

# LA FACTURA BASURA. EL BEC



Proyecto P-  
45 "Audaz"



**B**uenas a todos ciber-navegantes. En esta entrega me gustaría hablaros de un problema de seguridad **importante y muy dañino para empresas**: El **Business Email Compromise** o **BEC**

Este timo tengo constancia de que está afectando a empresas en toda España, y además, **es una variante** de uno que ya os hablé en semanas anteriores: **el fraude del CEO**.

💡 *No creas que esto es algo que le pasa solo "a las grandes". En 2023 impartí una jornada de concienciación y un asistente de una pequeña empresa local me confesó que habían sido víctimas de un BEC dos veces en menos de una semana, con un impacto económico terrible para ellos 😞*

## ¿En qué consiste?

Veréis, a este timo se le suele llamar también en la prensa y otros medios **fraude de la falsa factura o fraude del proveedor** y afecta sobre todo a empresas que tienen proveedores que les mandan las facturas a pagar por correo electrónico. Si habéis escuchado mi sección del **fraude del CEO**, en este fraude se le enviaba un correo a la víctima diciéndole que se había cambiado la cuenta bancaria al que hacer ciertos pagos desde un proveedor falso. En este caso también, pero va con un punto extra de "mala leche" para que la víctima "caiga" todavía más fácilmente.

Y es que el correo que comunica eso llega **con una factura adjunta a pagar**. Pero no una cualquiera, no, una de un proveedor que usas y por un concepto conocido, es decir, pagas algo que ya has pagado antes (pero en este caso no a quien lo haces habitualmente, aunque creas que sí 😞).

Para empeorar las cosas, la factura llega en las fechas que lo hace habitualmente, **y además es exactamente igual a la factura que la víctima está acostumbrada a ver del proveedor** ...solo que con un número de cuenta (un IBAN) diferente. Y no creas que la redacción es "extraña" ni nada de eso la mayoría de las veces. Fíjate en un BEC real que tiene documentado el INCIBE, ¡es una falsificación de todo prácticamente perfecta! 😞:

<input type="button" value="Enviar"/>	De <input type="button" value="&gt;"/> Para... <input type="text" value="facturacion@proovedor.com"/> CC... <input type="text"/> CCO... <input type="text"/>
Asunto	<input type="text" value="Envío Factura Factura001_Proveedor"/>
Adjunto	<input type="button" value="Factura001_Proveedor.pdf (138 KB)"/>
<p>Hola José Manuel,</p> <p>Adjunto factura correspondiente al último pedido de mercancía. Te aviso que hemos cambiado de banco. Envío el pedido en cuanto hagas el ingreso.</p> <p>Saludos, Enrique Rique Proveedor S.A. Tlfno.: XXX XXX XXX</p>	

Figura 1. Email real de un BEC. Fuente: <https://www.incibe.es/empresas/blog/historia-real-pague-factura-ciberdelincuente-entro-mi-cuenta-correo>

Claro, ahora **poneos en la piel de la víctima**: le llega un correo de supuestamente alguien que conoce, con una factura exactamente igual a la que está acostumbrado a ver, en un perfecto castellano, en las fechas acostumbradas y diciéndole de forma razonable que han cambiado la cuenta del banco, y que ahí tiene la factura siguiente... *¿Entiendes que el escenario que plantea el delincuente es extremadamente creíble?*

**Lógicamente es muy fácil caer en el engaño y que pagues, como me consta que ha pasado a unas cuantas empresas** 😞

## ¿Por qué la empresa pierde el dinero pagado aunque se dé cuenta del ataque?

El problema de todo esto es que si tú das una **orden de transferencia a la cuenta para hacer el pago**, cuando te quieras dar cuenta de que algo va mal seguramente ya habrá pasado bastante tiempo, por lo que estás perdido.

**Ten en cuenta que, normalmente, el problema se descubre cuando el proveedor real se queja de que no le has pagado o no te llega la mercancía porque... bueno realmente no se la has pagado...**

¿Por qué digo que estás perdido? Pues porque la orden de transferencia, una vez dada, o te das mucha prisa (y tienes suerte) o el banco normalmente **ya no la puede revocar** sin la autorización del receptor... ¡que como es el delincuente no te va a decir que sí!. Por tanto, solo te queda denunciar y esperar que las fuerzas del orden puedan detener al delincuente.

**Porque el dinero una vez transferido se moverá a cuentas "mula" en otros países, se cambiará a criptomonedas o cualquier otro mecanismo para que no pueda trazarse**

## ¿Y por qué la gente "pica" tan fácilmente?

Supongo que después de lo que te he contado entenderás que esta estafa **es muy peligrosa** por la facilidad de caer en ella. No obstante, hay gente que me dice: "bueno pero si a mí de repente

*me llega una factura en fechas muy cercanas a otra qué es la real me voy a dar cuenta*", es decir, algunas personas asumen que, si el delincuente les envía una factura suplantando a la del mes del proveedor real, coincidirán las dos más o menos en el tiempo (para no levantar sospechas por ser un pago fuera del plazo habitual) y se darán cuenta de que algo raro pasa.

Pero, aparte de que eso es confiar en la suerte, y eso es algo muy peligroso en casos de fraude, **tengo malas noticias**: *¿Recuerdas que el fraude se llama Business Email Compromise?* La traducción es algo como "Compromiso del correo profesional", es decir, que en esta estafa el delincuente **ha conseguido acceder a tu correo, ve y controla todo lo que recibes**.

*¿Y sabéis qué pasa?* Que si está dentro de vuestro correo "sin hacer ruido" un tiempo, entonces la cosa se pone **MUY FEA**:

- Pueden saber **cómo son las facturas que recibes** para copiarlas exactamente, cambiándoles, por supuesto, solamente el nº de cuenta.

