

TIMOS COMBINADOS CON MENSAJE + LLAMADA TELEFÓNICA



Proyecto P-45 "Audaz"



Buenas a todos ciber-navegantes. Mirad, os voy a hablar de un timo que está activo cada poco y, aunque encaja dentro de la categoría de los "**timos del susto**" de los que os hablé hace muy poco, creo que merece atención especial porque **es un timo combinado**: un 1-2 compuesto por un "susto" seguido de un alivio de dicho susto, que te hace más crédulo...



En otras palabras, te atacan usando dos hechos enlazados, primero te hacen llegar uno, que es algo preocupante y/o inquietante, y, cuando aún no te has repuesto del susto, te contactan con otra para ofrecerte una "solución" para ese problema (que es donde está el timo).

¿Combinado? ¿Cómo las bebidas?

En general se trata de un ejemplo de un timo donde dos o más estafadores **se coordinan** para llevar a cabo una "**historia fantástica**" usando una supuesta coincidencia de hechos para mejorar su credibilidad. Esta coincidencia de hechos es muy variable, pero siempre sigue un patrón:

- Un primer hecho que es **alarmante** (el susto), siempre algo falso pero no muy fantasioso (debe ser creíble): Un movimiento no autorizado de dinero, un pago, un cierre de la cuenta de un servicio, etc.
- Y un segundo hecho que es **relajante** (la solución al susto de antes) que busca "que bajes la guardia" para que te lo creas y seas víctima.

Pero por mucho que os cuente la teoría, esto no se ve bien del todo a no ser que os cuente **un ejemplo real práctico** para que lo veáis. ¡Pues vamos a ello!: en este caso involucra a un banco, concretamente a la *Caja Rural* (aunque ya sabéis que ese detalle es irrelevante porque hoy es uno y mañana es otro completamente distinto), y estas son las dos fases que tiene:

- **En la primera** recibes un SMS avisándote de algo preocupante relativo a tus cuentas (en este caso es la suspensión de una cuenta por falta de información, pero con tal de darte un susto sirve cualquier cosa: una compra que no reconoces, un cargo por la razón que sea que no te corresponde....). Este es un ejemplo real:

CaixaBank: Su cuenta ha sido suspendida, La cuenta permanecera limitada hasta que apruebe su informacion y se reactivara desde:
<https://cutt.ly/E0o8bCK>

 **Recuerda que existen muchas más opciones, incluso con servicios que no son bancos, como Netflix, etc.**

- Una vez has recibido este mensaje (o incluso varios de ellos, porque hay variantes que llevan lo de “darte un susto” a un nuevo nivel), muy poco tiempo después llega **la segunda fase, una llamada telefónica** relacionada con el primer mensaje, obviamente haciéndose pasar por alguien de la entidad bancaria. En esta segunda llamada le confirman lo dicho en el primer mensaje, y le urgen a que le suministren los datos pedidos (claves, datos personales, copia del DNI...lo que sea para llevar a cabo el timo que tengan planeado).

 **Se han dado casos en los que la víctima estaba llamando ella al nº de teléfono del banco real (que es lo que siempre debe hacerse) cuando le llegó otro SMS anunciándole que enseguida le llamaría el banco. La víctima se creyó que esto era por la llamada que el estaba haciendo y tenía en espera, colgó y entonces le llamaron los estafadores...como ves se las saben todas** 😞

Y tú claro, ahora piensa... recibes un SMS supuestamente de tu banco comunicándote algo preocupante. E inmediatamente después alguien te llama contándote una historia coherente con el primer mensaje. ¿Sabéis qué pasa? Que esta combinación está demostrado que es más efectiva que mandar un solo mensaje, más que nada porque el periodo de tiempo entre ambos no te deja tiempo pensar bien lo que está ocurriendo. Si todo esto no fuera ya muy preocupante, además tienes que añadir dos factores más de riesgo:

- El primero es que la persona que te llama está **entrenada para convencerte**. Sí, hay grupos organizados profesionales de la estafa, así, como suena....
- Y el segundo, del que ya os hablé en el pasado, es que os recuerdo que **los números de teléfono se pueden falsificar muy fácilmente**, cosa que unos estafadores profesionales es muy probable que hagan. El mensaje te entra en la lista de los mensajes de tu banco reales que hayas podido recibir (mira la imagen siguiente). Esto es muy frecuente hoy en día, y merece la pena que hablemos más de ello y de cómo afecta al timo y su peligrosidad.

sábado, 17 de octubre de 2020



Su cuenta ha sido bloqueada temporalmente por motivos de seguridad para activarla puede acceder de forma segura desde: bancosatanderapp.com/es

17:26

Este timo es más peligroso de lo que parece...

