

EL TIMO DE LA FALSA DEUDA DEL BANCO



Proyecto P-45 "Audaz"



Buenas a todos ciber-navegantes. Y esta semana vuelvo a traeros un “timo del susto”, pero no porque a mí me apetezca, sino porque **la Guardia Civil da periódicamente alertas de campañas como estas** y es mejor estar prevenido por si acaso para cuando llegue la siguiente. Lo que vas a ver es un ejemplo de una estafa que usa un banco como excusa, pero hay más variantes de la misma: **el timo de la falsa deuda del banco**.



Todas las variantes de este timo tienen cosas en común:

- Se usa la imagen de un banco para **ganar credibilidad**, incluso copiando exactamente el formato de los correos reales del mismo. Si no es un banco, es una entidad similar: compañía de seguros, etc.
- Siempre hay uno o varios **documentos adjuntos**
- El documento se dice que es **de un tipo distinto** al que realmente tiene o bien se enfatiza en la importancia de su contenido: En general, **se pone una excusa para que la víctima lo abra**
- **El documento tiene dentro malware** que empieza a funcionar de diversas maneras, pero se incita al usuario a que lo abra de una forma concreta donde ese malware empieza a funcionar

 **El malware que contiene puede ser casi de cualquier tipo: robo de datos bancarios, spyware (observa y filtra a un tercero todo lo que haces y tecleas para usarlo contra ti), ransomware...hay todo tipo de casos**

¿Cómo me dan el susto?

Como ya dijimos en otros casos, los timos del susto se basan en que os envían algo que os inquieta y os preocupa para que hagáis una acción sin pensarlo mucho, que es la que os compromete. En este caso los estafadores recurren a que **tienes una deuda con un banco** para daros ese susto.

Lo que hacen es una campaña de correos donde suplantan a bancos grandes, como por ejemplo el Banco Santander o el BBVA, diciéndote que tienes una deuda pendiente (o varias). Los asuntos del correo, aunque pueden ser variados, suelen ser algo como “*Confirming: aviso de pago*”, “*Confirme facturas pagadas al vencimiento*” o algo similar. En ocasiones se recurre a un asunto

de carácter más “técnico”, con la intención de dar más credibilidad. Este incluye caracteres que parecen códigos de factura o algo así. Estas son muestras de asuntos de facturas que llegaron en correos con esta clase de timo, para que te hagas una idea:

- 2B6AF4 – EC297 – *Ilego tu factura* – E68C-ABC2
- 38UC674A – 26D52856 – *Factura Electrónica* – 13BC-8C74
- 41352 – FA347 – *Tu factura ya está disponible* – B6AB-6CB1
- 6A3723E894 – A1ED9YABE2 – *Factura Vencida* – 12EF-CA81
- 8A4576691 – 6CA22CK6A7 – *Pago pendiente* – F41D-A7J6

 **Recuerda que el nombre del banco es irrelevante en estos casos. Se usa como excusa y los bancos reales no saben nada de estas estafas. Probablemente se haga con todos los bancos del territorio nacional...**

Para que tengas claro el tipo de mensajes que llegan, esto es una muestra real. Al darle al botón puedes **descargarte la factura** con el *malware* o ir a **una web de descarga** (que también puede usarse para que des datos privados tuyos bajo engaño).

