What's next

Empresa

La revolución de los nuevos años 20: la edad de oro de la prevención del fraude

Una nueva década con nuevos comienzos y nuevas oportunidades, 2020 fue un año anunciado como el punto de inflexión para la tecnología y la innovación. Pero 2020 no ha empezado como nos hubiéramos imaginado ...

Brett Beranek
Posted 6 mayo 2020

El Covid-19 ha generado una situación de incertidumbre para todos. La ola de sentimientos, tan contradictorios como cambiantes, ha cambiado el comportamiento del consumidor. Muchos llaman con frecuencia a sus bancos para verificar los pagos y buscar garantías. Algunos se vuelcan en el trabajo para mantenerse ocupados y sentir sensación de progreso. Y otros simplemente prefieren desconcertar del bombardeo de noticias diarias sobre la pandemia a la que estamos sometidos en prensa y televisión, para disfrutar de la variedad de

películas, series y documentales que nos brinda Netflix.

Pese a todo esto, hay una cruda realidad vinculada a la incertidumbre y estos cambios de comportamiento: el fraude. Y es que los estafadores, aprovechan situaciones de crisis como esta, para desarrollar intentos cada vez más sofisticados para engañar a las personas y tener acceso a sus datos personales. Desde la ingeniería social hasta el phishing por correo electrónico y la creación de sitios web falsos.

Empresas en todo el mundo han sido testigo de un aumento significativo del volumen de ataque de fraude, que van desde el 200% al 400% en las últimas semanas, dependiendo de la industria. Algunos de estos ataques se relacionan directamente con la pandemia, con informes recientes que sugieren que ha habido cientos de estafas relacionadas con el coronavirus y miles de intentos de phishing hasta el momento. Y, se espera que estas cifras aumenten con el tiempo.

La debilidad de los métodos tradicionales de autenticación

En tiempos de incertidumbre como este, es aún más importante ofrecer a los consumidores la tranquilidad de que su organización está haciendo todo lo posible para protegerles de actividades fraudulentas: la autenticación juega un papel clave en este proceso. El Oxford English Dictionary define la autenticación como «el acto de demostrar que algo es real, verdadero o lo que alguien dice ser».

Tradicionalmente, se han utilizado las credenciales basadas en el conocimiento para demostrar que somos quienes decimos ser: el uso de nombres y direcciones, contraseñas o códigos PIN, o el apellido de soltera de su madre, por ejemplo. Sin embargo, este medio de identificación es aún más susceptible a la ingeniería social en tiempos de COVID-19.

Los consumidores son el objetivo de muchos estafadores que utilizan, por ejemplo, los conocidos ataques de phishing para obtener dicha información confidencial. Ya sea por correo electrónico, teléfono, mensaje de texto o en persona, este tipo de técnicas no son especialmente sofisticadas, pero si efectivas para acceder a los fondos o cuentas bancarias de un individuo.

Las contraseñas de un solo uso (OTP) a través de SMS, por ejemplo, dan una falsa sensación de seguridad, pero no evitan de ninguna manera la suplantación de identidad y apropiación indebida de cuentas. Si un estafador tiene suficiente información sobre la víctima para señalar a su cuenta bancaria, entonces tiene todo lo que necesita para acceder a su cuenta de teléfono e interceptar cualquier SMS que se le envíe.

El año pasado, incluso antes del impacto del coronavirus, el fraude le costó a la economía global $ 5 (USD) billones. Una encuesta global realizada por Nuance al mismo tiempo señaló que uno de cada cuatro (24%) de los consumidores había sido víctima de fraude en los últimos doce meses, perdiendo un promedio de $ 2,000 (USD) debido a contraseñas ineficientes. Es probable que este número aumente, dado el volumen de actividad fraudulenta vinculada al coronavirus.

Esa pérdida por fraude no solo afecta al consumidor ni a las primas de seguro del banco. Golpea a las empresas asociadas involuntariamente con el fraude. Los consumidores se dan de baja rápidamente de aquellas empresas relacionadas con el fraude. Dos tercios (62%) señala que cambiaría de empresa sin pensárselo dos veces, si fuera víctimas de fraude.

Incorpore la biometría

La biometría es una solución para aquellas organizaciones que buscan prevenir y detectar el fraude y garantizar la seguridad tanto de sus clientes como de sus empleados del contact center.

Es la mejor alternativa a las contraseñas y los códigos PIN. La biometría de voz, por ejemplo, no puede verse comprometida de la misma manera que los métodos de seguridad basados en el conocimiento. Esto se debe a que las voces humanas son tan únicas como una huella dactilar. Al emplear algoritmos sofisticados para analizar más de 1,000 características propias de voz, la tecnología biométrica de voz usa la voz de quien llama no solo para validar su identidad sino también para protegerla contra los hackers. El método de autenticación a través de OTP, por ejemplo, podría ser eficaz si se combinase con biometría y notificaciones push.

Otra modalidad como alternativa a la biometría de voz, es la biometría del comportamiento. Esta tecnología mide cómo interactúa un individuo con un dispositivo: cómo escribe, cómo teclea, cómo desliza el cursor o incluso cómo sujeta el teléfono, para identificar si es quién dice ser.

Cuando se les informó de que la tecnología biométrica está probada para ayudar a atrapar delincuentes en el acto de intentar cometer fraude y prevenirlo antes de que ocurra, un tercio el (36%) de los consumidores dijo que haría negocios con empresas que ofreciesen biometría. Un número similar (25%) incluso pidió que más empresas lo usaran.

Entonces, ¿nos encontramos ante la edad de oro de la prevención del fraude?

La biometría está desempeñando un papel fundamental, a medida que aumenta la demanda en el contact center, y los clientes solicitan mayor tranquilidad y mayores garantías. En el contexto actual en el cual los agentes se ven obligados a trabajar desde casa, es más importante que nunca que los Contac centers refuercen los procesos de autenticación mediante biometría para poder centrase en lo que más importa: la atención al cliente. Dado que las circunstancias actuales obligan a las empresas a tomar medidas extraordinarias para volver a movilizar su fuerza de trabajo, alterar los estilos de trabajo y, en algunos casos, reinventar por completo los modelos de negocio, ahora es el momento de considerar cómo su organización autentica a sus usuarios y los protege de actividades fraudulentas. La incertidumbre a menudo impone innovación. Si esa innovación ayuda a proteger a los consumidores de los estafadores, se habrá dado un paso adelante para evitar la creciente amenaza de fraude, ahora y en el futuro.

Tags:

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