

CÓMO FUI VÍCTIMA DE UNA FALSA OFERTA DE EMPLEO



En la actualidad, resulta sumamente sencillo que empresas que ofrecen distintos puestos de trabajo puedan publicarlos en Internet a golpe de clic, así como la realización de búsquedas de esas ofertas de empleo por parte de los usuarios se ha extendido en los últimos años y ya es parte del día a día, gracias a las diferentes plataformas y redes sociales especializadas en este tipo de servicios. Sin embargo, debemos mantenernos al tanto de posibles situaciones que podrían convertirse en engaño cuando creamos perfiles laborales o aplicamos a ofertas.

Este tipo de estafas tienen como objetivo principal la obtención de información del usuario y a partir de ahí obtener también un beneficio económico. Por supuesto, tratando de manipular al usuario haciéndole creer que obtendrá un puesto de calidad en una empresa y que además las condiciones laborales serán excelentes.

¿QUÉ LE SUCEDIÓ?

Hace pocas semanas, un usuario perdió su empleo, por lo que se vio obligado a realizar una búsqueda de trabajo intensiva a través de la Red. Una vez que realizó su registro en distintos portales de búsqueda de empleo y mandó su CV a distintas empresas a través del correo, esperó alguna respuesta que ofreciera un puesto de trabajo acorde a su experiencia profesional y expectativas salariales.

Días después, recibió una respuesta a través del correo electrónico que procedía de una de las empresas con la que había contactado. Dicho puesto ofrecía un sueldo llamativo, horario flexible y le permitía además teletrabajar, por lo que no dudó en estar atento a las actualizaciones del hilo de correos.

En dicho correo se le indicaba que se había intentado contactar con él vía telefónica, sin embargo, no había sido posible en los distintos intentos realizados. El correo adjuntaba un número telefónico de tarificación especial, indicando que contactase él mismo con el departamento de recursos humanos de la empresa para ofrecerle la información sobre el puesto de trabajo ofrecido, dado que su perfil encajaba a la perfección.

Sin ninguna duda, a pesar del coste de la llamada, nuestro protagonista no podía perder la oportunidad y se puso en contacto con ellos. Tras largos minutos de espera y redirecciones dentro de la centralita de la supuesta empresa, una persona de recursos humanos respondió y así comenzó el proceso de reclutamiento. En éste se le informó de las condiciones laborales con más detalle y se le solicitaron datos bancarios y personales con la excusa de necesitarlos para ingresar la nómina y darle de alta en la seguridad social.



Habiendo compartido muchos de sus datos personales, dio por finalizada la llamada y quedó a la espera de un nuevo contacto por parte de recursos humanos para finalizar la contratación. Dicha llamada nunca llegó y no pudo contactar con la empresa nuevamente, tan solo quedó registrada una llamada con un alto coste en su factura de teléfono.

¿CÓMO FUNCIONA ESTE FRAUDE?

El ciberdelincuente trata de engañar al usuario creando altas expectativas sobre una oferta de trabajo ficticia, ya sea a través de una empresa falsa o suplantando la identidad de otra real, apoyándose en técnicas de ingeniería social. Su objetivo final es la obtención de beneficios a través de llamadas que tienen un coste para el usuario que las realiza, venta de material supuestamente necesario para realizar el trabajo, o bien, la obtención de información para venderla a terceras partes o usarla de manera fraudulenta, entre otros.

¿QUÉ HIZO NUESTRO PROTAGONISTA PARA INTENTAR REDUCIR EL IMPACTO DEL FRAUDE?

El usuario no dudó en denunciarlo ante las los organismos competentes, así como reportar el anuncio desde el que contactaron con él para que otros usuarios no cayesen en la misma estafa en el portal de empleo dónde estaba publicada.

También hizo copia de todos los datos que la empresa había compartido para tener las pruebas suficientes del caso de estafa, para demostrar que había sido víctima de un fraude.

Finalmente, contactó con su compañía telefónica para informar sobre la situación e intentar conseguir, tanto recuperar esa cantidad invertida, como tratar que dicho número fuese registrado y reportado a las autoridades como fraudulento.

¿QUÉ DEBEMOS HACER NOSOTROS PARA PROTEGERNOS?

Pese a prestar especial atención a las distintas ofertas de empleo y ser muy selectivos a la hora de decantarnos por alguna de ellas, no estamos exentos de caer en una estafa. Sin embargo, existen una serie de pautas a seguir y/o tener en cuenta a la hora de realizar esta selección:

- Asegúrate que la empresa de la que encuentras la oferta de empleo exista y que la información sea coherente en base a lo que ofrece. ¿Es la empresa real? ¿Son las condiciones del puesto de trabajo coherentes al sueldo ofrecido?
- Revisa los correos electrónicos que recibas en base a tus solicitudes, puedes estar cayendo en un caso de *phishing* si respondes a la persona equivocada.
- Si recibes una oferta de empleo a través de un portal al que no has accedido, sospecha. Realiza una búsqueda e infórmate sobre la veracidad de ésta.
- Puedes contrastar con CIRBE (Central de Información de Riesgos) la información que tengan registrada sobre una empresa o los datos que te pidan de ella por medio de su formulario de contacto.
- Revisa las faltas ortográficas, las empresas suelen repasar sus publicaciones antes de que éstas sean publicadas para evitar un lenguaje informal o mensajes con mala sintaxis.



- Evita aquellas empresas que solicitan dinero o realizar un pago previo por algún servicio o material. Es poco probable que esa inversión sea realmente necesaria para la búsqueda de candidatos y podrías estar ante un caso de fraude.
- Evita ofertas cuyo trabajo consiste en mover dinero de unas cuentas a otras, ya que se trata de un delito, a esta práctica se la llama ‘mulero’.
- Un puesto de trabajo con pocas responsabilidades y muy bien remunerado puede ser una forma de llamar la atención para atraer candidatos. Trata de revisar las condiciones para identificar si realmente corresponde a un puesto real.
- Al contrastar la veracidad de la oferta, reporta dicha oferta en el portal de empleo donde se encuentre, en caso de que sea fraudulenta, para que otras personas no estén en riesgo de caer en un fraude.

Además de estas pautas, es importante mantener el antivirus de tu dispositivo funcionando para evitar mayores amenazas, y para protección de todos, denuncia a organismos competentes, para evitar que otras personas puedan ser víctimas de estos fraudes.

AUTOR:

INCIBE (INSTITUTO NACIONAL DE CIBERSEGURIDAD)

ENLACE:

<https://www.osi.es/es/actualidad/historias-reales/2023/01/24/como-fui-victima-de-una-falsa-oferta-de-empleo>

