Unicaja Banco es condenada a reembolsar miles de euros a sus clientes víctimas de estafas informáticas o phishing | Rankia

Unicaja Banco es condenada a reembolsar miles de euros a sus clientes víctimas de estafas informáticas o phishing

Autor Consumerista
09/04/2024

Tras conocerse un episodio de fraude masivo a clientes de Unicaja, tras la integración de la plataforma digital de Liberbank, en que unos estafadores desconocidos consiguieron ordenar transferencias contra sus cuentas por distintas cantidades, publiqué en julio de 2022 una primera nota sobre este tipo de estafas, consejos para prevenirlas y una primera aproximación a lo ocurrido en ese caso. Cuando van a cumplirse dos años de aquel episodio hemos llegado a conocer con detalle la operativa del fraude y los fallos de seguridad de Unicaja, con ayuda de un pequeño equipo de peritos muy cualificados, profesores de Informática en la Universidad de Oviedo, y estamos acumulando sentencias, que en todo caso están estimando las demandas, condenando a Unicaja a reembolsar la totalidad del importe defraudado más su interés legal y el pago de las costas del procedimiento judicial.

Hoy sabemos que el número de víctimas del fraude superó muy ampliamente el millar de clientes. Se prolongó durante más de un mes, sin que, sorprendentemente, Unicaja pudiera atajarlo en tan largo espacio de tiempo. Los defraudadores siguieron dos estrategias sucesivamente, en que demostraron una elevada capacitación en ingeniería informática, ingeniería social y conocimiento de los procedimientos de Unicaja, que imitaban muy fielmente de tal forma que para los clientes del Banco resultaba imposible detectar que quien les enviaba mensajes y/o llamaba por teléfono era un estafador y no personal de Unicaja.

Cernícalo vulgar Falco tinnunculus tinnunculus

Esa operativa puede resumirse así: enviaban un SMS (o una sucesión de ellos) a clientes de Unicaja (lo que sugiere que hubo algún tipo de filtración, por la que probablemente tuvieron acceso a un listado de clientes con su número de teléfono) advirtiendo de un acceso irregular a su banca digital, de alguna operación extraña o que se iba a cancelar su acceso a la cuenta digital, y que podían evitarlo accediendo a la web de, aparentemente, el propio banco, clicando en el enlace que se incluía en el propio SMS. Al pinchar en la URL, se accedía a una web que clonaba fielmente la del Banco, en la que el cliente debía incluir sus claves de acceso a la banca digital; a continuación se les pedía que introdujesen una clave para vincular el dispositivo (aparentemente, para volver a vincular el propio dispositivo, expulsando al que hubiese accedido previamente, de forma irregular), clave que les llegaba con otro SMS remitido realmente por Unicaja. Tras introducir esta clave, el dispositivo que se vinculaba era el de los estafadores, que podían ordenar las transferencias que quisieran, habitualmente dentro de los límites establecidos en cada caso para

las transferencias. A partir de cierta fecha, después de varios días en que se ejecutaron cientos de fraudes de esta forma, Unicaja estableció alguna medida de seguridad que impidió completar el fraude por esta vía, pero entonces siguió con otra variante: los defraudadores llamaban a las víctimas, identificándolas por su nombre y apellidos y numeración de la cuenta corriente, simulando ser empleados del servicio de ciberseguridad o atención al cliente del Banco, les informaban de algunas operaciones fraudulentas, y que se podían cancelar comunicando verbalmente los códigos que les llegarían a continuación por SMS; efectivamente, acto seguido llegaba uno o varios SMS de Unicaja con las claves referentes a esas operaciones, pero no para cancelarlas sino para autorizarlas definitivamente.

En esta operativa hay varias cosas que llaman la atención:

- que se confirmasen los cambios de dispositivo combinado con un código de un sólo uso remitido por SMS, práctica que Unicaja tenía adoptada a pesar de que el Banco de España ya había advertido meses antes del riesgo que entrañan las operaciones basadas en SMSs. En la actualidad, sólo se puede cambiar el dispositivo en las oficinas.

- que los SMSs con la claves de cambio de dispositivo o autorizando las transferencias eran enviados realmente por Unicaja, pero quien desencadenaba inicialmente la operación y provocaba la remisión de esos SMSs era el estafador. Unicaja estaba actuando simultáneamente con dos aparatos distintos entre sí, distantes, con sus propios IPs, sin detectar nada anómalo.

