Publicado en Ciudad de México el 15/12/2017

# [5 Consejos de Avast para evitar ofertas falsas en estas fiestas](http://www.notasdeprensa.es)

## En esta época de compras navideñas, los ciberdelincuentes se muestran más activos que nunca, es por ello que los usuarios deben estar más alertas que nunca y por ello, Avast comparte 5 consejos para evitar caer en ofertas falsas

 Llegó la hora de las compras navideñas y muchos mexicanos optarán por las compras en línea para evitar el tráfico, las largas filas, el frío y para no tener que cargar pesadas bolsas. Los ciberdelincuentes saben lo mucho que los usuarios de internet aprecian la conveniencia de este tipo de compras y aprovechan esto para propagar sus propias ofertas “especiales” falsas, es por eso que Avast, líder mundial en productos de seguridad digital comparte 5 consejos para evitar caer en ofertas falsas. Los ciberdelincuentes aprendieron de los malhechores que ofrecen mercadería falsa en las calles: para vender, hay que hacer que los productos se vean tan reales como sea posible, por lo que los ciberdelincuentes suelen hacer que sus ofertas falsas sean muy parecidas a los productos reales. Cristian Gallardo, Gerente Regional de Avast para América Latina, comparte cinco puntos que los compradores deben tener en cuenta para evitar ser engañados con ofertas falsas: 1. Algunos precios son demasiado buenos para ser ciertosUn descuento siempre entusiasma, pero hay que tener cuidado cuando las ofertas son muy inferiores al precio de mercado, ya que puede ser una señal de alerta. 2. Hay que tener cuidado con lo desconocido Ya sea en las redes sociales o en un aviso en línea, los compradores deben tener cuidado cuando se trata de comercios desconocidos, en especial si promocionan ofertas a precios ridículamente bajos. Antes de arriesgarse a comprar en una tienda en línea desconocida, los compradores deben tratar de averiguar algo más sobre ese comercio, como por ejemplo su sitio web o sus redes sociales. Más importante aún, deben buscar comentarios de otros compradores sobre ese vendedor. Si no hay comentarios positivos, y si el sitio web o el perfil en las redes sociales no parece ser algo establecido o profesional, es preferible dirigirse a una tienda conocida y confiable. 3. Correos electrónicos con phishingEs habitual que las bandejas de entrada del correo se vean abarrotadas con descuentos, promociones y publicidad, por lo que es entendible que alguna correo de oferta con phishing se cuele y logre engañar al usuario. Muchos de estos correos incluyen enlaces a sitios maliciosos que se ven igual que los verdaderos y es difícil darse cuenta de que no lo son. Siempre es más seguro escribir la URL directamente en el navegador y no pulsar los enlaces o abrir archivos adjuntos que se incluyen en correos electrónicos promocionales. Las mismas precauciones deben tomarse no solo en las tiendas en línea, sino también con los bancos y otras instituciones financieras. 4. Los usuarios deben ser responsables al momento de pagarAl confirmar la compra, los usuarios deben fijarse en el candado HTTPS verde que se encuentra junto a la dirección del sitio en la barra de direcciones del navegador. El protocolo HTTPS encripta los datos cuando se envían a través de la red. Si la página de pago no tiene el candado HTTPS, no se deben ingresar datos personales ni financieros. Es más, si una tienda no acepta medios de pago como tarjetas de crédito, y en su lugar solicita criptomonedas, probablemente no sea un sitio seguro. Las tarjetas de crédito no solo permiten que los compradores puedan hacer un seguimiento de sus compras, sino que, sobre todo, les dará la posibilidad de rechazar un cargo indebido, de modo que podrán recuperar su dinero si tuvieran algún problema. 5. Las aplicaciones no son inmunes Si bien las tiendas de aplicaciones oficiales como Google Play y App Store de Apple realizan comprobaciones de seguridad antes de permitir que ingrese una aplicación en sus tiendas, sigue siendo importante estar atentos a la posibilidad de que sean falsas. Recientemente, Avast informó sobre aplicaciones falsas en Google Play Store que utilizaban logos y nombres de desarrolladores muy parecidos a ciertas aplicaciones populares, para engañar a las personas y lograr que las descargaran. En la mayoría de los casos, las aplicaciones falsas están diseñadas para robar datos personales, pero algunas van un paso más allá e interceptan los SMS para captar los códigos de autenticación de dos factores. Los compradores siempre deberían asegurarse de descargar aplicaciones legítimas, solo buscando en el sitio web de la tienda y descargando desde allí la aplicación. Hay que estar más alerta durante la época navideñaAvast ve como los ciberdelincuentes envían ofertas “especiales” todo el tiempo, pero durante esta temporada los compradores pueden ser especialmente vulnerables. Por ello, Avast recomienda que se utilicen herramientas de seguridad y se preste atención a los detalles al hacer compras en línea. Acerca de AvastAvast (www.avast.com), líder global en productos de seguridad digital, protege a más de 400 millones de personas online. Avast ofrece productos bajo las marcas Avast y AVG que protegen a las personas de las amenazas en internet y del escenario de amenazas de Internet de las Cosas en constante evolución. La red de detección de amenazas de la compañía se encuentra entre las más avanzadas en el mundo, utilizando tecnologías de aprendizaje automático e inteligencia artificial para detectar y detener amenazas en tiempo real. Los productos de seguridad digital de Avast para Móvil, PC o Mac están mejor clasificados y certificados por V-100, AV-Comparatives, AV-Test, OPSWAT, ICSA Labs, West Coast Labs, entre otros. Avast cuenta con el respaldo de las principales firmas globales de capital privado CVC Capital Partners y Summit Partners.

**Datos de contacto:**

Flor Carreno

56152196

Nota de prensa publicada en: [https://www.mexicopress.com.mx/5-consejos-de-avast-para-evitar-ofertas-falsas](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Software Ciberseguridad



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