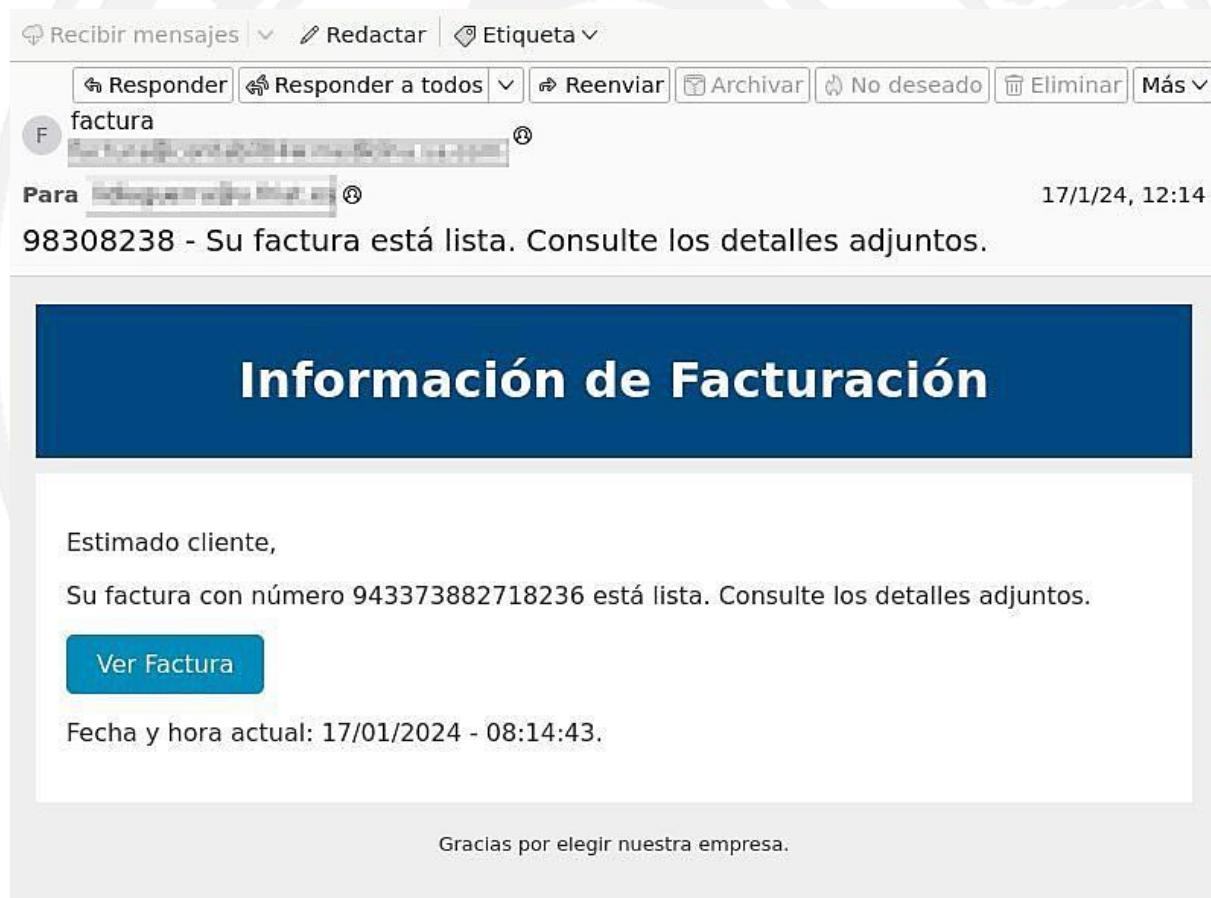


Figura 1. Ejemplo de correo de la falsa deuda del banco: <https://www.incibe.es/empresas/avisos/phishing-con-facturas-falsas-que-descargan-malware>

Otro correo similar sería este.

 **Fíjate que en este caso se están usando los logos y los colores de los correos reales del Banco Santander para dar más credibilidad a la estafa**

#AvisosDeSeguridad



Figura 2. Otra factura falsa de esta clase de timo. Fuente: <https://techconsulting.es/campana-distribucion-malware-grandoreiro-traves-factura-falsa/>

En este caso el correo viene con un fichero adjunto, que es el supuestamente la factura, y el texto intenta convencerte de cualquier forma de que lo descargas y lo abras.

 **Piénsalo:** al fin y al cabo es algo que le debes (supuestamente) a una entidad importante y de lo que según lees el correo no tienes ni idea, por lo que te da inquietud. A nadie le gusta tener deudas desconocidas ¿verdad? con lo cual si no lo piensas mucho, y no conoces este tipo de cosas, el primer impulso es descargar el fichero y abrirlo

¿Y qué pasa en ese momento si abro el documento?

Pues que si te descargas el fichero y lo abres, te puedes encontrar con un documento de *Office* que dentro tiene alguna clase de *malware* y que te pide desbloquearlo para verlo. Se trata del famoso botón de habilitar contenido (ver imagen siguiente) que **nunca nunca nunca debes tocar** a no ser que el fichero sea algo que conoces y manejas habitualmente), lo cual es un clásico.

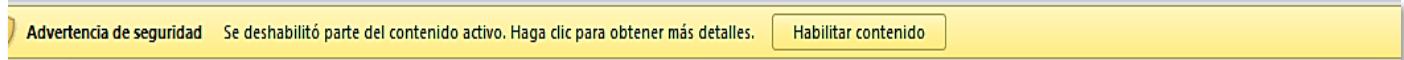


Figura 3. Si te sale este aviso en un documento que no conoces de antes, NO LO TOQUES. Pasa en todos los programas de Office, no solo Word. ¡Si habilitas contenidos, dejas al malware que funcione!

Como cada vez son más las personas que saben que este botón no debe tocarse y que tienen actualizado su *Office* (las dos vías principales por las cuales puedes ser víctima de un documento malicioso), los estafadores recurren a otra táctica. Te mandan un adjunto que **es un programa**, pero que tiene su aspecto "trucado" para **hacerte creer que es un documento**. En el

momento que lo abres con el famoso doble clic se ejecuta un *malware* que compromete tu sistema. La curiosidad mató al gato... Mira este ejemplo:



Figura 4. Otro ejemplo de este timo. El adjunto no es una carta, sino un keylogger (programa malicioso para robar nuestras pulsaciones de teclado) que entrará a funcionar si lo abrimos. Fuente: <https://blogs.protegerse.com/2022/04/19/transferencia-del-santander-nuevo-correo-usado-por-el-keylogger-snake-para-robar-informacion/>

