. Asegurar dispositivos IoTEs vital configurar dispositivos con una fuerte seguridad, a través de los siguientes pasos. Cambiar la contraseña predeterminada en el dispositivo a algo que no se pueda rastrear. Muchos dispositivos vienen con credenciales de inicio de sesión predeterminadas, la mayoría de las cuales se pueden encontrar en línea, ya que generalmente se incluyen en el manual del usuario del dispositivo. Las contraseñas seguras deben tener al menos 10 caracteres, idealmente 16 o más que se recuerden con facilidad, para evitar tener que escribirlas. Crear oraciones como contraseñas puede ayudar. Hacer lo mismo que arriba para el router al que se conectará el dispositivo. Agregar un nuevo dispositivo brinda una buena oportunidad para cambiar la contraseña del router al mismo tiempo. Y si permite la autenticación de dos factores, es recomendable habilitarlo. Estar atento a las actualizaciones del software o firmware del dispositivo, y actualizar tan pronto como estén disponibles. Esto mantendrá el dispositivo funcionando con un rendimiento óptimo con la máxima seguridad. Acerca de AvastAvast (LSE: AVST) es el líder global en productos de seguridad digital. Con más de 400 millones de usuarios en línea, Avast ofrece productos bajo las marcas Avast y AVG que protegen a los usuarios de amenazas en la red y en el escenario de amenazas cambiantes del Internet de las Cosas. La red de detección de amenazas de la compañía se encuentra entre las más avanzadas del mundo, usando tecnologías de aprendizaje automático y de inteligencia artificial para detectar y detener amenazas en tiempo real. La seguridad de productos digitales de Avast para dispositivos móviles, computadores personales y Mac están bien conceptuados y certificados por VB100, AV-Comparatives, AV-Test, OPSWAT, ICSA Labs, West Coast Labs y otros. Para más información, visite www.avast.com

**Datos de contacto:**

Marketing Q S

Agencia de Relaciones Públicas

+ 52 55 5615

Nota de prensa publicada en: [https://www.mexicopress.com.mx/avast-comparte-consejos-de-seguridad-para-la](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Artes Visuales Software Ciberseguridad Dispositivos móviles Ciudad de México



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)