

SMS + LLAMADA TELEFÓNICA SINCRONIZADA

PARA VACIARTE LAS CUENTAS



Proyecto P-
45 "Audaz"



Buenas a todos ciber-navegantes. Hoy os voy a hablar de una estafa que pasó en Asturias recientemente y que incluso llegó a salir en algún periódico local por lo elaborado y lo sincronizado que está el equipo de delincuentes que la hace. **Se trata de un SMS y llamada coordinados para robarte las cuentas del banco.**



¿Cómo empieza este timo?

Todo empieza cuando alguien **recibe un mensaje SMS** diciendo que ha habido un **acceso no autorizado su cuenta bancaria**. Eso no sería nada novedoso en el mundo de las estafas si no fuera porque esta vez los estafadores hicieron los deberes y están enviando mensajes en nombre de un banco real: **Están suplantando un nº de teléfono**.

 En este caso fue Unicaja. Aunque ya os he dicho en otras entregas que el nombre del banco es irrelevante porque todos pueden ser víctimas.

¿Y qué quiere decir esto? Pues lo mismo que destacamos en entregas anteriores: los mensajes fraudulentos que **aparecen en el mismo hilo de conversación** que los mensajes reales de Unicaja, lo cual le da un plus de credibilidad, especialmente si andas con prisa o te despistas:

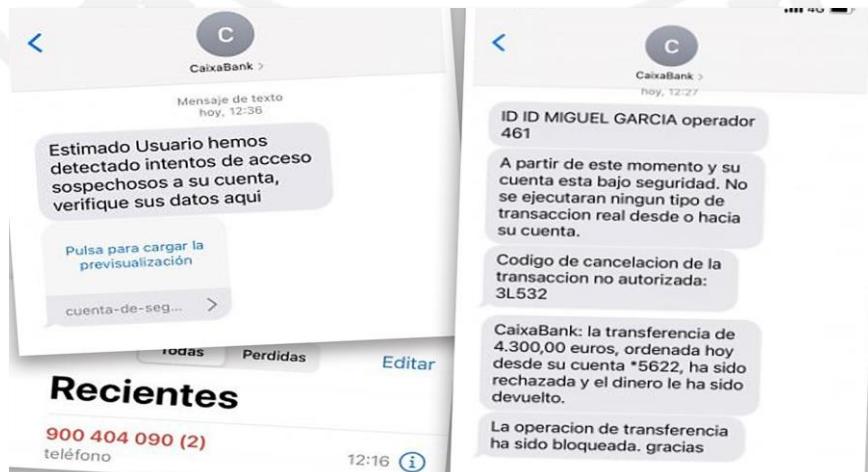


Figura 1. Todos estos mensajes son falsos, pero el teléfono los reconoce como de "CaixaBank" metiéndolos en la misma lista que los verdaderos, porque el delincuente ha suplantado el teléfono real. Fuente: <https://facua.org/noticias/detectan-de-un-nuevo-ciberfraude-que-roba-los-datos-bancarios-de-los-usuarios-de-caixabank/>

Se trata de un mensaje muy similar al de esta imagen:

Un dispositivo no autorizado se ha conectado a su cuenta online. Si no reconoce este acceso verifique inmediatamente: <https://unicaja.web-soporte.co/>

Figura 2. Mensaje fraudulento del estilo al que inicia esta estafa. Fíjate como aunque el enlace es falso, incluyen la palabra "Unicaja" en el para despistar y pillar a la gente que leer rápido. Fuente: <https://www.diariosur.es/tecnologia/dispositivo-autorizado-conectado-fraude-banco-20220828191413-nt.html>

Como se ve en la imagen, ese mensaje te pedía que accedieses a un enlace para confirmar el acceso no era legítimo. Y nuevamente, como os decía, los estafadores hicieron sus deberes y el enlace era bastante realista porque incluía las palabras Unicaja y .es dentro del mismo.

Si el engaño tiene éxito, la víctima entra al enlace y se encuentra con una copia exacta de la página de Unicaja, que como ya os dije más de una vez es muy muy fácil de hacer. Mete su contraseña y clave del banco y le dicen que muchas gracias por confirmar el acceso.

En realidad **en este punto el estafador todavía no tiene lo que quiere**, porque para sacar dinero de la cuenta necesita una clave que la víctima recibe en el teléfono. Si tú recibes una clave confirmando una transferencia que tú no has solicitado evidentemente se te activan todas las alarmas. Ellos lo saben y ahí llega la segunda parte del timo. **Te llaman**.

 **Date cuenta de que hoy en día por la normativa de seguridad europea uno no puede hacer ninguna operación sin confirmarla antes mediante el teléfono (habitualmente). Las medidas de seguridad han evolucionado...y los delincuentes también.**

¿Te llaman? ¿Además te llaman?

