¿Cuáles son las formas comunes en las que operan las entidades fraudulentas?

CIUDAD DE MÉXICO. 17 de septiembre de 2020.- El fraude en comercio electrónico actualmente es un problema común y un riesgo latente, tanto para comercios como para compradores, que adquieren a diario miles de productos online.

En México, tan solo en la primera mitad del 2019 se presentaron 5.4 millones de reclamaciones contra la banca por fraude ante la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef), esto representa un incremento de 21% con respecto al año anterior, siendo el comercio electrónico el canal de 55 de cada 100 casos de este tipo. Cabe destacar también que, de acuerdo con un informe de Merchant Risk Council, las empresas online rechazan en la actualidad el 2.5% de todos los intentos de sospecha de fraude.

Dicho lo anterior, es importante saber que los fraudes electrónicos evolucionan de forma constante, por lo que como empresa debes estar seguro de contar con herramientas tecnológicas que ayuden a mitigar el riesgo ante los defraudadores. **Erick MacKinney, Country Manager de Adyen México**, explica que en la actualidad el fraude se realiza de manera sistemática, por lo que los comercios requieren de soluciones que les ayuden a combatirlo de manera masiva y no mediante revisiones caso tras caso, como se realizaba en el pasado.

Algunas de las modalidades más comunes para cometer fraude electrónico en la actualidad:

‘Clonación’ sistemática a través de generación aleatoria de números de tarjeta

El especialista de Adyen explica que actualmente los delincuentes cibernéticos utilizan *BINes* para obtener números de tarjeta bancaria válidos mediante un algoritmo. Un BIN o *Bank Identification Number* son los primeros 4 a 6 dígitos de cualquier tarjeta bancaria. Para obtener un número de tarjeta válido a partir de un BIN se puede utilizar un algoritmo simple disponible en internet para generar los números restantes de la tarjeta.

MacKinney explica que todas las tarjetas bancarias tienen un BIN asociado que de manera tradicional está impreso en relieve con el resto de los números de la tarjeta o PAN o Primary Account Number. Cuando se conocen esos 4 a 6 primeros dígitos, se tiene acceso a toda la información sobre una tarjeta bancaria, desde el nombre del banco emisor, el tipo de tarjeta (crédito o débito), el país en el que fue emitida, entre otros.

Con esos 4 a 6 primeros dígitos legibles en cualquier tarjeta circulando en el mercado, el defraudador utilizará un algoritmo para adivinar los dígitos restantes pero para hacerlo no

estará una sola persona detrás de su computadora haciendo un intento a la vez, sino que se utilizan granjas de servidores que harán miles de pruebas consecutivas con distintas combinaciones hasta conseguir un número válido. Posteriormente sólo requieren obtener una fecha de expiración y un código de seguridad de 3 dígitos, lo que no significa un gran reto para quienes cuentan con tecnología de vanguardia para perpetrar este tipo de operaciones fraudulentas.

"Este es un juego de tecnología. Muchas veces pensamos al defraudador como una sola persona detrás de una computadora, pero no. Esto es fraude sistemático: existen granjas de servidores patrocinadas por cibercriminales que están intentando comprar y comprar y comprar en línea. Es por eso que no se puede combatir el fraude únicamente con revisiones manuales o con llamadas a los clientes validando datos. Requieres utilizar toda la tecnología disponible porque del otro lado está alguien con todas esas herramientas", indicó Erick McKinney.

Phishing: la técnica de engaño 'por excelencia'

Quizá hablamos de la forma más utilizada en la actualidad para estafar y defraudar a las personas, siendo el correo electrónico la principal herramienta para perpetrar este tipo de engaños.

Los ciberdelincuentes envían correos electrónicos o mensajes apócrifos que suplantan la identidad de una empresa o institución bancaria, acompañado de un enlace a un sitio falso, muy similar a uno oficial, en donde se le solicitarán datos sobre sus tarjetas bancarias y personales.

El phishing puede tener distintos objetivos, desde instalar malware e infiltrarse en sistemas, hasta robar dinero a la gente gracias a la información obtenida e incluso solicitarlo mediante donaciones falsas o venta de productos inexistentes.

En México, todas las instituciones financieras identificaron algún evento que atentó contra la seguridad de la entidad y de sus clientes en 2018, de acuerdo con el 'Estudio de la ciberseguridad en el sistema financiero mexicano' elaborado por la Organización de Estados Americanos (OEA) y la Comisión Nacional Bancaria y de valores (CNBV). El informe indica que el 43% de esos ataques fueron exitosos, siendo malware (56%) y phishing (47%) los más comunes.

Adyen recomienda a los compradores nunca hacer clic en enlaces de correos electrónicos que soliciten información personal y datos bancarios, pese a que sean correos membretados correctamente por alguna institución financiera. Cuando se trata de comprar en línea, es importante comprobar que la dirección de la página web en la que harás la transacción comience con 'https://', que significa que el sitio cuenta con un protocolo de encriptación para la transferencia de datos entre comercio y usuario.

# # #

Acerca de Adyen
Adyen (AMS: ADYEN) es la plataforma de pagos preferida por las compañías de mayor crecimiento alrededor del mundo, ofrece una moderna infraestructura de punta a punta que elimina fronteras y entrega la mejor experiencia de compra para los consumidores, sin importar el lugar o momento tiempo. Adyen integra los servicios de entrada , software anti fraude y adquirente, abriendo así la "caja negra" con los insights que las empresas necesitan para alcanzar una mayor tasa de conversión.

Con oficinas alrededor del mundo Adyen cuenta con clientes como Uber, eBay, Spotify y Cabify, entre otras, impactando a millones de consumidores a lo largo del mundo.

Síguenos:
Facebook: https://www.facebook.com/AdyenPayments/
Twitter: https://twitter.com/Adyen
LinkedIn: https://www.linkedin.com/company/adyen/

Contacto para prensa:
Another Company
Salvador Sánchez/ Ejecutivo de cuenta
Cel: (+52 1) 55 4582 7151
salvador.sanchez@another.co