What's next

Empresa

La lucha contra el fraude

Robert Ross, inversor en tecnología, padre de familia y ahora ferviente defensor de la lucha contra el fraude relacionado con el SIM swapping tras haber perdido casi 1 millón de euros en menos de una hora. Puedes escuchar su historia en esta entrevista con Brett Beranek de Nuance.

Brett Beranek
Posted 18 noviembre 2020

Recientemente he tenido el privilegio de sentarme con un invitado muy especial, Robert Ross, inversor tecnológico, padre y ahora ferviente defensor de la prevención del fraude por duplicado de tarjeta SIM, o *SIM swapping*, tras haber perdido casi 900.000 euros en menos de 1 hora.

El objetivo de nuestra conversación era que Rob tuviera la oportunidad de compartir cómo se produjo el ataque, cómo le ha afectado a él y a su familia, y qué ha aprendido de toda esta experiencia para ayudar a educar tanto a empresas como a consumidores.

Sucedió muy deprisa

Un viernes por la noche de finales de 2016, Rob estaba en casa y recibió una notificación de su banco por una solicitud de retirada de efectivo. En aquel momento, coincidió que tenía delante el móvil y el ordenador portátil, por eso pudo ver en tiempo real cómo se cerraba la sesión de su correo electrónico y que no tenía servicio de red en su *smartphone*. Inmediatamente supo que algo iba mal, aunque todavía no era consciente de las inminentes implicaciones que aquello tendría.

Nada más darse cuenta de todo esto, Rob se dirigió a su tienda de Apple y pasó un sinfín de horas con su operador, sus proveedores de servicios financieros, y otras partes implicadas en la ecuación. Fue entonces cuando escuchó hablar del *SIM swapping* por primera vez.

El caso de Rob es el típico ataque de libro por *SIM swapping*. En primer lugar, el defraudador se puso en contacto con el operador de telefonía móvil de Rob, haciéndose pasar por él y convenciendo al agente para cambiar su número de teléfono a una nueva tarjeta SIM, con su correspondiente numeración. A continuación, el estafador solicitó cambiar la contraseña del correo electrónico y de las cuentas bancarias de Rob e hizo que las nuevas credenciales se las enviaran por mensaje de texto. Dado que el defraudador había intercambiado la SIM asociada al número de teléfono de Rob por una que él controlaba, todas las contraseñas de un solo uso fueron enviadas a su dispositivo y en cuestión de minutos tuvo acceso a todas las cuentas de Rob.

Todo ello se podría haber evitado si el operador de telefonía móvil de Rob hubiera utilizado factores de seguridad biométricos para validar la identidad de la persona que intentaba materializar la estafa. En lugar de eso, los procesos de autenticación laxos del operador permitieron al defraudador hacerse con facilidad con el control del teléfono de Rob, acceder a sus cuentas y robar todos sus ahorros.

La búsqueda de respuestas y la repercusión

A los pocos días, Rob supo que los miles de euros que había en su cuenta habían sido convertidos a bitcoin y los habían retirado de su cuenta completamente. Imagínate por un momento que los ahorros de toda tu vida desaparecen en cuestión de minutos. Para Rob, estos ahorros eran para la universidad de su hija, su plan de pensiones y gastos familiares: se sentía abatido y sin saber a dónde ir. El impacto físico y mental que esto tuvo para él fue importante, yendo del insomnio a la agonía emocional. No obstante, Rob no está solo; de hecho, muchas víctimas de fraude han vivido consecuencias devastadoras para sus vidas, como divorcios o graves efectos en su salud mental.

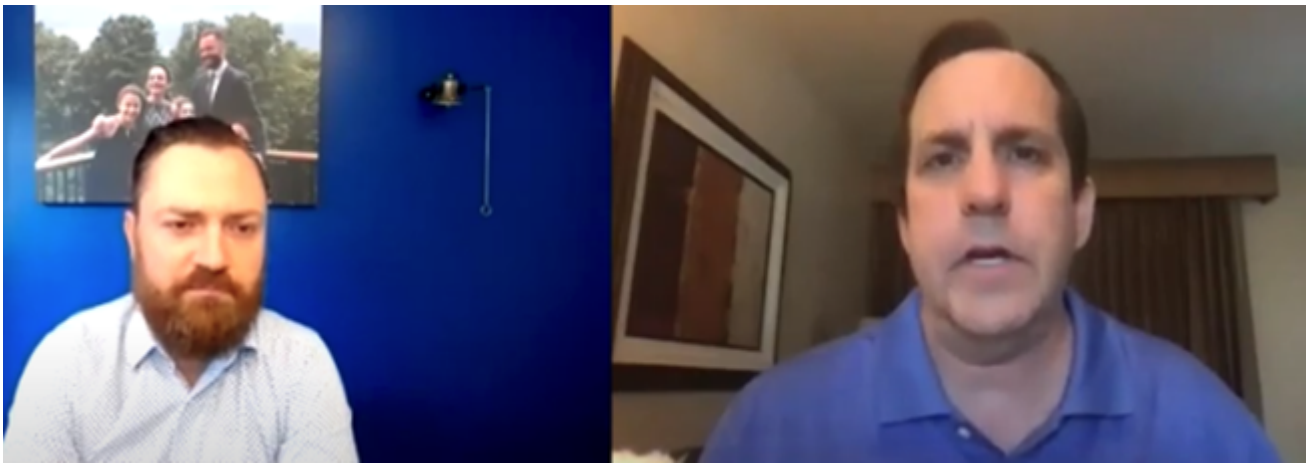
Rob trabajó con varias agencias para descubrir al defraudador. Es más, hay un estafador que se enfrenta a veintiún cargos por el delito contra Rob y contra otras once víctimas, pero, por desgracia, una parte importante de los ahorros de Rob no ha podido rescatarse.