¿Y qué quiere decir esto *último que hemos mencionado como riesgo*? Que el mensaje de la primera fase avisándote del problema te aparecerá **dentro del hilo de mensajes reales** pertenecientes a la *Caja Rural* (o el banco que sea). El teléfono no tiene forma de distinguir uno falso de uno real. Lo mismo ocurre con el número de la llamada telefónica de la segunda fase, puede ser perfectamente el de tu sucursal local, ya que si tienen datos tuyos pueden haberlo mirado.

Todo depende de la sofisticación de los estafadores. Y cada vez es mayor...

Lógicamente sólo tiene peligro de caer en algo de esto alguien que **tenga una cuenta de verdad en la Caja Rural** o en el banco que toque. Pero esta gente **juega con la probabilidad**, porque saben que tarde o temprano encontrarán a alguien que sí que encaja con el perfil. Por otro lado, en el momento que les descubres simplemente te cuelgan, incluso a veces insultándose, y se van a por otras víctimas.

 Hay incluso un factor "ambiental" a veces. Por ejemplo, cuando Cajastur (un antiguo banco Asturiano) se fusionó con otras entidades, hubo una oleada de estafas de este tipo alertando de incidencias debidas a la fusión. Los estafadores estaban "al día" de las noticias en el país...

¿De dónde sacan los teléfonos de las víctimas?

Pues es más fácil para ellos de lo que parece. Piensa que, por desgracia, hay por ahí **listas de teléfonos filtradas robadas** de múltiples empresas a lo largo del tiempo, que se compran y que estos estafadores usan para ir recorriendolas poco a poco en busca de alguien que pique. Y no son precisamente pocas, fíjate las que reporta la conocida página para comprobar si tienes filtraciones en tus cuentas *Have I been pwned?* (<https://haveibeenpwned.com/>). ¡12 mil millones de cuentas filtradas! (eso son las conocidas a nivel mundial en Febrero de 2024, reales puede haber bastantes más...).



Este timo es tan grave que incluso la propia Caja Rural ha emitido un mensaje a todos sus clientes **previniéndolo**, por el peligro que tiene. Y dice algo como (mira la imagen siguiente): "AVISO: Si recibes un SMS de desactivación de servicio y luego una llamada en nombre Caja Rural, ¡no facilites tus datos ni claves! No somos nosotros!"

AVISO: Si recibes un sms de desactivacion de servicio y luego una llamada en nombre de Caja Rural, ¡no facilites tus datos ni claves! No somos nosotros.

Así que es mejor hacerles caso *¿no creéis?* Y fijaros que indica lo que al final piden los estafadores: tus datos bancarios y claves para hacer operaciones en tu nombre.

🔍 *¿Te has dado cuenta de que este mensaje real no tiene enlaces a ninguna página web? Pues ya sabes cómo distinguir uno real de uno falso 😊 (¡recuerda además que esto es algo que ya mencionamos en otros timos!)*

¿Y cómo actúo en estos casos?

Así que ya sabes: cuéntale esto a todo el que conozcas y **no facilites los datos por teléfono a quién te llame**, ya te diga que es la Caja Rural o quien sea: **un banco real te va a pedir que pases por la oficina**, nunca te pide datos. Un banco solo te llama si tú les has llamado antes con algún problema o incidencia e, insisto, **NO TE VA A PEDIR DATOS COMPLETOS TUYOS**. Es más, las pocas veces que lo hace es una máquina automática la que te puede llegar a pedir un par de dígitos o letras de alguna información que tengas, **nunca el dato completo**.

¿Tienes dudas? Accede a tu banca online de siempre o vete tu personalmente a la sucursal. ¡Mejor prevenir que lamentar! y **¡Que corra la voz!**

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

Y recuerda amigo/a, da igual cómo se pongan en contacto contigo y cuantas veces lo hagan. ¡Un banco JAMÁS te pide datos de tu cuenta por teléfono o mensaje!



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

- [Escúchalo en IVOOX](#)
- [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?



- [Caja Rural alerta a sus clientes de una posible estafa en su nombre \(20/01/2023\)](#)
- [Te llama tu banco, pero no es tu banco: alerta por una nueva campaña de la estafa del falso agente \(24/09/2023\)](#)

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 13/02/2023

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