



## Retail, más vulnerable que nunca en el Buen Fin y cierre de año

CIUDAD DE MÉXICO. XX de octubre de 2022.- Los volúmenes de venta para los *retailers*, tanto físicos como *online*, se incrementan de forma exponencial durante el Buen Fin y el resto del último trimestre del año.

Para muestra, el hecho de que **6 de cada 10 mexicanos** decidieron comprar al menos un producto en el Buen Fin del año pasado, debido a las atractivas ofertas y descuentos que se presentaron en ese evento, según la [Asociación Mexicana de Ventas Online](#).

Pero desde luego ese incremento sustancial en las ventas implica un crecimiento inusual en el tráfico de los sitios de comercio electrónico, lo cual a su vez se traduce en mayor riesgo para las empresas de ser afectadas por cibercriminales.

Es decir, las altas ventas significan, para los *hackers*, a millones de personas escribiendo sus datos bancarios, navegando por distintos sitios web, y gastando dinero en línea: una 'mina de oro' sumamente atractiva.

De por sí el *retail* ya es un sector sumamente vulnerable en el que [el 77% de las organizaciones del mundo](#) fueron afectadas el año pasado; pero en esta época del año, es una realidad que el riesgo crece.

*“Desde la perspectiva de [Strike](#), es importante que antes de estas temporalidades de ventas online al por mayor, las empresas comiencen a anticiparse al pensamiento de los cibercriminales y empleen técnicas como el hacking ético para detectar y corregir aquellas vulnerabilidades que, de no ser detectadas oportunamente, podrían ser explotadas por entes maliciosos”,* considera Santiago Rosenblatt, CEO y Fundador de [Strike](#).

- ¿Cómo deben prevenirse los retailers?

Santiago Rosseblatt, ante el riesgo antes descrito, recomienda hacer uso del *pentesting*. Se trata de pruebas de penetración de los sistemas internos de las empresas del *retail* por un *hacker ético*, quien como experto en ciberseguridad encuentra vulnerabilidades que un *hacker malicioso* puede aprovechar para propagar un ataque o realizar un secuestro de datos.

De ese modo, a medida que avanza el proceso el Striker, como se le conoce al hacker ético, va confeccionando a la compañía un reporte en el que detalla todas las vulnerabilidades, la forma de resolverlas y las recomendaciones pertinentes, así como el diagnóstico de la empresa y el impacto que un ataque puede tener.



En cuanto a este último aspecto, es importante mencionar que para el *retail* existe un costo muy alto en materia de ciberataques. Se estima que el año pasado el *ransomware* le costó a las empresas más de USD \$20,000 millones, según [Cibersecurity Ventures](#).

- Más consejos de protección anti-cibercrimen

**1. Autenticación digital:** Las contraseñas quedaron en el pasado, ya que estas pueden ser fácilmente robadas por ciberdelincuentes. Lo más adecuado, hoy en día, es hacer uso de autenticación mediante biométricos como la huella digital y el reconocimiento facial del usuario, para evitar que entes maliciosos comprometan las operaciones de los usuarios.

**2. Aprovechar los datos del usuario:** además de personalizar la experiencia de compra, los comercios pueden utilizar los datos de los consumidores para crear perfiles más exactos en materia de riesgo y detectar de forma más fácil a los compradores falsos que en realidad quieren realizar fraudes y comprometer información del negocio.

**3. Verificación de plataformas:** tanto las tiendas *online* como sus redes sociales, y otros métodos de contacto, deben estar previamente verificados para generar mayor confianza al usuario. De no hacerlo, es probable que los cibercriminales puedan crear sitios web apócrifos muy similares al original de la empresa y comenzar a lanzar ataques mediante phishing hacia los consumidores.

### **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](mailto:ahtziri.rangel@another.co)