NUANCE | WHAT'S NEXT BLOG

Autenticación y Prevención del Fraude, Interacción con el cliente multicanal

El fraude por SIM swapping y la importancia de proteger a los clientes de las `telcos´

Nuance Communications

1 marzo 2022

A medida que aumenta el número de estafas por SIM swapping o suplantación de tarjetas SIM, las empresas de telecomunicaciones, las instituciones financieras y otras organizaciones deben hacer todo lo posible para proteger a sus clientes y liderar la seguridad. Todos los productos, servicios e interacciones deben tener un enfoque de seguridad multicanal.

En los últimos años, el número de casos de estafas por SIM swapping (o suplantación de la tarjeta SIM) ha ido en aumento: desde Jack Dorsey de Twitter en 2019 hasta Stefan Thomas, que perdió toda su inversión en criptomonedas mediante esta técnica. Aunque no es un nuevo tipo de fraude, ahora hay mucho más en juego que antes. La adopción acelerada de la banca móvil y las aplicaciones fintech supone que los recursos financieros de las personas podrían estar en riesgo.

Muchas organizaciones han publicado guías sobre cómo los consumidores pueden ayudar a protegerse del fraude de SIM swapping, pero el hecho es diferente. Colocar esta responsabilidad sobre los hombros de los consumidores ignora la realidad de cómo operan realmente los estafadores. Además, cuando se trata de prevenir el fraude de identidad, las empresas son las que tienen más poder, mucho más que los consumidores.

En este sentido y a medida que aumenta el número de fraudes por suplantación de las tarjetas SIM, las empresas de telecomunicaciones, las instituciones financieras y otras organizaciones deben hacer más para proteger a sus consumidores y liderar la seguridad. Todos los productos, servicios e interacciones deben tener un enfoque de seguridad multicanal.

Biometría para frenar los casos de fraude de suplantación de identidad

La seguridad no puede ser una idea tardía. Todavía existen muchos casos que ilustran cómo la seguridad queda relegada a un segundo plano respecto al diseño del producto, la interfaz y la usabilidad, cuando debería de integrarse en cada uno de los productos, en cada servicio y en cada interacción.

La buena noticia es que hay soluciones disponibles, y son cada vez más las empresas de telecomunicaciones que han empezado a adoptarlas. Las transacciones de alto riesgo deben protegerse con verificaciones adicionales, como la autorización de dos factores que aprovechan factores biométricos como la voz. Esto ayudará a evitar modificaciones no autorizadas en la cuenta de un abonado, algo que puede dar lugar a ataques mucho más dañinos contra cuentas bancarias, carteras de criptomonedas, y más.

Por ejemplo, la biometría multimodal ha ayudado a una empresa de telecomunicaciones brasileña a identificar a los defraudadores de forma más eficiente y eficaz, lo que ha contribuido a reducir sus pérdidas por fraude. Otro ejemplo es el de Deutsche Telekom, que ha adoptado la biometría de voz para crear un proceso de autenticación rápido y seguro para sus clientes, algo que también ha tenido un impacto positivo en el personal de primera línea de la empresa.

Dado que la suplantación de la tarjeta SIM y otros fraudes en los *contact center* siguen afectando a las organizaciones, las empresas de telecomunicaciones deben reconocer su responsabilidad en la prevención del fraude. Un enfoque de seguridad multicanal es un primer paso necesario para proteger a los consumidores y mitigar la exposición al riesgo. A fin y al cabo, las soluciones biométricas multimodales de prevención del fraude ayudan a las empresas de telecomunicaciones y a otras organizaciones a encontrar a los estafadores conocidos y desconocidos antes de que puedan cometer sus delitos.

Los estafadores acechan nuestro país atacando mediante la técnica de SIM swapping

Álvaro Sanjuán fue una víctima de una estafa de fraude que le ocasionó serios daños personales y económicos mediante la técnica del SIM swapping. Tanto su línea telefónica como sus claves bancarias dejaron de funcionar y su entidad no tenía forma de identificarle y de comprobar que era quien decía ser. Con la denuncia ya puesta, Álvaro acudió 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 comprobó 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 donde consigue escuchar perfectamente al estafador haciéndose pasar por Álvaro para cambiar las claves de acceso a su cuenta.

Otro caso ha sido el de la desarticulación por parte de la Policía Nacional de España de una red acusada de vaciar las cuentas bancarias de las víctimas haciéndose pasar por ellas mediante la misma técnica de SIM swapping. Enviaban mensajes maliciosos, a través de SMS y correos electrónicos, en los que se hacían pasar por una persona o empresa, como el propio banco, para conseguir información confidencial (contraseñas bancarias, números de tarjetas de crédito o copias del DNI). Con ello, simulaban una apariencia física parecida a la de la víctima, para engañar a las tiendas de telefonía para conseguir que les duplicaran las tarjetas SIM, teniendo así acceso a los mensajes de confirmación de seguridad del banco y operar en la banca “online” para vaciar sus cuentas.

Toda esta situación se podía haber evitado con una mayor seguridad por parte de las compañías implicadas. La biometría, y en concreto la biometría de voz, es una solución ideal para este tipo de fraude. 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.

Tags: Fraude, Estrategia del contact center, Fraude SIM

More Information

Protégete del fraude del SIM swapping

En Nuance queremos ayudar a las empresas a proporcionar a sus clientes experiencias seguras y sin fricciones en todos los canales. En este episodio escucharéis la historia de una víctima de fraude a la que vaciaron sus cuentas bancarias en menos de 24 horas siendo cliente de una de las top 3 telcos y bancos de España.

Learn more