

Las 5 grandes tendencias del fraude en 2024 | #Tech



La utilización de la inteligencia artificial (IA) ya es una realidad en varios sectores, desde la agricultura hasta el transporte.

Particularmente en el mercado financiero, las aplicaciones relacionadas a esta tecnología han transformado y seguirán transformando la oferta de bienes y servicios en todo el mundo. Actualmente, el uso responsable y ético de la IA es el foco de discusión de los grandes y poderosos grupos en todo el mundo. Pero más allá de eso y de la regulación también es importante prestar atención al uso indebido de la IA para difundir información errónea, invadir la privacidad de las personas y cometer fraudes.

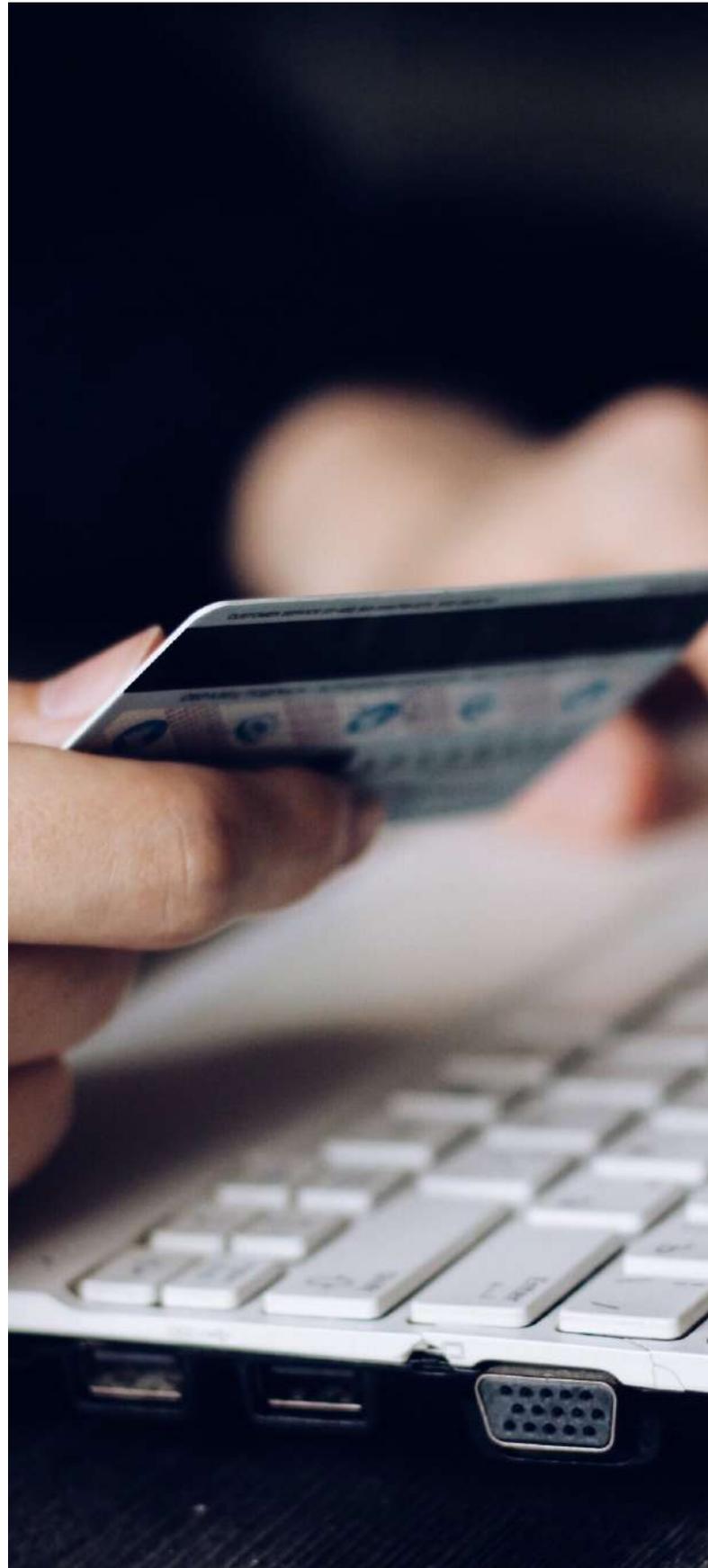
En este 2024, identifico cinco grandes “puntos ciegos”, todos ellos ya reconocidos y estudiados cuidadosamente en otras ocasiones, pero que siguen llamando la atención sobre el astuto desarrollo de los estafadores para crear estrategias evasivas que confunden o bloquean los sistemas activos antifraude.



El phishing sigue siendo una amenaza común y, con la evolución de la IA generativa, la creación de correos electrónicos o mensajes falsos tiende a volverse más convincentes. Es en este contexto que los usuarios deben estar cada vez más atentos a los mensajes recibidos por correo electrónico, SMS, WhatsApp, contactos en las redes sociales o llamadas telefónicas, especialmente si estos contactos van acompañados del envío de enlaces para acceder a los detalles de la comunicación y así recopilar datos e información para cometer fraudes.

La práctica del consumidor de comprar en línea tiende a ser cada vez más significativa, según la Asociación Mexicana de Venta Online (AMVO), México está avanzando velozmente en cuestión de desarrollo y consumo en el sector de comercio electrónico y se tiene una proyección para el país de alcanzar un crecimiento del 11% de 2021 al 2025. **El consumo digital es una puerta de entrada para los estafadores. Es necesario prestar atención y tener cuidado al proporcionar información personal y de pago para evitar que el robo de identidad y fraudes en los medios de pago.**

Hablando de identidad robada, el fraude de esta naturaleza es una preocupación creciente. Con los avances del machine learning y el uso cada vez mayor de aplicaciones de inteligencia artificial, han surgido los «deepfakes» (videos o grabaciones de audio falsos que se ven y suenan exactamente como los reales).



Estos fraudes combinados con el fraude online se han convertido en una herramienta muy utilizada por los estafadores mediante el uso de datos personales o incluso la creación de identidades falsas.

También irá en aumento el uso de la ingeniería social, o manipular a las personas con alguna información veraz para inducirlos a realizar alguna actividad. Por lo tanto, es necesario poner mucha atención al momento de proporcionar datos, hacer transferencias, reenviar mensajes y acceder a enlaces. **Por lo general, los delincuentes utilizan esta información para realizar estafas financieras.** Es importante tener cuidado con las promesas de inversión que dicen tener poco o ningún riesgo y ofrecen márgenes de rendimiento muy por encima de lo que brinda el mercado. También se debe estar alerta ante mensajes de supuestas gratificaciones, sorteos o pagos de cuentas, transacciones inesperadas y/o transferencias de recursos urgentes (emergencias).

Por último, se debe poner atención a las filtraciones de datos. **Además de los datos personales, otros datos están en la mira de los estafadores, como los de los dispositivos que se encuentran conectados a Internet, desde teléfonos móviles y computadoras, hasta electrodomésticos, vehículos y hogares.** Los estafadores ahora también 'secuestran' estos dispositivos y datos, y para liberarlos piden el pago de un rescate, provocando interrupciones, pérdidas financieras o incluso la pérdida permanente de datos valiosos.



En el mundo del fraude una cosa es segura, **por cada solución creada, surge una nueva estafa.** En este sentido, la IA es un motor importante para recalcular rutas, comprender patrones o sus desviaciones. Con la ayuda de la ciencia y las matemáticas es posible integrar redes neuronales y predecir escenarios posibles y certeros.

Fuente de información: geekandlife.com.mx