Y te llaman haciéndose pasar por un operario del banco diciéndote que, efectivamente, ha habido una filtración y que para anularla necesitan que les digas el código de un mensaje que te va a llegar al móvil que es “una clave secreta de anulación”, etc. Ya sabéis, toda la verborrea que se saben para convencerte de que todo eso es normal.

Pero, si lo haces, **estarás realmente confirmando una transferencia que el delincuente habrá hecho en tu cuenta**, cuyo usuario y clave sabe ya que tú se los has dado antes en la página falsa de Unicaja de la primera fase del timo. **Por tanto, tanto estarás autorizando el robo.**

 **Como ves, todo el timo consiste en saber tu cuenta, operar en tu nombre y obtener el código que te llega cuando hace la operación mediante engaño. El banco no sabe que no eres tú si todos los datos que introduce el que hace la operación son correctos...**

El problema que tienes en ese punto es que, una vez hecha la transferencia, **es muy difícil recuperar el dinero** porque se ha hecho con los cauces legales: tu nombre, tu contraseña y el código de confirmación. Es muy probable que te toque una batalla legal para recuperar tu dinero, que el delincuente ya habrá movido a cuentas fuera del alcance del banco y quizás de la justicia española.

💡 **Normalmente se mueven a las llamadas “cuentas mula”, o a servicios que se encargan de ocultar el origen del dinero. ¿Quieres saber más? Lee la próxima sección.**

¿A dónde va a parar el dinero robado y por qué es tan difícil seguirlo?

Uno de los destinos más frecuentes del dinero robado en estas estafas es lo que se denomina una “**cuenta mula**”. Una “cuenta bancaria mula” es una cuenta que se utiliza para recibir y transferir fondos obtenidos de manera fraudulenta. Las personas que facilitan sus cuentas para esto, a menudo sin saberlo, se conocen como “mulas bancarias”. Estas personas ayudan a los delincuentes a blanquear sus beneficios ilícitos, haciendo que estos fondos parezcan legítimos.

Los delincuentes **captan** mulas bancarias de varias formas. En algunos casos, las atraen con la promesa engañosa de **ganar dinero rápido y fácil** por Internet, o entregándoles una comisión por prestar este servicio (en este caso no hay engaño, la persona suele saber perfectamente lo que hace). En otros casos, se basan en una relación de confianza. Mira esto:

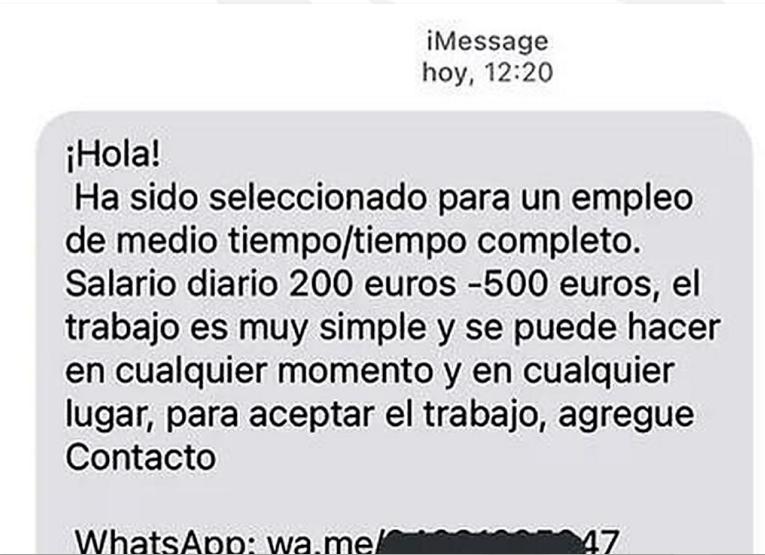


Figura 3. Típico mensaje ofreciendo "empleo" con el que puedes acabar haciendo de cibermula si sigues el juego. Fuente: <https://www.telemadrid.es/programas/madrid-trabaja/INCIBE-alerta-de-una-oferta-fraudulenta-de-empleo-via-SMS-9-2442745718-20220418044345.html>

💡 **¿Alguna vez te has topado con una oferta de empleo que dice que es un trabajo fácil, a media jornada, desde casa, que vas a ganar un dinero bastante sustancial por un esfuerzo mínimo? Ese es el típico engaño con el que te captan como mula. ¿Sabes lo peor? Cuando la policía descubra la trama, la culpa recaerá sobre ti, no sobre el delincuente, que probablemente desaparezca dejándote a ti el "marrón" 😞. Pero el dinero de la víctima del fraude original se lo habrá llevado el delincuente...**

Otra forma de blanqueo de dinero se hace **mediante criptomonedas**. Con el dinero que te roban el delincuente compra criptomonedas de algún tipo, con lo que automáticamente sus operaciones se hacen más difíciles de rastrear. Esto se debe a que las transacciones con

criptomonedas son **pseudónimas**, es decir, no están directamente vinculadas a la identidad real de una persona. No obstante, todas las transacciones que se hacen quedan registradas en lo que se llama una cadena de bloques o **blockchain**.

