

¡ESTÁ MUY FEO ESTO DE LOS FRAUDES DEL CEO!



Proyecto P-
45 "Audaz"



Buenas a todos ciber-navegantes. En esta entrega me gustaría hablaros de una estafa que es particularmente dañina, tanto para las empresas que la sufren como psicológicamente para las personas que "pican" y que pueden causar, sin querer, **una gran pérdida económica: El Fraude del CEO**

¿Qué es un "Fraude del CEO"?

¿Sabéis? Aún hay gente que cree que las ciberestafas se originan en mensajes que se envían masivamente a millones de personas, y que te "tocan" simplemente por tener email, WhatsApp o similar. Es decir, como dicen en las películas, "**no es nada personal**"...y, la verdad, en muchas ocasiones tienen razón. Si lanzas un millón de flechas, alguna dará en la diana, ¿no? 😊

El problema es que hay otro tipo de estafas (cada vez más frecuentes) que **SÍ son algo personal** *¿qué quiero decir?* Pues porque los estafadores **van directamente a por ti**, o a por la gente que trabaja donde tú lo haces.

Y te preguntarás... *¿Y eso por qué?* ¡Si yo no soy un ministro/a, ni un/a influencer, y soy más pobre que la excusa que puse el otro día para no ir al gimnasio! Da igual, se ha comprobado que **invertir en conocerte mejor** para lanzarte un mensaje con "veneno" especialmente pensado para ti (qué detallazo por parte de los delincuentes, ¿eh?) tiene un % de éxito mucho más alto que "lanzar flechas" a lo loco 😊. Y créeme, **todos tenemos algo que los estafadores quieren**, aunque unos más que otros...Pero si invierten en ti, es porque tienes algo que quieren (robarte, claro, y no, no me refiero al corazón 😊)

Para saber qué pueden sacar de ti los estafadores tienen que saber **quién eres**, de qué trabajas y, en definitiva, qué haces. *¿Cómo lo hacen?* *¿Alquilan el piso de al lado tuyo y te vigilan por la ventana "marujeando"?* ¡Qué va! (demasiado Hollywood), lo hacen a través **de tus redes sociales, comentarios** que te hacen, o simplemente mirando **la web de tu empresa** (que te sorprendería saber la cantidad de información da). Es decir, "**cibermarujeando**" 😊. Una vez que han hecho su investigación para saber quién eres y a lo que te dedicas, determinan si puedes ser un objetivo "goloso".



¿Y qué es un objetivo goloso? Fundamentalmente buscan personas que están a cargo de **cajas pagadoras, pago a proveedores** y, en general, cualquier actividad que conlleve **manejar dinero** que se tiene que enviar a otras personas o empresas.

Cómo “atacan” estos estafadores

Localizada una víctima adecuada, atacan: Una vez que tienen toda la información que creen que necesitan, se ponen en contacto con la víctima (email, teléfono...), y dicen ser alguien que representa a uno de tus clientes o proveedores...o **alguien que está “muy arriba” en tu empresa.**

En este punto el modus operandi es variado, pero siempre guarda en común dos cosas: te hablan de una **situación calamitosa** en la que solo tú puedes ayudar y, sobre todo y más importante, **te meten prisa** para que hagas lo que ellos quieren sin que te dé tiempo a pensar demasiado. Combinar el factor de “sacar de un apuro grande a alguien” (y más si es tu jefe/a) y la urgencia es un cóctel mortal en una ciberestafa....

De estas estafas he visto **muchas variantes** y a cada cual le echa más imaginación. Por ejemplo:

- **Un supuesto jefe** que escribe a un empleado para pedirle que haga una transferencia urgente esa tarde, porque si no van a perder un cliente multimillonario, con la excusa de que está de viaje, que es muy urgente, que no encuentra a otro compañero, que debes ser tú porque eres en quien más confía (unas palmaditas a tu ego ayudan a convencer)...
- **Una empresa proveedora** de otra cuyo supuesto representante llama a la persona que se encargaba de hacer los pagos por los servicios, quejándose de que han sido víctimas de un ciberataque, y que por eso han tenido que cambiar la cuenta del banco en la que se le hacían los pagos. Así que llama con la intención de que cambies el número de cuenta actual por el nuevo que van a usar ahora...que pertenece al delincuente, claro ☹

Para reforzar el engaño pueden usar incluso **datos más personales** que saquen de redes sociales, como reuniones a las que podéis haber ido juntos tu y el suplantado, eventos...o cualquier cosa que sirva para **mantener el “teatro” que se montan**. Todo depende del esfuerzo que dedique el delincuente a investigar, y de sus dotes de interpretación. Te aseguro que algunos podrían haber invertido su talento en la TV o el teatro, porque seguro que algún premio ganaban...

Por desgracia para las empresas que son víctimas este timo, suelen descubrirlo cuando la empresa real suplantada se queja de que tiene un impago de uno o varios meses o cuando en la revisión de cuentas de la empresa se descubren transferencias sin justificar, y para entonces el estafador ya ha huido con el dinero a un paraíso fiscal y seguirlo es muy complicado ☹.

¡Vale! Ya me has metido miedo...¿Qué hago?

Esto suena un poco a película de Hollywood, pero **es muy real**: si buscamos “**Fraude del CEO**” en los periódicos podemos incluso encontrar casos recientes en todas partes del país y de fuera del mismo.

Así que hay que tener mucho cuidado con estas peticiones de **cambiar datos sensibles que involucren pagos**. Si quieras saber cómo actuar cuando recibas un mensaje de esta clase, mi consejo es que saques tu agenda de teléfonos, contactes con el teléfono de quien supuestamente te está escribiendo (**nunca uses un dato que venga en el propio mensaje o que**

te diga por teléfono la persona) y confírme que esa petición es real. Si al llamar tú al cliente o a tu jefe/a, con el teléfono que sabes que es el bueno, te dice que no sabe de lo que le estás hablando: ¡Enhorabuena! acabas de evitar una estafa compleja en la que mucha gente ha caído: ¡Has sido más listo que el delincuente!

Y recuerda, aunque tú no trabajes en estos puestos, puedes conocer a alguien que sí . Y para estar ciber seguros **necesitamos la colaboración de todos**: así que si transmites este mensaje a tus amigos, conocidos o familiares, entre tú y yo conseguiremos que los delincuentes lo pasen un poco peor. **¡Que corra la voz!**

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

Y recuerda amigo/a, ¡no aceptes encargos que supongan manejar dinero de la empresa o revelar datos privados, aunque el que te lo pida sea tu jefe, sin comprobar su identidad antes!



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



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

¿Quieres leer alguna noticia relacionada?



- [El «fraude al CEO» llega a Asturias \(12/02/2020\)](#)
- [Estafan a una empresa de Avilés un total de 194.000 euros por el 'timo del CEO' \(01/06/2020\)](#)
- [El Ayuntamiento de Oviedo, víctima del 'fraude del CEO', denuncia que le han estafado 60.000 euros \(13/04/2021\)](#)

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 11/10/2022

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