# Nueva cuenta de fraude

Uno de los fraudes más prevalentes que tuvo lugar en el espacio digital ahora es una nueva cuenta de fraude, también referido a cuentas sintéticas. Puede ocurrirle a cualquiera. Todo lo que los estafadores requieren es un poco de información – nombre, fecha de nacimiento y número de seguro social- y con esto pueden fabricar una nueva cuenta en tu nombre.

Ningún tipo de cuenta es inmune, tarjetas de crédito, de débito, aplicaciones de préstamo, incluso aplicación para préstamo estudiantil puede ser suficiente para un estafador competente para crear una identidad sintética. Un buen timador puede tener numerosas de estas identidades sintéticas activas al mismo tiempo. Se gana la confianza basando el crédito en cuentas realmente pagadas. Cuando es obtenido el máximo disponible de crédito y todos los préstamos están en orden, el estafador sobrepasará el límite de las tarjetas de crédito, tomará el dinero y desparecerá. Dado que la persona en realidad nunca existió, no hay muchas pistas para investigar al protagonista.

Si la información es el nuevo oro entonces debemos empezar a hablar sobre las consecuencias de explotarlo. En la prisa de convertir los datos en dinero no hablamos sobre vulnerabilidades de los mismos tanto como deberíamos. En un mundo donde más y más personas viven en línea, sin pruebas biométricas que los definan – apariencia, voz, personalidad – la información es todo lo que se requiere para crear identidades sintéticas. Es como el antiguo oficio criminal de falsificar esteroides.

Las estadísticas colocan al número de cuentas sintéticas en 1.5 millones de casos por año o más desde 2019, con pérdidas en promedio de más de 20 billones por año. Así como los estafadores se hacen más competentes se hace más competente también la seguridad. Sumado al problema tenemos el cambio radical en compras en línea que se ha venido dando desde 2019.

Hay un número de factores en juego, uno de ellos y no en menor medida fue la pandemia y las ordenes de permanecer en casa, posterior a esto una confianza general de las compras online ha emergido en los últimos años. Como en todas las cosas nuevas, valentía y atrevimiento, carga la primera y la vieja guardia, espera hasta que todo parezca legítimo para ponerlo en práctica. Piensa en la criptomoneda. Hay abuelos comprando en línea ahora mismo, incluso si no obtienen pronto un Bitcoin.

La seguridad es tanto responsabilidad del comprador, como del vendedor. Como dueño del rango de crédito debes mantenerlo por encima de lo estimado. Mantener la cuenta vigilada, asegurarse de comprender todo lo relacionado a la cuenta y poder contabilizar todas las transacciones. Nunca compartir información personal en redes sociales ni a través de redes públicas de Wi-fi. Las contraseñas seguras son importantes, así como el paso dos de autenticación si el vendedor así lo sugiere.

De acuerdo a un reporte de Fraude y Pagos de Comercio Electrónico Global (2023) preparado por el Consejo de Riesgo Mercantil (MRC), Cybersource y Verifi, los comerciantes están utilizando gran diversidad de herramientas de detección de fraude. Con más de la mitad en tarjetas de crédito y servicios de verificación de identidad. Pequeños proyectos se vuelven más grandes. Los bancos más pequeños usan menos herramientas colocándolos en una posición más vulnerable. Conforme emerge la tecnología las instituciones financieras más grandes son las primeras en adoptar – indicadores biométricos, modelos de marcas individualizadas de fraude, modelos de velocidad multi-mercantiles de compra- y las instituciones más pequeñas podrían ser forzadas a salir del negocio o a encontrar soluciones para el incremento de problemas de seguridad y la necesidad de tecnología. Esta es la realidad del panorama emergente de la información repleto de inherentes vulnerabilidades.

Lo mejor en tecnología de clase para prevenir cuentas sintéticas está emergiendo de comunidades de inteligencia artificial (AI) y aprendizaje autónomo (ML). La Al conduce un sistema de identidad de detección de robos operando a niveles de reconocimiento de patrones hasta ahora desconocido para la seguridad digital capaces de detectar anomalías tempranas, antes que el culpable penetre al servidor o a información sensible. Tras permitir al ML estudiar una transacción de un cliente del banco emerge un patrón de comportamiento. Este patrón es mucho más complejo de lo que cualquier observación humana y conjunto de datos puedan lograr. Esto previene los fraudes de tarjetas de crédito antes de que ocurran o finaliza el uso del instrumento de crédito al momento en que una anomalía logra ser detectada. Las anomalías no son fuentes aisladas. Son la suma de un número de diferentes fuentes, localización, artículo, momento del día y mucho más. El ML es capaz de agregar todos estos patrones a un perfil de exactitud infalible que detecta cuando el usuario o servicio financiero no es el verdadero.

A como crece la utilidad de datos en nuestra sociedad, también lo hace la vulnerabilidad inherente a los mismos. Sin embargo, la tecnología parece más que lista para afrontar los problemas de seguridad de comercio digital, de la banca abierta y de identidad sintética. Está siendo envuelta tan rápidamente que es solo cuestión de tiempo antes que los modelos de investigación y arresto se formen dentro del mundo digital. Basta con que el estafador cace una institución financiera dándole crédito a una cuenta falsa, pronto viviremos en un mundo donde a través de AI y ML se establecerá a estos estafadores como operaciones policiales encubiertas.