Publicado en León el 06/02/2023

Fin a las estafas por SMS: los jueces respaldan derechos de los consumidores

Según la empresa especializada en reclamaciones bancarias Economía Zero, se está produciendo un incremento de las sentencias en las que los bancos están siendo obligados a devolver el dinero a los consumidores que han sido víctimas de estos fraudes

En los últimos meses, el incremento de los fallos de seguridad de las entidades financieras, está propiciando un aumento exponencial en este tipo de estafas conocidas como Phishing o Smishing.

Estos mensajes maliciosos, suelen intentar engañar al usuario con frases como "Tu tarjeta ha sido bloqueada, ponte en contacto inmediatamente con la entidad" e incluyen un enlace que llevará a una página exactamente igual a la de la entidad suplantada.

El objetivo de estos mensajes es siempre el mismo: robar información y dinero.

"Los ciberdelincuentes, utilizan técnicas de ingeniería social para ganar la confianza de los usuarios y obtener acceso a sus cuentas e información".

¿Se puede recuperar el dinero estafado?
La ley de servicios de pago es muy clara.

"Cuando un cargo no ha sido autorizado, la entidad financiera debe devolver el dinero".

Si el importe sustraído es pequeño, los bancos suelen devolverlo con facilidad. El problema viene cuando la cifra es más elevada. En muchos de estos casos, a los consumidores no les queda más remedio que reclamar por la vía judicial.

Cada vez hay más sentencias en las que se condena a los bancos a la devolución del importe robado. Uno de los principales motivos, es que las entidades bancarias no han implementado las medidas de seguridad adecuadas, o no lo han hecho correctamente. Cuando el importe sustraído es considerable, es posible que el banco intente responsabilizar de su fallo de seguridad al cliente, llegando incluso a acusarlo de negligente.

"El banco es el que tiene que demostrar la negligencia del cliente y no al revés".

Economía Zero, una empresa especializada en derecho bancario con despachos de abogados colaboradores en todo el país, enfatiza la importancia de que los usuarios mantengan toda la documentación relacionada con su caso. Conservar los mensajes y tomar capturas de pantalla es esencial para tener éxito en un juicio.

¿Qué ocurre si se pincha en uno de estos enlaces?
Recibir uno de estos mensajes, no tiene por qué suponer ningún riesgo siempre y cuando la víctima no pinche en el enlace. El problema es que estos SMS, suelen llegar en la misma conversación que los de la entidad entidad suplantada y desde el mismo número de teléfono.

Con tan solo pulsar en el enlace, y dependiendo de varios factores técnicos, los atacantes pueden llegar a infectar con malware el dispositivo de la víctima. Independientemente de si la infección llega a producirse o no, el enlace malicioso llevará a una página falsa exactamente igual a la de la entidad bancaria.

Es importante tener en cuenta que las entidades financieras nunca solicitarán información confidencial a través de mensajes de texto o correos electrónicos. Si se recibe un mensaje sospechoso, es recomendable que se compruebe su autenticidad antes de proporcionar cualquier información. Una forma de hacerlo es verificando el enlace incluido en el mensaje. Aunque puede parecer la misma página que la entidad bancaria, nunca será la oficial.

Hay que fijarse en el nombre del dominio. Suelen utilizar subdominios o nombres que incluyan el nombre de la entidad bancaria, o dominios que no tienen extensiones habituales.

Un ejemplo de página fraudulenta podría ser: "https://bbva.dominiocoatacante.com"

En este caso, el dominio al que se conectará la víctima es dominioatacante.com y no la conocida entidad bancaria. Por eso, es muy importante tomar precauciones y ser cauteloso al proporcionar información personal en línea.

¿Qué debe hacer la víctima en estos casos?
Lo primero que hay que hacer, es bloquear la cuenta y tarjetas de crédito lo antes posible.

Es muy importante que la víctima recopile toda la información de la que disponga; extractos, cargos, mensajes, capturas de pantalla, etc.

"Economía Zero recomienda NO BORRAR los mensajes del dispositivo, ya que pueden llegar a ser una prueba determinante en caso de llegar a juicio".

Posteriormente, hay que acudir a la sucursal bancaria a pedir un extracto detallado del movimiento o movimientos fraudulentos. Estos extractos que proporciona la entidad suelen tener mucha más información de la que aparece en los extractos ordinarios.

Con toda esta información, la víctima tendrá que acudir lo antes posible a la policía o la guardia civil para poner una denuncia.

Ya con la denuncia, hay que acudir de nuevo al banco a poner una reclamación para pedir que la entidad devuelva el dinero robado.

Con importes pequeños, no suele haber problema, ya que el banco se lo reclama directamente a Visa, MasterCard, etc. y estas empresas tienen seguros que cubren este tipo de "daños económicos".

El problema surge cuando se trata de transferencias no autorizadas o cargos de cantidades considerables.

"En los casos en los que el dinero sustraído es considerable, las entidades intentarán hacer responsables de su fallo de seguridad a los clientes, haciéndoles responsables del robo y acusándolos de negligentes".

Por eso es muy importante estar bien asesorado por un abogado experto en este tipo de reclamaciones. Economía Zero, líder en reclamaciones bancarias, es una de las pocas empresas que asesora a sus clientes totalmente gratis, presentando en su nombre una reclamación extrajudicial que aumentará considerablemente las posibilidades de recuperar el dinero robado.

Datos de contacto:
Clara
987025011

Nota de prensa publicada en: León

Categorías: Nacional Derecho Finanzas Sociedad E-Commerce