Publicado en Madrid el 17/05/2019

Las 5 reglas de oro en la seguridad de la banca móvil, según N26

Implantar funcionalidades como Mastercard 3D Secure, notificaciones push en tiempo real tras cada transacción o desarrollar sistemas de control interno sobre transacciones, procesos y sistemas cruciales en la seguridad de la banca móvil

La seguridad informática se ha convertido en un elemento indispensable a tener en cuenta en relación con la innovación financiera. Los clientes piden una experiencia bancaria cómoda en la que las interacciones se realicen con total garantía y seguridad, en horario continuo y sin interrupciones.

Estos puntos se han convertido en un factor clave de la revolución digital de la banca, máxime cuando según el informe 'Mobile en España y en el mundo 2018', España es el quinto país de Europa en que más usuarios acceden a la entidad financiera desde el móvil. Concretamente, más de la mitad de su población (52%).

Además, siete de cada diez consumidores españoles (69%) ha utilizado alguna vez un mobile wallet para pagar y aseguran que las técnicas biométricas de autentificación generan confianza en los usuarios. Es por ello que las entidades gastan hasta tres veces más en seguridad que las organizaciones no financieras, tal y como se desprende del informe elaborado por la empresa global de seguridad, Kaspersky Lab y B2B International.

Ante esta realidad, con motivo del Día de Internet, expertos de N26, el primer banco móvil global que está revolucionando el sector, han seleccionado las cinco reglas de oro en la seguridad de las entidades bancarias móviles para evitar ataques de phishing o pharming y garantizar la seguridad de las cuentas de sus clientes:

Una de las medidas de seguridad más relevantes para la banca móvil es implantar funcionalidades como 3D Secure de Mastercard. Este sistema, que valora las transacciones según el riesgo y se activa cuando detecta una transacción poco habitual, aporta aún más seguridad a los pagos en internet. Gracias a él, los clientes están al tanto de los movimientos en su cuenta bancaria y pueden confirmar el pago sin tener que recordar la contraseña en un sistema desarrollado por un algoritmo.

La inmediatez que permite la tecnología puede también emplearse para transmitir transparencia y confianza a los clientes a nivel de seguridad gracias a las notificaciones push automáticas. Algo tan simple como las notificaciones, a las que está acostumbrada prácticamente la totalidad de la población española, permiten informar en tiempo real de todos y cada uno de los movimientos que se producen en la cuenta sin necesidad de ver una transacción o esperar al final del periodo de facturación.

Otra medida que permite a las entidades financieras digitales poner freno a los ciberataques es colaborar con investigadores expertos en seguridad. Establecer un sistema de recompensas para

contar con investigadores expertos en materia de seguridad es crucial para identificar puntos débiles de cualquier tecnología. Un ejemplo seria el N26, el banco móvil que está revolucionando el sector. Además de haber establecido un nuevo equipo de desarrollo de software en Barcelona, dispone de un programa llamado Bug Bounty en el que ofrece recompensas en efectivo a expertos en seguridad por informarles sobre errores o vulnerabilidades detectadas.

Sin duda, lo más idóneo para evitar apertura de cuentas fraudulenta en la banca móvil es contar con procesos de verificación de la identidad de clientes que minimicen este riesgo. N26 apuesta por la verificación por vídeo en España, un proceso ágil y garantiza la seguridad del cliente sin añadir obstáculos o papeleos. Además, para evitar accesos no deseados en las cuentas de los clientes, lo más recomendable es instaurar varios niveles de acceso a la cuenta. Por ello, conviene que solo esté disponible desde un único terminal móvil a la vez. Además, es importante que haya que introducir una contraseña o huella dactilar además de un PIN que confirme cualquier transacción online y offline.

Datos de contacto:
TRESCOM

Nota de prensa publicada en: Madrid

Categorías: Finanzas Ciberseguridad Universidades