#### **Créeme, se puede hacer muchas veces con el propio Office de toda la vida. Hay auténticos artistas**

- Pueden averiguar **quiénes son vuestros proveedores**, el montante de lo que les pagáis (para elegir la mejor víctima para suplantar) y cualquier otro detalle para ayudarle a hacerse pasar por ellos.
- Conocen también **qué días os mandan los pagos** para calcular el *timing* adecuado para mandar su factura falsa.
- Ponen **reglas para manejar vuestro correo** para que cuando llegue la factura del email real se borre y tú nunca la veas. Así la suya "cuela mucho más fácil", ya que te la estabas esperando...
- También así es más fácil **crearse un correo fraudulento muy parecido al real** para completar la "gracia".
- O comprobar que tu proveedor de correo **no está correctamente configurado** y que pueden suplantar al proveedor directamente

#### **Los emails pueden suplantarse en determinadas situaciones**

- O, rizando el rizo, si tu email está configurado para detectar la falsificación y en lugar de eliminarlo lo manda a la carpeta de *Spam*, puede **mover el correo a la Bandeja de Entrada**
- ... (lo que el delincuente puede hacer es lo mismo que tú, porque a efectos prácticos está sentado en su PC con acceso pleno a tu correo. Pero sin que te enteres. Imagínate... 😞)

#### **Mucha gente asume que cuando te acceden a una cuenta de un servicio siempre te cambian la clave y pierdes el acceso a ella. Y sí, eso ocurre, pero no siempre. Es más, cuando no lo hacen y se quedan "latentes" es aún más peligroso, como puedes ver...**



## ¿Qué puedo hacer?

Bueno, y aparte de tener una buena clave de correo, intentar hacer eso del **segundo factor de autenticación** con el teléfono (que a lo mejor no conocéis pero ya lo explicaré otra semana), y no dejarle vuestra contraseña de correo a nadie, *¿Qué más puedes hacer para no ser víctima de esto?*. Pues te lo voy a decir: **establecer un protocolo**.

🔍 **Otra cosa que puedes hacer es consultar si la contraseña de tu cuenta de correo electrónico tiene riesgo de haber sido comprometida en una brecha de datos a un servicio (porque estés usando la misma en varios servicios), en webs como <https://haveibeenpwned.com/>**

Normalmente se tienen las cuentas de banco a las que se hacen los pagos registradas en alguna parte (aunque sea una Excel). Es decir, normalmente no se paga a la cuenta del banco “al vuelo” que te llega en una factura cada mes, ya que sería menos operativo. El delincuente sabe que esto ocurre, y por **eso te suele decir que la ha cambiado** (como ves en la Figura 1), para que no vayas “en automático” y, aunque te mande una factura falsa, tú la pagues a la cuenta de siempre. Un primer indicio de que algo está pasando es precisamente esto: **si alguien (quien sea) te dice que ha cambiado su cuenta de banco, sospecha. MUCHO.**

Vale, pongamos que lo de cambiar la cuenta podría ser una petición real, porque la situación descabellada no es *¿Que se hace?* lo que te he dicho: **protocolo**.

1. **Siempre usa las cuentas que tengas apuntadas**, sin tener en cuenta las de las facturas. Si detectas que el nº de cuenta de una factura es distinto, pasa el siguiente punto
2. Cada vez que alguien te pida cambiar un dato personal, especialmente cuentas bancarias y similares, cogen el teléfono, **llamas al nº de teléfono que tú conoces** y confirmas si el cambio es real.
3. Jamás uses para la verificación un dato (nº de teléfono, enlace...) que venga en el email que recibas.

🔍 **Y no aceptes llamadas de tu interlocutor para verificar o cambiar nada, ¡los nºs de teléfono se pueden falsificar! Llama tú siempre.**

Puede parecerte pesado, un rollo... *¡Pero de verdad es la única forma de estar seguro de que eso no te va a pasar, y creedme que está pasando, y mucho!*

Y como de esto no se libra nadie, ya sean negocios grandes, pequeños almacenes, tiendas, o lo que sea te pido, como cada entrega, que corras la voz y le digas a la gente que conozcas y que pueda tener este problema lo que te dicho: **protocolo**. Levanta el teléfono y confírmalo con la persona real que supuestamente te está pidiendo eso. Asúmelo y actúa en consecuencia y, por favor, no te dejes engañar. **¡Que corra la voz!**

🔍 **¡Dale al delincuente con la factura en las narices!** 😊

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

**Y recuerda amigo/a, ¡que te pidan cambiar un dato para hacer un pago de cualquier forma debe ponerte muy en alerta!**



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



- [Escúchalo en IVOOX](#)
- [Escúchalo en Amazon Podcast](#)

**¿Quieres leer alguna noticia/artículo relacionado?**



- [Historia real: cómo pagué una factura a un ciberdelincuente que entró en mi cuenta de correo \(24/05/2022\) por Elisa Vivancos \(INCIBE\)](#)
- [Cómo protegerte de la estafa del pago de las facturas \(05/07/2022\)](#)
- [La estafa de las facturas crece en España: qué hacer si caes en la trampa \(07/07/2022\)](#)
- [¿Qué son los ataques BEC \(Business Email Compromise\)? \(21/05/2023\)](#)

*Este documento usa material generado con IA<sup>2</sup>*

<sup>1</sup> Audio emitido en "Más de Uno". 95.2 Onda Cero Oviedo (<https://www.ondacero.es/emisoras/asturias/oviedo/directo/>) el 21/11/2022

<sup>2</sup> Las imágenes del texto del documento han sido generadas con la IA Bing Chat