NUANCE | WHAT'S NEXT BLOG

Autenticación y Prevención del Fraude, Interacción con el cliente multicanal

Caso real: SIM Swapping y fraude online

Brett Beranek | Vice President & General Manager, Security & Biometrics

31 marzo 2021

C

A few weeks ago we were lucky enough to interview Álvaro Sanjuán, victim of a fraud scam that caused him serious personal and economic damage at the end of 2019, in our program for customers in Spain, to give visibility to a type of fraud that is increasingly common among the main telecommunications companies and financial institutions in our country. SIM Swapping. If you missed it, here are all the details.

Álvaro comienza el encuentro contando su historia. El 4 de septiembre de 2019, hablando con un amigo por teléfono, su línea se cortó. Aunque al principio no le dio mucha importancia, al salir a la calle esa misma tarde y ver que no volvía a la normalidad, empezó a preocuparse. A pesar de que los teleoperadores le aseguraron que todo estaba bien cuando llamó a su compañía telefónica para pedir explicaciones, al regresar a su casa y conectar su *smartphone* a la red WiFi, empezó su calvario. Álvaro empezó a recibir varios emails en su bandeja de entrada, notificándole una serie de transferencias bancarias por un importe de doce mil euros. Transferencias que, por supuesto, no había realizado él.

Tras el estado de shock inicial, Álvaro llamó a su banco para poner freno a este robo y evitar que su cuenta se quedase a cero. Una nueva sorpresa llegó en ese momento: sus claves bancarias no funcionaban y su entidad no tenía forma de identificarle y de comprobar que era quien decía ser. Con el uso de datos como su número de DNI o las terminaciones de sus tarjetas, el agente pudo cancelar las transferencias que los criminales habían realizado para sacar el dinero y bloqueó la cuenta de Álvaro como medida preventiva.

Aunque de forma irónica fue su salvación, que el banco accediera a su cuenta con los datos que consiguió suministrarle al teleoperador, tampoco le hacía sentir muy seguro. Al fin y al cabo, la información que Álvaro le facilitó al agente se puede obtener de forma relativamente sencilla en las dark webs.

Pese a la tranquilidad de haber bloqueado su cuenta bancaria, Álvaro empezó a relacionar el hecho de quedarse sin línea telefónica con lo ocurrido. Lo primero que le vino a la cabeza fue pensar que alguien debió llamar al teléfono de atención al cliente de su banco haciéndose pasar por él, para cambiar su contraseña y clave de acceso a través del sistema telefónico automatizado que tienen. ¿Pero cómo había

sido posible?

Acto seguido se puso en contacto con su operador de telefonía para entender por qué seguía sin línea de teléfono y confirmar su sospecha. Sin embargo, ante la imposibilidad de hablar con un agente y después de más de hora y media colgado al teléfono, consiguió bloquear su tarjeta SIM.

Un proceso largo y tedioso

Al día siguiente, con el extracto de movimientos de su banco, Álvaro pudo denunciar los acontecimientos. No obstante, y para su asombro, de camino a la comisaría su pareja le avisó de que, en una cuenta conjunta, también había desaparecido dinero, unos mil trescientos euros. En este caso, la entidad – filial del banco con el que ya había tenido problemas el día anterior – le dijo que se debía a retiradas de efectivo en cajeros con su tarjeta de crédito, una tarjeta que, según comenta, nunca había utilizado y que ni siquiera había salido de su casa.

How did they withdraw the money without the card?

Los peligros reales del SIM Swapping

Con la denuncia puesta, nuestro invitado nos cuenta que su siguiente movimiento fue ir a una oficina de su compañía telefónica para pedir explicaciones y recuperar su línea de teléfono. Para su sorpresa, le confirman que se tramitó un duplicado de su tarjeta SIM el día anterior.

Con su línea operativa de nuevo y la nueva tarjeta SIM en su móvil, Álvaro comprueba el registro de llamadas desde su línea de teléfono y confirma sus sospechas al ver varias llamadas desde su teléfono al servicio de atención al cliente de su banco. Llamadas que consigue escuchar, tras solicitar una transcripción del audio de dichas llamadas al propio banco, donde podemos escuchar perfectamente al estafador haciéndose pasar por Álvaro para cambiar las claves de acceso a su cuenta.

Biometrics to curb fraud

This whole situation could have been avoided with greater security on the part of the companies involved. Biometrics, and specifically voice biometrics, is an ideal solution for this type of fraud. If the fraudster, when he called the bank, had found that Álvaro is registered in the system, in a matter of seconds the situation would have taken a 180-degree turn, since the entity would have been able to verify that the person who was calling was not actually Álvaro Sanjuán.

Usar medidas de seguridad no biométricas o enfocar nuestros esfuerzos únicamente en el canal telefónico/IVR no será suficiente; los estafadores siempre encontrarán la manera de llegar a los agentes porque los humanos siguen siendo la vulnerabilidad más fácil de explotar.

La biometría y la IA analizan miles de características únicas de cada individuo para generar una huella única e intransferible de cada individuo, cuyos algoritmos mejoran y son más precisos con cada interacción. Esa huella siempre está encriptada y no compromete en ningún caso la privacidad del usuario, que siempre tiene pleno derecho a decidir cuándo y cómo quiere utilizar y/o eliminar su huella de los sistemas de identificación de su entidad bancaria.

Incorporar tecnología biométrica en los procesos de verificación de la identidad de los clientes garantiza la protección de los activos de los clientes, reduce el fraude y permite a las empresas trabajar de manera eficiente al predecir patrones en el comportamiento del usuario, detectar operaciones sospechosas y reducir el tiempo medio de gestión de la operativa con cliente.

Muchas gracias a todos los que habéis asistido a este episodio y, sobre todo, gracias a Álvaro Sanjuán por haber compartido su historia con nosotros para intentan concienciar de la importancia de la seguridad y la prevención del fraude.

Tags: Experiencia de cliente, Fraude SIM

About Brett Beranek

Brett Beranek es General Manager de la división de biometría y seguridad en Nuance Communications. Antes de unirse a Nuance, ha trabajado durante más de una década como responsable de desarrollo de negocio y marketing en distintas empresas de software y seguridad. Brett posee una amplia experiencia en el campo de las tecnologías biométricas, donde es importante destacar su papel como socio fundador de la startup Viion Systems, empresa de desarrollo de software de reconocimiento facial. Su conocimiento en materia de seguridad abarca una amplia variedad de tecnologías que incluyen, desde la biometría de huella dactilar, hasta tecnologías de análisis de videos para el entorno de la seguridad física y reconocimiento de matrículas. Brett es licenciado en comercio, con la especialidad de sistemas de información por la Universidad McGill y posee un máster en marketing por la Sloan School of Management de Massachusetts Institute of Technology.

View all posts by Brett Beranek