Hot Sale 2023: ¿cómo evitar un fraude electrónico al comprar en este evento?

CIUDAD DE MÉXICO. 29 de mayo de 2023.- Más de 12 millones de mexicanos quieren comprar en el Hot Sale 2023, que se llevará a cabo durante los últimos días de mayo y los primeros de junio en México.

Aunque sin duda es una excelente oportunidad para los consumidores de encontrar descuentos atractivos y productos a precios bajos, también deben saber que el riesgo de ser víctima de fraude electrónico en dicha temporalidad se incrementa.

Esto se debe a que los cibercriminales aprovechan este tipo de temporalidades, en las que hay demasiados compradores conectados, para engañar y propagar amenazas en busca de robar la información de los usuarios, suplantar su identidad, acceder a sus datos bancarios, o simplemente realizar ventas desde sitios apócrifos, entre las amenazas más comunes.

Lo anterior implica un riesgo importante tanto para comercios como para sus compradores. De hecho un estudio de Juniper Research señala que las pérdidas para los consumidores a nivel global este año podrían alcanzar hasta USD $48 mil millones de dólares, debido a los fraudes en el *e-commerce*.

Por eso, desde la perspectiva de Strike, estos son los cinco principales consejos que los consumidores deben seguir en este Hot Sale para no caer en las manos de los cibercriminales:

1. Verifica la autenticidad del sitio web: Antes de realizar cualquier compra en línea durante el Hot Sale, es importante asegurarse de que el sitio web sea legítimo y seguro. Verificar la URL para asegurarse de que comience con "https://" es un paso básico a seguir, además de verificar que haya un candado en la barra de direcciones. Estos son indicadores de que la conexión es segura y que la información que se intercambia estará encriptada.

2. Habilita la autenticación de dos factores (2FA): La autenticación de dos factores proporciona una capa adicional de seguridad al requerir un segundo método de verificación, como un código enviado a tu teléfono móvil o incluso el acceso mediante datos biométricos, además de tu contraseña.

Activar esta función siempre que se disponga a comprar en las plataformas de comercio electrónico durante el Hot Sale es fundamental. Esto dificulta que los *hackers* accedan a las cuentas de los usuarios, incluso si obtienen la contraseña.

3. Mantén tus dispositivos actualizados: Los usuarios deben asegurarse de mantener sus dispositivos, como la computadora y el teléfono móvil, actualizados con los últimos parches y actualizaciones de seguridad.

Las actualizaciones suelen contener correcciones de seguridad importantes que ayudan a protegerte contra vulnerabilidades conocidas. En el caso de los comercios, esas correcciones se realizan luego de un proceso de *pentesting*, en el cual el *hacker* ético detecta las vulnerabilidades del sistema.

4. Cuidado con los correos electrónicos y mensajes sospechosos: Durante el Hot Sale, es común que los ciberdelincuentes envíen correos electrónicos y mensajes de texto fraudulentos para engañar y robar tu información personal. Esos correos electrónicos suelen tener ofertas muy atractivas y poco creíbles, que son el principal factor para sospechar. Toda vez que el usuario cae, es redirigido a sitios apócrifos en donde se les solicitan datos para hacer mal uso, o simplemente se les realiza una venta fraudulenta. Como recomendación, los usuarios deben tener cuidado con los enlaces o archivos adjuntos desconocidos y no proporcionar información confidencial en respuesta a solicitudes no solicitadas.

5. Utiliza tarjetas virtuales o servicios de pagos seguros: Hoy en día las tarjetas digitales son una excelente opción para no comprometer los dígitos del plástico físico, así como otros servicios como PayPal, para realizar transacciones.

Estos servicios actúan como intermediarios entre la información financiera del usuario y el comercio, lo que significa que los compradores no deben proporcionar directamente sus datos de pago a cada tienda en línea. Además, las tarjetas virtuales suelen tener características de seguridad adicionales, como la capacidad de generar códigos dinámicos de seguridad, que son de un solo uso.

“Es importante concientizar a los usuarios sobre el riesgo que representan las temporalidades como el Hot Sale. Si bien es un excelente momento para comprar, también representa una posibilidad muy amplia de ser vulnerado si no se cuentan con las medidas necesarias para proteger sus compras. Estar atentos a amenazas como el “phishing” y el robo de información, que preocupan al 60% a nivel global, es imperativo cuando se quieren realizar compras exitosas y a precios bajos”, concluye Santiago Rosenblatt, CEO y fundador de Strike.

Sobre Strike

Strike es la plataforma de ciberseguridad en Latinoamérica. Su principal misión es ayudar a que las compañías estén protegidas a través de la detección y resolución de vulnerabilidades en sus sistemas. Esto se realiza a través de tests de penetración - o pentests - llevados a cabo por su red global de hackers éticos, conocidos como “Strikers”, una comunidad global que reúne a los mejores expertos de ciberseguridad con reconocimientos y certificaciones internacionales. Su objetivo es impulsar una cultura de ciberseguridad de calidad y accesible, en la que la misma sea parte del ciclo de vida de las empresas y no algo estanco o independiente. Más información en: https://strike.sh/

Síguenos en nuestras redes sociales:
Instagram - @strikesecurity
Twitter - @strike_secure
LinkedIn - Strike

Contacto para prensa México
another
Ahtziri Rangel | PR Expert
+ 52 1 55 1395 6970
ahtziri.rangel@another.co