Otras técnicas para engañarnos son **usar una imagen con el icono de descarga de un PDF encima de un enlace**. Este enlace puede descargarse un fichero (que no es un PDF, sino un fichero comprimido ZIP con un programa malicioso) o ir a una web donde se nos engañe para robarnos datos, como en esta imagen:



Formas más avanzadas de engañarte también son **adjuntar una imagen que imite el típico ícono de descarga** en un programa típico de email. En realidad esta imagen si haces clic no descarga nada, sino que te lleva a una **falsa pantalla de login** de *Gmail* (o un servicio similar., con un aspecto exacto a la original) donde se te dice que debes introducir tu usuario y contraseña de *Gmail* para ver el documento (con lo cual se los regalas al delincuente)



Esto es una imagen que imita el ícono de descarga de un adjunto de Gmail. En realidad te lleva a un *login falso* donde te piden tu *login* y contraseña para ver el supuesto documento...

Y entonces ya tienes el problema. Habitualmente estos timos están orientados a **entrar en tu ordenador y robarte cualquier dato** que sea valioso para los atacantes, pero en general puedes tener dentro de tu equipo una amplia gama de malware con efectos diversos que son difíciles de predecir aunque todos ellos son malos claro está. De esta manera...

- Te pueden **robar tus datos bancarios**, o datos personales con los que luego pueden extorsionarte posteriormente para sacarte dinero.
- Puede **ser un ransomware**, con lo cual intentarán extorsionarte para que recuperes estos datos
- Pueden **mantenerse a la escucha** para espiar lo que haces e ir extrayendo información que luego puedan usar también para extorsionarte o robarte.
- Pueden **suplantarte en otras plataformas** o servicios para hacer alguna fechoría y luego tú tendrás el problema
- Pueden **usar tu equipo para lanzar más ataques** tomando el control de este y que si algún día les pillan al primero que me de investigar es a ti.

Finalmente, ten en cuenta que otra variante de este timo **usa los SMS para llegar a sus víctimas**. Los SMS no pueden llevar ficheros adjuntos, por lo que se enlaza una web falsa (pero de aspecto idéntico a una real) para seguir cometiendo el delito. Esta imagen muestra dos ejemplos:



Figura 5. Timo de la falsa deuda por SMS. Fíjate como enlaza a una web o da un teléfono para seguir con el engaño. Fuente: https://www.salamanca24horas.com/local/aumentan-mensajes-deudas-falsas-suplantando-bancos-en-salamanca_15083833_102.html

¿Qué me aconsejas hacer?

Como puedes ver hay una gran variedad de cosas que te pueden pasar y ninguna de ellas es buena... A lo mejor puedes pensar: bueno pero tengo un antivirus. Sí, todos lo tenemos en realidad si manejamos un *Windows* moderno, pero los antivirus son como las vacunas: previenen pero **no son cien por cien efectivos**.

 **Da igual que sea el omnipresente Windows defender o uno de pago, siempre cabe la posibilidad de que los atacantes tengan un malware tan sofisticado que puedan evadir la protección del antivirus.**

Lo mejor siempre es no dejar entrar a "la bestia" en tu equipo y, si ya es demasiado tarde, lo que se suele aconsejar **es llevar el equipo a un servicio profesional** para que te asesore, porque con tanta variedad de "maldades" es muy difícil dar una solución. Aunque ya te prevengo que muchas veces es tan complejo que la única solución es devolver a tu equipo al estado de fábrica, con el riesgo de perder tus datos si no tienes una copia.

Y es un poco todo; como siempre te recomiendo dos cosas:

1. Si tienes dudas **contacta tú con el banco**, vete a una sucursal o entra tú a tu banca online para ver si eso que te cuentan es verdad o no

 **Ya te aviso que no va a ser verdad porque un Banco no envía facturas impagadas por correo; como mucho te llamará a casa o te lo notificará dentro del mail de tu plataforma de banca online.**

2. Un poco lo de todas las semanas. Por favor, **cuéntaselo a la gente** porque esto es una campaña activa que vuelve periódicamente, y es muy muy probable que mucha gente que conozcas vaya 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, los bancos nunca emiten nada relativo a deudas o pagos por correo electrónico. ¡Tienen su propia banca online para eso!



¿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?

¹ Audio emitido en "Más de Uno". 95.2 Onda Cero Oviedo (<https://www.ondacero.es/emisoras/asturias/oviedo/directo/>) el 28/02/2023



- [La falsa factura que suplanta a dos conocidos bancos para instalar un virus](#) (15/02/2023)
- [Aumentan los mensajes de deudas "falsas" suplantando a bancos en Salamanca: se trata siempre de entidades donde la víctima no dispone de cuenta bancaria](#) (15/07/2023)
- [Campaña de distribución de malware Grandoreiro a través de una factura falsa](#) (08/06/2022)
- [Phishing con facturas falsas que descargan malware](#) (19/01/2024)

Este documento usa material generado con IA²



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