

UN TIMO “DEL SUSTO”: LA COMPRA QUE NUNCA FUE



Proyecto P-45 “Audaz”



Buenas a todos ciber-navegantes. En esta entrega os voy a hablar de un ejemplo de una categoría de timo, a la que yo llamo personalmente **“timos del susto”** 😱. Y la llamo así porque todos los timos de este tipo se basan en esta secuencia:

- El delincuente te da un susto **contándote algo alarmante**
- Debido a eso, **te precipitas** y actúas sin pensar, haciendo algo que no debes, y de lo que el delincuente saca partido, para intentar solucionar esa supuesta urgencia.
- Cuando recapacitas (o cuando ves el resultado de tus acciones) **es ya demasiado tarde** y te toca denunciar y recuperar lo que has perdido, si es posible.



💡 *En otras palabras, te dan un susto para que no pienses y actúes de manera precipitada, de manera que, cuando te des cuenta de que algo está mal, ya sea demasiado tarde y que el delincuente ya tenga lo que buscaba: tu dinero, tu identidad...*

¡Vaya plan! ¿Y cómo es este ejemplo?

En esta ocasión os voy a hablar de una versión de este timo muy frecuente. Consiste en que recibes por SMS un mensaje parecido al siguiente: *“Compra aceptada por un importe de €1000. Si no ha sido usted siga los pasos de este enlace para cancelarla <y aparece Luego la dirección del enlace>”. Además, esa dirección qué es normalmente similar a la dirección del banco real que es tú estás acostumbrado a ver.*

💡 *Para colmo, a veces falsifican el remitente y el mensaje te aparece justo debajo de SMS reales del banco en sí! 😞. Pero recuerda, ¡los remitentes se pueden falsificar!*

Para que os deis cuenta de que estas direcciones están falsificadas con “mala leche”, en uno de los mensajes que he visto de este timo, una de ellas ponía abanca.servicios-particulares.co. La real, sin embargo, es <https://www.abanca.com/es/banca-personal>. ¿Son muy diferentes verdad? Ya, pero pone “abanca” y “servicios-particulares”. Esas son palabras muy relacionadas con lo que se está diciendo: **da confianza. Pero la dirección no tiene nada que ver con ABanca.**

🔍 Las direcciones de páginas web se leen de derecha a izquierda a partir del último ". ". www.abanca.com es un comercio (.com) llamado "abanca". El otro enlace es una compañía (.co) llamada "servicios-particulares" que tiene una sección dentro de ella que "curiosamente" se llama "abanca" (mira tú que cosas). ¿Entiendes el engaño? ¡Te estás conectando a una web llamada "servicios-particulares" (vale, que dentro tiene una sección llamada "abanca", pero eso no tiene nada que ver con el banco: sigue siendo otra web), en lugar de a la buena. Si no sabes leer estas cosas, es más fácil ser víctima...

Como podéis ver, es una dirección pensada para engañar a la gente que no sepa interpretar las direcciones o a los que la lean rápido (ven "abanca" y clican). Y da la "casualidad" de que es más fácil de pasar por alto sí vas con prisas porque te han dado un susto. ¿Entendéis ahora el *modus operandi* del timo? Te cuentan que alguien ha hecho una compra de €1000 con tu cuenta bancaria, y te ponen una dirección que "da el pego" para que, con el susto que te acaban de dar, no la leas correctamente y entres en ella.

¿Crees además que esta es la única dirección en la que hay páginas destinadas a estafarte vinculadas a ABanca? No, hay muchas más, y todas intentarán engañarte con trucos parecidos. Mira esta imagen y date cuenta de que al final hay varios trucos basados en el mismo principio: dirigirte a una web falsa que "suena como" pero no es.

