Nuevas iniciativas para cerrar el paso al fraude: los bancos, contra la ciberdelincuencia

Las entidades bancarias ponen en marcha multitud de medidas operativas y de concienciación para ayudar a los clientes frente a los intentos más sofisticados de comprometer su seguridad

El mundo de los timos y las estafas se reinventa prácticamente cada día. A pesar del esfuerzo de las entidades por atajar estas nuevas prácticas, siguen apareciendo nuevas. **Los intentos de fraude se sofistican cada vez más** y, por eso, cada vez debemos estar más preparados. La clave es sencilla: no desproteger jamás nuestros datos personales.

La última de las estafas, que se viene dando en los últimos meses, es la recepción de mensajes con una finalidad fraudulenta. El ataque se dirige en este caso contra usuarios de numerosas entidades financieras y aseguradoras. En ellos, **los ciberdelincuentes se hacen pasar por el banco** con la única finalidad de robar las credenciales de los clientes.

La técnica utilizada en este caso se llama **«smishing» o fraude por SMS** y no es nueva, aunque cada vez están mejor diseñadas. En este caso, el cliente recibía una comunicación en forma de mensaje en el móvil y se le invitaba a seguir un link. La página que abren es una **réplica de las webs reales de los bancos** y servía para averiguar el usuario y contraseña de las víctimas.

Las entidades financieras reaccionan con la máxima velocidad y transparencia una vez detectan este tipo de campañas cuyo único objetivo es engañar al máximo de clientes posibles. Sin ir más lejos, **ABANCA envió más de 900.000 mensajes al móvil de sus clientes**, con información sobre cómo actuar y qué tipo de acciones concretas seguir para evitar ser víctimas de este tipo de fraudes. La concienciación a los clientes, a través de todos los canales disponibles, es clave para evitar que se conviertan en víctimas de los ciberdelincuentes.

La banca trabaja —desde hace ya unos cuantos años— para que los clientes reconozcan aquellos indicios que deben levantar sus sospechas. Estas iniciativas informativas y didácticas sirven para nos familiaricemos con ciertas reglas básicas, como que **el banco nunca nos va a enviar enlaces o links donde se pidan claves de acceso**, ni solicitará proactivamente por teléfono las contraseñas que hayamos recibido por mensaje de SMS (y que sí sean las que nos ha enviado la entidad).

En los últimos años, ha crecido el abanico de opciones de fraude, como los SMS y las llamadas de voz, pero el trasfondo sigue siendo el mismo: **el cliente es el responsable de custodiar sus claves.**

Esto es algo que los ciberdelincuentes saben y por eso dirigen sus ataques contra ellos, porque son el eslabón más débil de la cadena. Suplantan identidades, piden actuar con urgencia en muchos casos y, en definitiva, añaden confusión para hacerse con su contraseña de acceso sirviéndose de un engaño.

Con la seguridad ya comprometida, actúan rápido para **vaciar cuentas a través de transferencias inmediatas al extranjero** o realizan compras con las tarjetas, dificultando enormemente seguir el rastro del dinero... y mucho más recuperarlo.

Es muy importante prestar toda la atención a los denominados OTP o **mensajes con códigos de confirmación que nos envían al móvil**. Sin ese SMS, los ciberdelincuentes no pueden hacer mucho y se sirven de cualquier treta para conseguir que les facilitemos ese código. La regla general es que, independientemente de lo que te cuenten para tratar de engañarte, en el texto del mensaje se devela el motivo real de la operación que estás a punto de confirmar, bien sea una transferencia o una instalación de la banca móvil en un nuevo dispositivo.

Por eso, y a pesar de todos los esfuerzos tecnológicos de las entidades financieras para atajar el fraude, el cliente es siempre quien finalmente va a comprometer su seguridad revelando sus claves. Por eso es de vital importancia **extremar las precauciones.**

Desarrollos de los bancos frente al fraude

Sin abandonar la línea de concienciación a los clientes, los esfuerzos de la banca también se centran en establecer medidas de carácter operativo que permitan **cerrarle el paso a los ciberdelicuentes**, incluso cuando las claves de sus usuarios ya han sido comprometidas.

Una de ellas es el establecimiento de **cortapasos centralizados** para hacer determinadas operaciones desde dispositivos que cumplen ciertas condiciones. Con ello, se busca identificar de manera más clara aquellas situaciones de riesgo para los clientes y que se escapan de su manera de operar habitual.

Estas y otras iniciativas son fundamentales para atajar toda opción de fraude y minimizar sus efectos. Los canales no presenciales son completamente seguros si se siguen unas reglas básicas, que se pueden repasar en el espacio de seguridad de la web de ABANCA.

Fuente: La Razón