13/05/2025

El Tribunal Supremo acaba de resolver quién es el responsable cuando te roban todo tu dinero por phishing: el banco

Una nueva sentencia protege a los usuarios en caso de estafa digital. El banco es el principal responsable

El **Tribunal Supremo** acaba de fallar a favor de los usuarios y en contra de la banca en uno de los temas más recurrentes de los últimos años: las estafas a través de internet. Declara que la banca es la principal responsable en estos casos de fraude, estando obligada a reponer de forma inmediata todo dinero sustraído al cliente.

No es cosa del usuario. El Tribunal Supremo ha confirmado una sentencia emitida el pasado 9 de abril, en la que la Sala de lo Civil rechazó el recurso de casación interpuesto por Ibercaja contra una resolución dictada por la Audiencia Provincial de Zaragoza en noviembre de 2022.

En esta **Sentencia 571/2025** se subraya que las buenas prácticas bancarias exigen la activación de sistemas capaces de detectar actividades sospechosas, así como de bloquear o verificar operaciones de alto riesgo.

Casi 60.000 euros, de vuelta al bolsillo. A menos que pueda demostrarse que el cliente actuó de forma negligente, el banco está obligado a asumir responsabilidad y devolver el dinero de inmediato. En este caso, Ibercaja Banco S.A. deberá reintegrar a un cliente 56.474,63 euros sustraídos de su cuenta mediante SIM Swapping, un sistema para suplantar nuestra identidad robando el número telefónico.

El magistrado Manuel Almenar Belenguer se vale de la Directiva Europea ante los servicios de pago, así como la normativa española, concluyendo que en caso de no haber negligencia, la única obligación del usuario es notificar a la entidad bancaria acerca de cualquier tipo de operación no autorizada.

La nueva jurisprudencia. Este caso sienta un precedente fundamental ya que establece que, a partir de ahora, las entidades bancarias serán las principales responsables en casos de phishing bancario. En consecuencia, deberán responder por operaciones no autorizadas por el usuario, marcando así un cambio significativo en la protección de los clientes frente al fraude electrónico.

> “Los avances de la tecnología actual hacen relativamente sencillo diseñar sistemas o aplicaciones informáticas idóneas para detectar ciertas anomalías en la prestación de los servicios de pago. Operaciones que, tratándose de empresas o sociedades con un concreto objeto social, pueden calificarse como ordinarias, deben inmediatamente levantar sospechas y dar lugar a una respuesta cuando afectan a personas físicas ajenas a tales actividad.”

Los bancos ya no tendrán excusa. En base a la judisprudencia, se expone que deben ser declaradas nudas las cláusulas contractuales que exoneren a las entidades bancarias de su responsabilidad con los usuarios respecto a las operaciones no autorizadas.

Hasta ahora, los bancos podían escudarse en supuestas malas prácticas llevadas a cabo por el usuario, como haber introducido sus datos en webs o enlaces maliciosos. Tras esta sentencia, son responsables de toda operación no autorizada.

Una plaga con la que el Gobierno intenta acabar. Las estafas por llamada y SMS son una plaga. Tanto, que el Ministerio de Transformación Digital lleva más de un año intentando ponerles freno. El fin de las llamadas comerciales llegó en febrero de 2025 bajo orden ministerial, pero esta es solo una parte minúscula en la tarta de las ciberestafas.

Llamadas falsas, estafas por WhatsApp, malware en tiendas como Google Play, suplantación de identidad por SMS... Las tácticas cambian y evolucionan para seguir teniendo una afectación y resultado. Recientemente, la Guardia Civil desmanteló una red de ciberestafas presuntamente liderada por un estudiante de 19 años.

La responsabilidad del usuario. Pese a la protección adicional que gozarán los clientes de las entidades en caso de ciberestafa, cae sobre el techo del usuario no caer en prácticas que puedan acabar considerándose como negligencia. Estas no se han establecido, pero no está de más no introducir nuestro teléfono, correo electrónico personal en webs cuya procedencia no tenemos clara.

En caso de usar Android, somos también responsables de lo que descargamos y de dónde lo descargamos, así como de los permisos que le damos a las aplicaciones. Protegerse va más allá de posibles sustracciones de dinero: es especialmente fácil acabar dándole todos nuestros datos a los ciberestafadores.

Fuente: https://www.xataka.com/

LINK DE LA NOTICIA