

¿De qué tamaño es el problema del fraude digital?

CIUDAD DE MÉXICO. XX de septiembre de 2023.- El fraude en el comercio electrónico es un problema común y latente. Todos los comercios, sin excepción, están en riesgo y son potenciales víctimas de cibercriminales que cada día se vuelven más sofisticados en sus métodos de ataque.

El problema es enorme. Datos de [Sophos](#) indican que el 69% de las empresas de retail fueron víctimas de ciberataques a nivel global en la primera mitad de 2023. Específicamente en México la [Condusef](#) señala que en un periodo de seis meses se reportan 3.5 millones de reclamaciones por posibles fraudes, lo que representa un monto de \$9,213 millones de pesos en pérdidas.

[Signifyd](#), partner de BigCommerce, señala que por cada USD \$100 en fraude, se derivan USD \$207 más en costos que vienen como consecuencia. Esto debido a que más allá del valor de la mercancía, existen costos operativos como el procesamiento del pedido, la gestión de la cadena de suministro, así como el costo por la ejecución de la venta y las tarifas por devolución.

Por ello, y sumado a lo anterior, un estudio de [Juniper Research](#) señala que las pérdidas para los comercios a nivel global durante 2023 podrían alcanzar hasta USD \$48 mil millones de dólares, debido a los fraudes en el e-commerce.

- ¿Qué tipos de fraude existen?

Fraude de tarjeta bancaria: se presenta cuando un estafador logra comprometer la información bancaria de un usuario y la utiliza para realizar compras y/o pagar servicios a nombre de la persona vulnerada.

Fraude de afiliación: los comercios cuentan con programas de afiliados en los que recompensan, con una comisión, a los usuarios que refieren a otros compradores. Dicho lo anterior, existen defraudadores que se inscriben a dichos programas y envían tráfico basura al sitio del comerciante utilizando bots para activar esas recompensas, lo cual consiste en un engaño al sistema.

Contracargos: este tipo de fraudes se presentan cuando el comprador solicita un reembolso de la compra, incluso aunque ya recibió los bienes o servicios comprados. En este tipo de casos, es el comercio el responsable de reembolsar al banco emisor de la tarjeta bancaria el monto que previamente la devolvió al usuario.

Phishing: es una de las técnicas más comunes de fraude al e-commerce con [17% de los casos](#). Consiste en el envío de correos electrónicos infectados con links maliciosos, mediante

los cuales engañan a los clientes para que revelen datos como su nombre de usuario y contraseña, para luego iniciar sesión y realizar compras no autorizadas.

- Las industrias más vulneradas

De acuerdo con datos recopilados por [BigCommerce](#), la industria de Artículos Coleccionables fue la más vulnerada el año pasado con un aumento de 106% anual. En segundo lugar, el sector de Artículos de Lujo con un crecimiento de 104% en la incidencia de fraude, seguido por Ocio y Entretenimiento con un aumento del 42%.

Si bien estas verticales muestran incrementos significativos en materia de fraude, eso no quiere decir que otras estén exentas. Por el contrario, el problema del fraude afecta a todos los sectores y cualquier compañía debe tener en cuenta la posibilidad de convertirse en una víctima.

- ¿Cómo atender el problema?

Es importante que los comercios cuenten con un proveedor de e-commerce que tenga, a su vez, aliados estratégicos que brinden herramientas de prevención de fraude basadas en Big data, aprendizaje automático e inteligencia artificial para distinguir entre operaciones apócrifas y legítimas.

Ese proveedor debe utilizar la data histórica, tanto de dicho comercio como de otros clientes, para entender el comportamiento de los clientes legítimos y fraudulentos y generar patrones más precisos que permitan detectar el fraude de forma anticipada, en lugar de hacerlo ya que se presentaron las vulneraciones.

Comprender ese comportamiento permite brindar a los comercios y marcas un margen de maniobra más amplio en puntos clave de su procesos de ventas, lo que es clave para evitar que el índice de fraude siga incrementándose.

En conclusión, el fraude en el comercio electrónico es un fenómeno habitual en 2023 y no va a disminuir. Desde el phishing y la apropiación de cuentas hasta el fraude con tarjetas de crédito, los actores maliciosos pueden emplear diversas técnicas para estafar a los comerciantes. Es imperativo que los comerciantes se mantengan en guardia mientras las tecnologías siguen evolucionando. Acudir a aliados tecnológicos que promuevan una infraestructura de comercio electrónico que incluya socios especializados sobre el terreno, se convierte en algo esencial para proteger tanto las operaciones internas como a los clientes de las empresas.