🔍 ¿Como es posible que se use para hacer fraudes si queda todo registrado? Sigue leyendo

Aunque queden registradas, existen servicios que permiten ocultar estas operaciones y hacer que su trazabilidad sea más compleja, aunque haya empresas vigilando esa cadena de bloques. Por ejemplo:

- **Paynym.is**: Este servicio hace uso de “direcciones fantasma” de monederos de criptomonedas. Se combina con una aplicación para *Android* llamada *Samourai Wallet*, que ofrece privacidad en las transacciones y permite evitar que las empresas de vigilancia del *blockchain* puedan identificar al que las hace.
- **Tippin.me**: Es una plataforma que permite recompensar a usuarios y creadores con una “propina” en bitcoins que se envía a usuarios de *Twitter*. La plataforma permite realizar micro-transacciones de forma rápida con privacidad mejorada.

Es importante destacar que, a pesar de esto, las criptomonedas no son completamente anónimas y las transacciones pueden ser rastreadas por las autoridades competentes. No obstante, si los robos son de baja cantidad, es muy probable que esa investigación no se termine realizando debido al esfuerzo que supone. También se puede hacer uso de un servicio que dificulta aún más el seguimiento de las transacciones hechas en criptomonedas como el llamado **TornadoCash**.

¿Y qué hago?

Así que ya veis, un timo doble que se basa en un SMS bien falsificado con un enlace también bien construido para engañar, junto con una llamada telefónica **con una temporización exquisita** confirmando la historia. Ya ha habido víctimas de esto en Asturias y en otras regiones y, como siempre que hay víctimas, los delincuentes pueden seguir con este modus operandi hasta que se genere suficiente alerta para que dejen de ser efectivos o les pillen.

🔍 Pero como al cabo de un tiempo esa “alarma” disminuye porque la gente olvida, vuelven a la carga. Muchos fraudes son periódicos.

Y para terminar os voy a dar el consejo de siempre **no le faciliteis datos bancarios a nadie** que os llame por teléfono, incluso aunque asegure ser la mismísima presidenta del banco central. **Ningún banco te pide las claves bancarias por teléfono**. Eso es un hecho contrastado que no admite discusión, ¡creedme!. ¿Qué pasa si te quedas con dudas? Lo de siempre: **¡Llama tú al banco al teléfono de siempre!** 😊

Y finalmente un poco lo de siempre. Por favor, **cuéntaselo a la gente**, porque esto es una campaña activa que vuelve periódicamente, y nunca sabes cuando alguien conozcas va a ser una víctima mañana mismo o dentro de poco. **¡Que corra la voz!**

¡Y esto es todo! Muchas gracias y...¡nos vemos en la próxima entrega!

Y recuerda amigo/a, las causalidades no existen y si recibes un SMS y una llamada seguidos con el mismo “cuento”, ¡sospecha!



¿Quieres escuchar como hablo de esta estafa en menos de 5 minutos?



- [**Escúchalo en Amazon Podcast**](#)
- [**Escúchalo en mi canal de YouTube**](#)
- [**¿Tienes otro cliente de Podcast? Este es el feed RSS**](#)

¿Quieres leer alguna noticia/artículo relacionado?



- [**Una ciberestafa vacía la cuenta bancaria de dos vecinos de Proaza \(06/03/2023\)**](#)
- [**INCIBE alerta de una oferta fraudulenta de empleo vía SMS \(18/04/2022\)**](#)
- [**Detectan de un nuevo ciberfraude que roba los datos bancarios de los usuarios de CaixaBank \(26/08/2021\)**](#)
- [**'Cibermulas': la última escala del crimen digital \(14/12/2011\)**](#)
- [**«Un dispositivo no autorizado se ha conectado a tu cuenta», el falso SMS del banco que es un fraude \(28/8/2022\)**](#)

Este documento usa material generado con IA²

¹ Audio emitido en “Más de Uno”. 95.2 Onda Cero Oviedo (<https://www.ondacero.es/emisoras/asturias/oviedo/directo/>) el 20/03/2023

² Algunas imágenes del texto del documento han sido generadas con la IA Bing Chat