🔍 También puedes ver claramente como la excusa de la compra no es la única que se usa. Pero todas son "sustos"

< Abanca

viernes, 23 de febrero

Se ha intentado realizar un cargo de 155,00 EUR en su cuenta. Si no reconoce esta actividad, verifique inmediatamente: <https://www.inicio-abanca.co>

19:35

Se ha iniciado sesión desde un nuevo dispositivo, si no reconoce dicha acción verifique inmediatamente en: abanca.weboperacion-es.com

viernes, 23 de febrero

Aviso retención -500 EUR en su tarjeta por compra en amazon. Desconoce esta operación cancela desde aquí : <https://es.abanca-ayudas.com/>

viernes, 23 de febrero

Por motivos de seguridad, hemos bloqueado la operativa de tu usuario. Puedes obtener ayuda en nuestra web: <http://abanca.banca-personal.info/>

¿Y qué pasa cuando haces clic?

¿Qué hay en esa dirección habitualmente? Una página web exactamente igual a la del Banco afectado ¿No me crees? Te reto a que encuentres diferencias entre la de arriba (falsa) y la de abajo (la real). Las etiquetas de texto las he puesto yo 😊.

//ABANCA

Bienvenido a la Banca electrónica y Buzón Digital de ABANCA.

Particulares



Empresas



1. Introduce tu NIF y el PIN

NIF: [No tengo NIF](#)

PIN (contraseña): [¿Has olvidado o no funciona tu PIN?](#)

[Limpiar](#)[Acceder](#)

¿Aún no tienes tus claves? [Solicitalas ahora.](#)

Acceso Banca Electrónica de Empresas



[¿Sabías que ... ?](#)

[Te puede interesar](#)

¡Muy importante!

Recuerda que ABANCA nunca te solicitará por correo electrónico claves de banca electrónica ni enlaces a esta página.

[Recomendaciones de Seguridad](#).

Página falsa

//ABANCA © ABANCA Corporación Bancaria S.A. Todos los derechos reservados.

[Política de privacidad](#) | [Política de cookies](#) | [Contrato](#) | [Tarifas](#) | [Seguridad](#)

Si tienes dudas puedes consultar la [Sección de ayuda](#).



//ABANCA

Bienvenido a la Banca electrónica y Buzón Digital de ABANCA.

Particulares



Empresas



1. Introduce tu NIF y el PIN

NIF: [No tengo NIF](#)

PIN (contraseña): [¿Has olvidado o no funciona tu PIN?](#)

[Limpiar](#)[Acceder](#)

¿Aún no tienes tus claves? [Solicitalas ahora.](#)

Acceso Banca Electrónica de Empresas



[¿Sabías que ... ?](#)

[Te puede interesar](#)

¡Muy importante!

Recuerda que ABANCA nunca te solicitará por correo electrónico claves de banca electrónica ni enlaces a esta página.

[Recomendaciones de Seguridad](#).

Página real

//ABANCA © ABANCA Corporación Bancaria S.A. Todos los derechos reservados.

[Política de privacidad](#) | [Política de cookies](#) | [Contrato](#) | [Tarifas](#) | [Seguridad](#)

Si tienes dudas puedes consultar la [Sección de ayuda](#).



Y mucho ojo, he dicho ABanca, pero desde luego ellos no son las únicas víctimas: hay casos conocidos por de CaixaBank, Bankinter y otros muchos bancos. Nuevamente quiero aclarar que los bancos reales no tienen nada que ver con este timo y son tan víctimas como nosotros: alguien les está suplantando. Y, por si te lo preguntas, no, para ellos es técnicamente imposible que les copien el aspecto de su web.

Al ser una página que es estéticamente igual a la real y que nos va a pedir vuestro nombre de usuario y contraseña para (supuestamente) ver que ha pasado, te puedes imaginar dónde está

el problema: automáticamente se lo acabamos de donar al delincuente (la página copiada es suya, puede ver todo lo que metamos en ella). Ahora podrá usar nuestros datos en la página del banco real para hacer lo que ellos estimen oportuno, es decir, **le acabamos de donar a un delincuente información para hacerse pasar por nosotros ante nuestro Banco por internet**.