Rob no ha sido la única persona afectada, ya que este tipo de delitos afectan a toda la familia. Sin ir más lejos, mantuvo una conmovedora conversación con su hija, que por aquel entonces iba al instituto, sobre su preocupación por el pago de la universidad, por cómo habría que ajustar su estilo de vida dada la nueva realidad financiera – menos vacaciones, menos tiempo juntos, etc. – y cómo el robo de todos sus documentos personales había expuesto su número de Seguridad Social, el carnet de conducir o el número de su pasaporte, lo que aumenta la posibilidad de sufrir otro ataque de fraude en el futuro.

El giro hacia la prevención y la educación

Durante todo este calvario, Rob ha trabajado para formarse y educar a consumidores y empresas sobre la importancia de contar con herramientas tecnológicas que puedan eliminar la duda para los agentes de los *call centers* y protegerles a ellos y a sus clientes de las técnicas de ingeniería social. De hecho, ha creado una organización para ayudar a otros que se llama Stopsimcrime.org, y cuyo principal objetivo es trasladar el mensaje de la importancia de contar con procesos fiables y soluciones técnicas para que lo que le pasó a él no ocurra nunca más.

Rob explica que es cliente desde hace mucho tiempo de Schwab y que le alegró saber que utilizan ID de voz para la autentificación. *«Todo lo que tengo que hacer es decir, mi voz es mi contraseña , y eso me da sensación de seguridad, de que han ido más allá para protegerme utilizando mi voz y sus atributos únicos para comprobar que soy quien digo ser».*



Rob Ross:

¿Tiene la sensación de que la mayoría de compañías de telecomunicaciones se están tomando este asunto lo suficientemente en serio? Sobre todo, dado que afecta, principalmente, a otras cuentas propiedad del consumidor (cuentas bancarias, de email, redes sociales, etc.), y no tanto a las que son propiedad de las *telcos* (cable, teléfono, internet, tv). Si no lo hacen, es decir, si no le dan la importancia que merece, ¿cuál es la mejor manera para que proveedores de tecnología como Nuance ayuden a convencerles de que ha llegado el momento de tomar acciones adicionales?

Brett Beranek:

Las compañías de telecomunicaciones son conscientes del riesgo que supone el *SIM swapping* para los consumidores, pero están tardando en reconocer su propia responsabilidad en la lucha contra este fenómeno. La falta de pérdidas financieras significativas y de regulación es, sin duda, una de las principales razones por las que estas organizaciones no están adoptando medidas igual de rápido que las instituciones financieras, e incluso que los comercios, a la hora de modernizar su estrategia de autenticación. Por suerte, en los últimos meses se está empezando a vislumbrar un cambio. Las *telcos* están empezando a unirse a la lucha contra el fraude y la responsabilidad social corporativa (RSC) está aportando innovación en el frente de la autenticación. Para empresas como Nuance, el mejor enfoque es seguir educando sobre los riesgos que la usurpación de cuentas representa y dar voz a las víctimas; al final, esas compañías tecnológicas actuarán porque sientan que es lo que hay que hacer, y no solo para mitigar las pérdidas financieras, algo que por sí solo no es lo suficientemente importante como para motivar el cambio.

RR:

Cuando los clientes deciden que no quieren registrar su huella de voz y/o las empresas no tienen la inversión para desplegar soluciones escaladas de este tipo, ¿qué pueden ofrecer para minimizar el riesgo de sufrir una estafa por *SIM swapping*?

BB:

Aunque los clientes no estén registrados con biometría de voz , todavía es posible para una empresa de telecomunicaciones analizar pasivamente todas las llamadas cuando un cliente solicita un cambio de tarjeta SIM y comparar la voz del interlocutor con una lista de voces de estafadores conocidos. En cuestión de segundos, el agente del servicio de atención al cliente recibirá una notificación de que existe un riesgo y podrá tomar medidas específicas o escalar la llamada al equipo de fraude. Este enfoque del fraude en primera instancia ligado a la biometría de voz ha demostrado aportar mucho valor, además de ser una implementación más rápida y sencilla. Esta solución permite que todo tipo de técnicas de investigación contra el fraude se vuelvan disponibles, como el *data mining* o el *voice clustering*.

Si desea escuchar más información sobre la historia de Rob o sobre lo que las compañías pueden hacer para protegernos ante el SIM Swapping y otros tipos de fraude, puede acceder a la conversación de 30 minutos o puede ponerse en contacto con Nuance para obtener más información.

Tags: biometría, Duplicado de tarjeta SIM, fraude, SIM swapping

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