- el mecanismo del fraude incluye una serie de detalles que debieron hacer saltar alguna alarma en el sistema de seguridad de Unicaja por apartarse de los antecedentes de la operativa de los clientes afectados y, en general, por una serie de peculiaridades impropias de las prácticas de los usuarios bancarios ordinarios: se ordenaban transferencias inmediatas, algo poco habitual en consumidores, puesto que habitualmente tienen costes superiores y muchos ni siquiera conocen esa posibilidad, y con ello se evita que los usuarios pudieran reaccionar y tratar de cancelar la orden. Se ordenaban nada más ejecutar el cambio de dispositivo vinculado, y a cargo de clientes que en su mayor parte nunca habían ordenado transferencias en absoluto, o habían realizado alguna transferencia por importes muy inferiores a los ahora ordenados; se transferían en su gran mayor parte a una financiera de dinero electrónico irlandesa, en otros casos a una de Estonia, ambas totalmente desconocidas para la gran mayor parte de consumidores españoles (hubo algunos casos de transferencias a otros bancos). En muchos casos se siguieron ordenando y ejecutando nuevas transferencias incluso después de que los clientes contactaran con el teléfono de atención al cliente para informar de lo ocurrido y tratar de cancelar la operación. Parece evidente que Unicaja no tenía implementadas las medidas de seguridad pertinentes para prevenir fraudes digitales, en contra de lo que anuncia en su web y lo que exige el Reglamento Delegado (UE) 2018/389 de la Comisión de 27 de noviembre de 2017 por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para

la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros.

- Y, lo más llamativo, creo, es que Unicaja demorase más de un mes en conseguir poner fin a este fraude. Creo que el fallo en los sistemas de seguridad, la demora en la reacción, que se permitiesen seguir ejecutando operaciones tan extrañas durante tanto tiempo, ordenadas por dispositivos de personas sin identificar y con destino a cuentas en financieras exóticas, que aparentemente los defraudadores debían tener identificados a los clientes del Banco, deberían dar lugar a intervenciones inspectoras en materia de disciplina bancaria, de protección de datos personales y de prevención del blanqueo de capitales.

Las víctimas de los fraudes no tenían posibilidad práctica de detectar que no era Unicaja quien les contactaba: los SMS llegaban con el identificador del Banco y se agrupaban con los demás mensajes legítimos remitidos por éste; el enlace a la web incluía el nombre del Banco, y la web a la que se llegaba, además de tener el candado cerrado, identificativo de web segura, era un clon de la auténtica; en los casos en que se recibieron llamadas telefónicas, éstas aparecían con un número llamante también auténtico de Unicaja, sea del Departamento de Atención al Cliente o de alguna oficina; existen medios informáticos que permiten realizar estas suplantaciones; un gran número de empresas, corporaciones y entidades públicas de todo tipo vienen enviando mensajes con enlaces a webs propias o comerciales, por lo que no es sospechoso recibir un SMS de esas características y que pida solucionar el acceso o transferencia irregular por medios digitales, sobre todo en estos tiempos en que la banca quiere que todos dejemos de ir a las oficinas y hagamos todos nuestros trámites digitalmente.

Las sentencias ya obtenidas destacan en varias ocasiones los fallos de seguridad de Unicaja y las explicaciones al respecto de nuestros peritos.

Cogujada montesina Galerida theklae theresae

A la fecha de publicación de esta entrada del blog, he obtenido las siguientes sentencias, todas ellas favorables:

- Sentencia del 8 de junio de 2023 del Juzgado de 1ª Instancia nº 3 de Oviedo, por 9.200 euros, firme.

- Sentencia del 3 de agosto de 2023 del Juzgado de 1ª Instancia nº 2 de Pola de Lena, por 5.000 euros, firme.

- Sentencia del 20 de noviembre de 2023 del Juzgado de 1ª Instancia nº 2 de Pola de Lena, por 19.999 euros.

- Sentencia del 21 de diciembre de 2023 del Juzgado de 1ª Instancia nº 3 de Mieres, por 6.000 euros, confirmada por la sentencia de 21 de marzo de 2024 de la Sección 4ª de la Audiencia Provincial de Asturias.

- Sentencia del 28 de febrero de 2024 del Juzgado de 1ª Instancia nº 4 de Oviedo, por 6.000 euros.

- Sentencia del 11 de marzo de 2024 del Juzgado de 1ª Instancia nº 2 de Gijón, por 5.000 euros.

- Sentencia del 25 de marzo de 2024 del Juzgado de 1ª Instancia nº 3 de Avilés, por 10.000 euros.

- Sentencia del 25 de marzo de 2024 del Juzgado de 1ª Instancia nº 3 de Avilés, por 9.000 euros.