

Boletín Informativo / Noviembre 2016

UPCLC/CFT

Tema: NUEVAS INNOVACIONES DE SEGURIDAD PARA EVITAR FRAUDES EN EL SISTEMA FINANCIERO

SEGURIDAD BIOMÉTRICA GANA POPULARIDAD, PERO ESTÁ LEJOS DE SER INFALIBLE

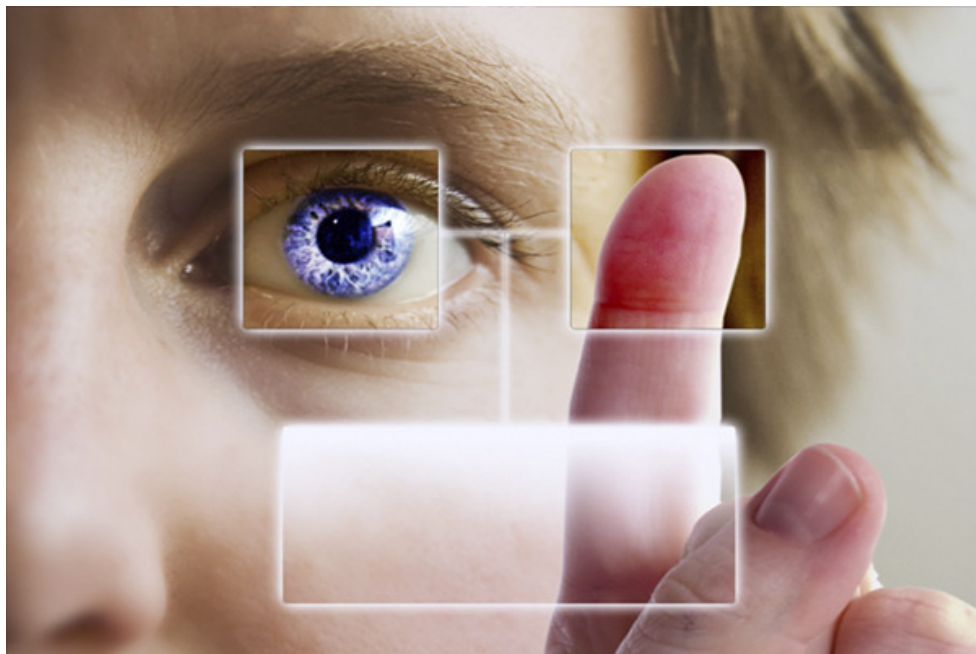
10 DE NOVIEMBRE DE, EL AÑO 2016

La importancia de la seguridad cibernética, sobre todo a la banca, está bajo un foco de luz por el momento, ya que los usuarios de banca en línea, móviles y los consumidores financieros tienen que tratar con hacks, troyanos, bots y software malicioso, todo ganando terreno en los últimos dos meses a nivel internacional.



Cuando se habla de seguridad cibernética, el tema de la autenticación biométrica se eleva junto a él como un mejor método, más seguro, más eficaz de la seguridad. Pero lo es?... ¿Los datos biométricos realmente ofrecen una manera más segura para completar las transacciones de compra en línea?

"La biometría es un método de autenticación específico del dispositivo," dijo Madeline Aufseeser (experto en seguridad biométrica), CEO de línea de la compañía de prevención del fraude Tender la Armadura , de las formas de autenticación biométrica se utiliza actualmente para asegurar una transacción de compra digital (en lugar de iniciar sesión en el sitio web de un banco, a ver una cuenta o transferir dinero). "Por lo general el mismo método biométrico no funciona a través de múltiples canales de compra en la actualidad. La huella digital se utiliza para hacer una compra con un teléfono inteligente no necesariamente puede ser utilizado para autenticar una orden de compra del teléfono o compra realizada con un ordenador. Al confirmar [una transacción de compra] con su huella digital en un teléfono inteligente, todo lo que está diciendo es que esa es la misma huella que ha permitido el uso de este teléfono, o la aplicación específica en el teléfono. Debido a que la huella digital es único residente y almacenados en el teléfono, el teléfono está autenticando en sí, no es el titular de la tarjeta que realiza la transacción".



Esto suena un poco extraño en comparación con lo que podría haber oído acerca de las capacidades de la biometría con anterioridad, sobre todo porque va en contra de un supuesto básico: que un identificador biométrico (como una huella digital) va con los datos transaccionales, desde el teléfono o dispositivo, al procesador de pagos, al comerciante.

Esto no sucede. Por el contrario, el uso de una huella digital para autenticar una compra en su teléfono solo permite que el teléfono sepa que se le permite enviar los datos al realizar la compra; cuando los datos que se mueve, el identificador biométrico no lo hace. Además, el identificador se guarda en ese teléfono específico.

Este es un problema, especialmente cuando uno mira en otro supuesto básico: la creencia de que una huella digital, patrón del iris, huella de voz, partido facial, u otras formas de identificación biométrica son inherentemente más seguro, ya que coincide con una persona individual, a diferencia de lo que algunos de biometría han denominado métodos "estáticos", al igual que los PIN o contraseñas. Sin embargo, los datos biométricos pueden no ser tan "activos" como algunos han pretendido.



"Tampoco es todos los datos biométricos dinámico, lo que significa que puede ser comprometida y copiado. ¿Cambia su huella digital? ", Dice Aufseeser. "Hay una percepción no probado, que la biometría puede ser un método fácil para autenticar una transacción. Va a reducir algunos de los fraudes? Absolutamente. Es a prueba de balas? No, como hemos visto con el troyano para Android".

Continúa Aufseeser:

"El mayor problema con la autenticación biométrica se utiliza para las compras es que los titulares de tarjetas de datos biométricos no está siendo recogido y almacenado por los bancos. Eso significa que los bancos no tienen medios para validar los datos biométricos se utilizan para autenticar la compra".

Estos supuestos son, de acuerdo con Aufseeser " creando una falsa sensación de seguridad en torno a la utilidad de datos biométricos con los consumidores y de la industria."

Como se pueden tener en cuenta, como un vigilante de Fintech, o simplemente un miembro del mundo moderno, que todavía tenemos que encontrar un método de seguridad que es invencible, e incluso los que están en el campo de la biometría admitimos no es una excepción.

Información extraída de la fuente:

<http://bankinnovation.net/>