Hay personas que creen que, como cualquier operación debe autorizarse con un código que te envían al teléfono, **en realidad no te pueden robar nada**. Ok. Pero ahora tienen acceso a todos tus datos. Y probablemente a una copia de tu DNI (los bancos te piden que subas una que no esté caducada a tu cuenta de banca online, ¿verdad?). Entonces con eso pueden **domiciliarte recibos** de lo que quieran, **usar tu identidad** para suplantarte y **registrarte en un servicio, usarte de tapadera** en una estafa...

🔍 *Y un montón de cosas en las que, créeme, no quieras verte envuelto. Tendrás que justificar que realmente no eres tú, ir a declarar a juicios por cosas que tu no has hecho, devolver recibos de cosas que no quieras y luego enfrentarte a que puedan meterte en una lista de morosos...problemas y más problemas*

También hay gente que me dice: bueno pero yo no tengo cuenta en ABanca, así que no pasa nada. Insisto: **suplantan a varios bancos** y encima envían estos mensajes de manera masiva, por lo que siempre van a dar con alguien que sí que la tenga. Con que un pequeño porcentaje “pique” ya sacan provecho.

🔍 *Así que, en el fondo, si hoy no te ves afectado mañana puede ser que sí, porque te llegó un mensaje de un banco en el que tú sí que tengas una cuenta. O le puede tocar a un familiar...*

¿Cómo puedo protegerme?

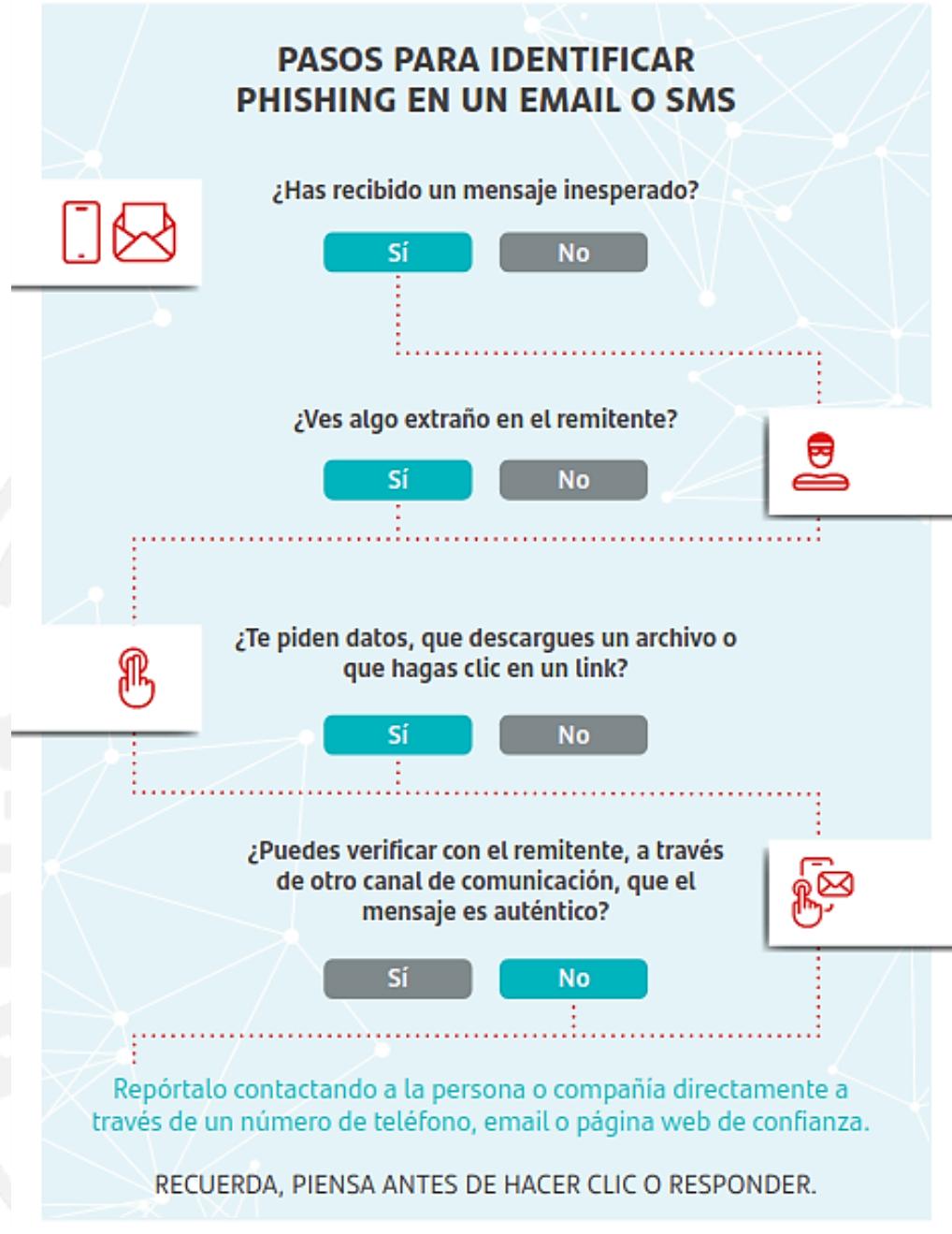
Defenderse contra estos timos “del susto” requiere tener una idea metida en la cabeza muy sencilla: **ningún banco te va a enviar un mensaje que tenga un enlace**. Nunca. Jamás.

