¿Cómo comprar en el Buen Fin sin ser víctima de la ciberdelincuencia?

CIUDAD DE MÉXICO. 03 de noviembre de 2020.- El comercio electrónico en México ha tenido un repunte importante este año. De acuerdo con la Asociación Mexicana de Ventas Online (AMVO), 5 de cada 10 internautas mexicanos compró al menos un producto durante el Hot Sale, que se celebró en mayo, lo que representó a más de 12.3 millones de personas. Ese volumen se prevé que se mantenga durante el Buen Fin 2020, a celebrarse del 9 al 20 de noviembre, y donde el mismo organismo prevé que el 41% de los clientes harán sus compras totalmente en línea.

Ese alto nivel de operaciones y compras mediante canales digitales también incrementa el riesgo de ser víctima de un ciberataque, lo puede poner en riesgo los datos bancarios, personales, y desde luego el dinero de los clientes. Los cibercriminales aprovechan que en este tipo de temporadas de ofertas el flujo de usuarios a los sitios de los comercios es muy alto. Según la AMVO, las visitas a este tipo de portales se incrementaron 99% a mediados de este año, en comparación con 2019.

Con ese número de personas en línea, los criminales propagan ransomware y ataques de Denegación de Servicios (DDoS) a los comercios electrónicos. Además, aprovechan el alto número de promociones publicadas en redes sociales o que se envían por mensajes SMS, WhatsApp y correos electrónicos, para lanzar campañas de *phishing* o *smishing.*

Sophos, empresa líder en ciberseguridad de última generación, asegura que pese a lo anterior, los usuarios deben tener cuidado con este tipo de amenazas siempre, ya que sin importar si es Buen Fin, Hot Sale, Cyber Monday o Navidad, los cibercriminales nunca descansan. Ante el inminente riesgo que representan estos eventos, te recomienda las siguientes buenas prácticas para comprar en las próximas temporadas de descuentos sin perder tu dinero en manos de entes maliciosos:

1. Utiliza filtros web

Los filtros web son soluciones que impiden al usuario navegar por sitios que son utilizados para realizar estafas y fraudes, ya sea mediante tácticas como el *phishing* o la propagación de ransomware. También conocidos como 'software de control de contenido', este tipo de programas pueden configurarse para permitir únicamente el acceso a una lista de sitios elegidos por el proveedor de la solución. Pueden configurarse para restringir la navegación en sitios no deseados luego de un análisis de la URL y de búsquedas en el contenido de un portal web en busca de palabras clave, lo que hace que el programa decida si bloquear o permitir la conexión.

Sophos recomienda también hacer una verificación de la URL en la que navegas y asegurarte de que contenga al inicio el protocolo de encriptación de datos https:// que asegura que el intercambio de información entre el usuario y el sitio, como pueden ser datos bancarios, se encuentra encriptado.

2. Cuidado con las ofertas más sorprendentes

Si parece demasiado bueno para ser verdad, ojo… deberías pensarlo dos veces. En ocasiones, las estafas comienzan con la publicación de un descuento descabellado que atrae a la víctima y la invita a hacer clic en un sitio malicioso. Recuerda que este tipo de estafas suplantan la identidad de marcas reconocidas e incluso redireccionan al usuario a sitios muy similares a los legítimos, lo que los hace parecer confiables y suelen engañar a las personas.

3. Evita las redes públicas

Debes cuidar en dónde y cómo es que te conectas a internet para comprar. En ocasiones, los ciberdelincuentes lanzan redes wifi gratuitas y públicas que simulan ser las de establecimientos como cafeterías o espacios públicos con la intención de que, cuando se conecta el usuario, pueda acceder a sus dispositivos y extraer la información que desean. Si no estás convencido de que la red es segura, es mejor conectarte en casa o utilizar tus datos móviles para conectarte.

4. Vigila tus movimientos bancarios en todo momento

Revisar la aplicación de tu banco, los movimientos y las operaciones es crucial para mantener un control y detectar si fuiste víctima de una estafa. Eliminar por completo toda amenaza de estafa es casi imposible, pero qué mejor que detectarlo a tiempo para actuar si encuentras movimientos fuera de lo normal. Es importante que con cada compra, revises los movimientos de tus cuentas en tu banca en línea y te asegures de que no existen operaciones que no reconoces.

5. No te presiones

Los ciberdelincuentes suelen jugar con la presión del tiempo que muestran algunas ofertas en línea. Esa estrategia también es usada por empresas legítimas para generar un impulso de compra en el consumidor, pero suele ser muy peligroso ya que puede prestarse a caer en trampas de *phishing* por error. Además, la presión puede generar *typosquatting*, término que se refiere a una técnica que aprovecha los errores tipográficos que los usuarios cometen por las prisas al escribir, especialmente en *smartphones*, para redirigirlos a páginas web y dominios previamente registrados que simulan ser legítimos y que pueden infectarlos.

# # #

Sobre Sophos

Como líder mundial en seguridad cibernética de última generación, Sophos protege a más de 400,000 organizaciones en más de 150 países de las amenazas cibernéticas más avanzadas de la actualidad. Desarrolladas por SophosLabs, un equipo global de inteligencia contra amenazas cibernética y ciencia de datos, las soluciones basadas en inteligencia artificial y nativas de la nube de Sophos ofrecen seguridad a endpoints (computadoras portátiles, servidores y dispositivos móviles) y redes contra las diversas técnicas de ciberdelincuencia que están en constante evolución, incluidos ransomware, malware, exploits, extracción de datos, incumplimientos de adversarios activos, phishing y más. Sophos Central, una plataforma de administración nativa de la nube, integra toda la cartera de productos de próxima generación de Sophos, incluida la solución de endpoint Intercept X y el Firewall XG, en un único sistema de "seguridad sincronizada" accesible a través de un conjunto de APIs.

Sophos ha impulsado la transición a la ciberseguridad de última generación, aprovechando las capacidades avanzadas en la nube, el aprendizaje automático, las API, la automatización, la respuesta ante amenazas y más, para brindar protección de nivel empresarial a organizaciones de cualquier tamaño. Sophos vende sus productos y servicios exclusivamente a través de un canal global de más de 53,000 socios y proveedores de servicios administrados (MSP). Sophos también pone a disposición de los consumidores sus innovadoras tecnologías comerciales a través de Sophos Home. La compañía tiene su sede en Oxford, Reino Unido. Para obtener más información visita www.sophos.com.

Síguenos en:

Facebook: https://www.facebook.com/SophosLatam/
Twitter: https://twitter.com/SophosLatAm
LinkedIn: https://www.linkedin.com/company/sophos/