



«Mi voz es mi contraseña»

● La banca da un paso más en la utilización de la biometría para validar operaciones

Gracias a la aparición de la biometría como sistema de identificación, el cliente bancario ya no tendría que recordar las molestas contraseñas ni tampoco tener que validar un PIN generado automáticamente en el dispositivo. Primero fue la huella dactilar, para después incorporar el reconocimiento facial. Entidades como BBVA permiten autorizar una compra o abrir una cuenta en el banco con un proceso tan sencillo como hacerse un selfie.

Ahora, Banca March ha dado un paso más y emplea el reconocimiento de voz en

el cierre de operaciones, convirtiéndose, de esta manera, en la primera entidad en hacerlo. Eso no es nada nuevo, ya que la tecnología que utiliza la voz para interactuar en el día a día ya llevaba años aplicándose a través de los teléfonos inteligentes y también en los asistentes de conducción o del hogar. «La voz ha llegado para quedarse, a fecha de hoy ya es una realidad llena de futuro dentro del ecosistema digital», explican fuentes de Banca March.

En concreto, el servicio de reconocimiento de voz de la entidad estará disponible para la firma de cualquier tipo de traspaso o transferencia que realice el



cliente, independientemente del destino o el importe.

Y para darse de alta, el usuario solo tendrá que entrar en la app de Banca March desde un dispositivo de confianza y grabar tres veces la frase: «Mi voz es mi contraseña». Una vez finalizada la grabación, el cliente tendrá que firmar el registro y su voz habrá quedado guardada para su ulterior utilización en la firma de operaciones.

Seguridad y rapidez

La incorporación de la biometría conlleva una serie de bondades dentro del ecosistema bancario. Por un lado, la banca busca aumentar la seguridad de las operaciones, ya que se usan características que son únicas de cada individuo y que, asociadas con otros mecanismos como la tokenización, generan una combinación imbatible en materia de seguridad.

«Los rasgos biométricos, como los físicos, morfológicos y fonéticos del patrón de voz, que generan su huella biométrica, lo convierten en el mecanismo más seguro de identificación», explican desde la entidad. En la práctica, esto significa que «nadie puede firmar por el cliente» incluso aunque se logre acceder a las contraseñas o se pierda el dispositivo móvil empleado para acceder a la banca digital.

Además, se agiliza la operativa. «Esta nueva utilidad supone una mejor experiencia para el usuario, ya que se validan las transacciones de manera más inmediata y sin fricciones de dependencias externas como la tarjeta de coordenadas», apuntan desde la entidad. Un claro ejemplo lo encontramos cuando desbloqueamos el teléfono (que según Internet Trends hacemos una media de 150 veces al día). La aplicación de la biometría permite hacerlo de manera mucho más rápida y cómoda.

Una mayor aceptación de la biometría

El empleo de la biometría en Europa se ha visto reforzado con la reciente recomendación de la Autoridad Bancaria Europea: hay que apostar por la biometría para poder cumplir con la nueva normativa de servicios de pago PSD2, que exige por lo menos dos elementos de autenticación reforzada.

Si bien el acceso por huella digital sigue siendo método hasta la fecha más empleado, todo indica que el reconocimiento de voz puede ser el que tenga más capacidad

de crecimiento, ya que su aplicación en otros servicios es cada vez más popular.

«Estamos en un proceso que está comenzando», admite Selva Orejón, profesora de EAE Business School y experta en ciberseguridad, quien recuerda que la biometría no sólo se aplica en las aplicaciones bancarias, sino que también se está incorporando a otros medios, como pueden ser los cajeros. Un ejemplo es Caixabank. La entidad tiene una de las mayores redes de cajeros con reconocimiento facial. Gracias a ello, sus clientes pueden retirar dinero en efectivo sin necesidad de introducir ningún tipo de clave.

Incluso, cada vez será más habitual la aplicación de la biometría del comportamiento, que analiza la forma de relacionarse el cliente con el teclado del móvil o con el ratón del ordenador, que unido a la geolocalización y a la IP pueden detectar riesgos, incluso en operaciones pequeñas para terminar denegándolas.

Un arma de doble filo

A pesar de ser una tecnología muy segura, existe un peligro latente relacionado con el robo de datos. No podemos olvidar que cuando hablamos de datos es fundamental saber dónde se almacenan y con qué nivel de seguridad. Y esto todavía es más importante aun cuando nos referimos a información biométrica; ya que son los datos más personales y privados que existen. Por otro lado, si son puestos en peligro o perdidos puede ser catastrófico ya que, a diferencia de una clave o PIN, éstos no se pueden cambiar.

El problema, admite Orejón, es que la «seguridad absoluta no existe, ya que intervienen múltiples factores para garantizarla».

Este experto hace referencia al hecho de que el usuario medio no navega con un anti-malware ni tampoco tiene en su dispositivo móvil medidas de seguridad suficientes a pesar de que sí está utilizando todos los beneficios que puede tener el ahorro de tiempo y de desplazamiento de las aplicaciones bancarias.

Orejón no descarta que continúen las campañas de phishing en tanto que las empresas no lleven a cabo acciones de automatización y de eliminación de la información del cliente.

● Cristina Casillas

● Los sistemas más utilizados



EN PORCENTAJE.
FUENTE: CONVERSIA.