🔍 *Recuerda esta frase: “Un mensaje con enlace hace que lo rechace” 😊*

Tal y como está el panorama hay que ponerse radical: los **mensajes con enlaces son estafas**. No obstante, *¿te llega un mensaje así y te inquieta?* Tranquilo/a, es normal. Lo delincuentes juegan con eso. Te digo cómo reaccionar correctamente:

- **No lo toques.** Nada de hacer clic en ningún sitio, llegue por SMS, WhatsApp, email...da igual. **No se toca ni se abre nada adjunto**.
- **Enciende el ordenador** (o desde el móvil)
- Vete a la página del banco en cuestión que tú conoces la de toda la vida, la que tienes guardada, la qué te la sabes la dirección de memoria...¿me entiendes, no?
- Entra allí, mira tus cuentas y verás que no ha pasado nada.
- *¿No te quedas tranquilo/a?* Coge el teléfono y llama a tu oficina. O pásate por allí. Ellos pueden verlo todo. Si ha pasado algo, lo sabrán.

Los bancos saben que este problema existe y tienen sus propios avisos y formación acerca del tema. Mira este por ejemplo del Banco Santander (**Fuente: <https://www.santander.com/es/stories/como-detectar-el-phishing>**)



Pero algo así es una estafa. Seguro. Podéis creerme. **Y repito:** No se hace clic jamás, o no se pone el dedo jamás en un enlace que venga a través de un mensaje: sea quien sea envíe quien te lo envíe es mentira. **¿Dudas?** vete tú a la página de toda la vida y lo miras. Un problema menos.

 **Siento ser tan repetitivo, pero es que muchos timos siguen este modus operandi y nunca me cansaré de decir qué siguiendo esta sencilla regla te librás en muchos problemas.**

¿Y sabéis cómo libráis de más problemas al mundo en general? Sí se lo contáis a los demás, como os digo siempre. Así que ya sabéis, a propagar la palabra: "**Mensaje con enlace papelera de reciclaje**" (es otra forma de recordarlo 😊). **¡Que corra la voz!**

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

Y recuerda amigo/a, tu banco nunca te va a mandar un mensaje con un enlace. Como mucho, te dirá que entres tú en tu cuenta. ¡Y eso es exactamente lo que debes hacer siempre!



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



1

- [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?



- [¿Has recibido un SMS de un cargo en tu cuenta de ABanca? Cuidado podría ser un smishing \(23/01/2023\):](#)
- [Alerta si es cliente de ABanca: este SMS puede robar sus claves de seguridad \(24/01/2023\):](#)

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 30/01/2023

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