What's next

Empresa

# Tendencias en seguridad y prevención contra el fraude para 2021

Cada año son más los usuarios que afirman haber sido víctimas de fraude online. Por desgracia, el número de ataques no ha hecho otra cosa que aumentar durante la pandemia, ya que el volumen de interacciones online – por ejemplo, las compras o los movimientos bancarios – se han multiplicado considerablemente dadas las circunstancias actuales. En este contexto, desde Nuance ofrecemos nuestras predicciones de ciberseguridad para 2021.

**Brett Beranek**
Posted 21 enero 2021

A continuación, presentamos un resumen de cinco tendencias clave de seguridad digital que abarcan desde la ciberseguridad, la prevención del fraude y la gestión de riesgos.

**Los CISO (Chief Information Security Officers) con visión de futuro pasarán a la autenticación sin contraseñas con el doble objetivo de mejorar la experiencia del cliente y la seguridad de las empresas**

Los consumidores quieren una experiencia digital que sea fácil, segura y sin contraseñas. Las contraseñas y los pines que hoy todavía seguimos introduciendo en el día a día, están cerca de convertirse en reliquias. A medida que los consumidores se instalan en los canales digitales para realizar operaciones bancarias, socializar, jugar o comprar, estos demandan una experiencia de usuario cada vez más sofisticada y segura. Las contraseñas han generado en los consumidores una falsa sensación de seguridad durante años, especialmente a medida que el número y la variedad de los smartphones desde los que se utilizan las apps se ha

disparado, y cada uno de ellos requiere que se introduzca información crítica repetidamente y esta información puede ser rastreada o robada. Así, las empresas deberán demostrar a sus clientes que se toman en serio su seguridad. Los consumidores son ahora más conscientes que nunca de los riesgos que rodean su identidad, por lo que comenzarán a exigir más de las empresas con las que tratan. Para las organizaciones, una mayor seguridad es ahora una cuestión de retención de clientes, lealtad y responsabilidad social corporativa.

**Un enfoque integrado para la prevención del fraude y la autenticación será clave para la protección contra la biometría débil de los dispositivos**

Los clientes van a exigir protocolos de seguridad que sean capaces de identificarles, evitando que cualquiera que pueda tener su identificación pueda hacerse pasar por ellos. Gracias a años de interacción con dispositivos inteligentes, las personas ya se sienten cómodas con opciones biométricas como la identificación de huellas dactilares o el reconocimiento facial. No obstante, la mayoría de estos métodos de autenticación no tienen ningún impacto real para detener a los estafadores. Su «valor» comienza y termina con que sean gratis y para un dispositivo concreto. Son los datos biométricos del lado del servidor, como la biometría de voz, los que tendrán impacto en la prevención del fraude y proporcionarán una experiencia gratificante a los clientes.

**La IA permitirá que la biometría resuelva desafíos de seguridad cada vez más complejos**

A principios de año, Telefónica S.A pidió a Nuance que le ayudáramos a desplegar la biometría de voz para analizar el sonido de la voz de sus clientes y determinar si eran mayores de 65 años o no. Así, el operador ha podido proporcionar una protección contra el fraude excepcional al grupo de clientes cuya edad les hace más vulnerables al fraude.

Aprovechar este tipo de tecnología vanguardista permitirá a las organizaciones no solo priorizar o adaptar los servicios a la demografía específica de los clientes, sino que también fortalecerá los esfuerzos de prevención contra el fraude al proporcionar factores biométricos adicionales a considerar.

**La seguridad necesitará fortalecerse para proteger los activos contra el aumento del fraude provocado por el trabajo en remoto.**

A medida que las organizaciones extienden el trabajo desde casa de manera indefinida – en lo que una de las portadas más recientes de Harvard Business Review llama «El futuro del trabajo desde cualquier lugar» (Nov.-Dic. 2020) –, el fraude contra empleados que estén teletrabajando aumentará, pero esta metodología también puede llevar a un aumento del

fraude ocupacional. Los empleados sin supervisión con acceso a Información Personal Identificable (PII) tienen una nueva oportunidad de defraudar al resto del personal y robar información valiosa. Bajo la presión cada vez mayor generada por la situación económica y social que estamos viviendo, las condiciones son adecuadas para un aumento de este tipo de fraude. Forrester Research se hace eco de esto, pronosticando que el 33% de las brechas de datos serán causadas por incidentes internos, un 8% más que en la actualidad. Las empresas deberán trabajar rápidamente para combatir los *voice fakes* y *deep voices* para asegurar que las interacciones entre trabajadores de todo el mundo se producen sin problema. Las medidas de seguridad tradicionales también deberán operar al máximo rendimiento con tantas personas fuera de los *firewalls* de una organización.

**La relación con el cliente cambiará drásticamente y pasará a ser por vídeo/virtual**

A medida que las consultas, transacciones e interacciones virtuales se convierten en la norma entre las marcas y consumidores, los canales digitales necesitarán ser tan seguros y prácticos como si de una interacción física se tratara. La atención al cliente por vídeo es una tendencia que estamos viendo emerger como respuesta al COVID-19, y la biometría de voz es un aspecto crítico de la autenticación y seguridad de los clientes.

Por ejemplo, IBK (Banco Industrial de Corea) ha implementado la tecnología de biometría de voz de Nuance para garantizar una autenticación de cliente sólida y sofisticada a medida que las transacciones virtuales aumentan significativamente. Con un 100% de consistencia en las tasas de validación, IBK ha podido revolucionar la experiencia de la banca digital.

*Podemos encontrar consuelo en un 2021 que impulse una mayor seguridad digital y, por ende, tranquilidad. Las formas tradicionales de hacer las cosas, incluso las tan rudimentarias y fundamentales como las contraseñas online, ya no son suficientes. Los sistemas de seguridad biométrica basados en rasgos verificables como el escaneo de retina, las huellas dactilares y los patrones de voz reemplazarán los códigos subjetivos, que se pueden robar fácilmente y muchas veces son mal utilizados. Quienes adopten esos sistemas biométricos darán un salto cualitativo en sus protocolos de seguridad y tendrán una transición fluida hacia una presencia digital más segura.*

**Tags:** AI, biometría, customer experience, transformación digital

## More Information

## 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