WORLD COMPLIANCE ASSOCIATION



Este es uno de los fraudes más peligrosos que afecta a empresas de todo el mundo

Si se detecta un intento de estafa, las compañías deberán contactar con la policía incluso aunque se haya logrado evitar

Los datos de la sociedad están más expuestos que nunca debido a la digitalización, por tanto, esto ha facilitado que se produzcan diariamente estafas por Internet y que los ciberdelincuentes puedan conseguir información sensible o dinero de aquellos más ingenuos. Esta problemática no ha parado de incrementarse en los últimos años afectando a particulares, empresas e incluso gobiernos.

Una de las estafas más peligrosas que afecta a empresas de todo el mundo es el fraude del CEO. Esta estafa consiste en engañar a aquellos empleados que tienen acceso a los recursos económicos y financieros de la compañía para que paguen una factura o realicen una transferencia falsa desde la cuenta de la empresa al ciberdelincuente en cuestión.

El primer paso consiste en que el estafador llame o envíe correos electrónicos a la víctima **haciéndose pasar por un alto cargo de la compañía, con el objetivo de que este le ayude con una operación confidencial y urgente**. En dicho mensaje pueden usarse expresiones como “la compañía confía en ti”, “ahora mismo no estoy disponible” o “confidencialidad”, tal y como explican desde el Departamento de Seguridad Nacional (DSN).

Asimismo, el estafador conocer bien como funciona la organización y el contenido hace referencia a una situación delicada como una inspección fiscal y, por tanto, se pide al empleado que **no se sigan los procedimientos habituales de autorización.**

Tras las instrucciones dadas por el estafador, el empleado acaba transfiriendo fondos a una cuenta controlada por este delincuente, que a menudo suele hacerse a bancos fuera de Europa.

¿Cómo puedo saber si es una estafa?

- Es una **llamada telefónica o correo que no se han solicitado.**
- Existe una **comunicación directa con un alto cargo** con el que normalmente el empleado no está en contacto.
- Solicitan una **absoluta confidencialidad.**
- **Presión y carácter de urgencia** en el mensaje.
- Es una solicitud que **contradice los procedimientos internos.**
- Se pueden producir **amenazas, comentarios aduladores o incluso promesas** de recompensa.

¿Cómo se puede prevenir este fraude?

Por parte de la empresa, **esta debe ser consciente de los riegos que existen a día de hoy en Internet**, y esta deberá transmitírselos a sus empleados para que los conozcan y animarles a que sean precavidos cuando les soliciten un pago.

Asimismo, **las compañías pueden implantar protocolos internos para los pagos o incluso un procedimiento que verifique la legitimidad de estas solicitudes** de pago y poder gestionar así el fraude.

En este contexto, la empresa también deberá revisar el contenido del portal web de la empresa, limitando la información; y además mejorar y **actualizar la seguridad de sus sistemas**. Cuando se detecte un intento de fraude, las compañías deberán contactar con la policía incluso aunque se haya logrado evitar.

En el caso de los empleados, estos deberán **respetar estrictamente los procedimientos de seguridad** de la empresa para pagos y compras; y no ceder a la presión.

Además, estos trabajadores deberán revisar las direcciones de correo al manejar información delicada, **no abrir nunca enlaces adjuntos sospechosos y no compartir información sobre la seguridad de la compañía**. En el caso de duda, se deberá consultar a un compañero experto en el tema e informar al departamento de informática si dicho correo o llamada es sospechosa.

Fuente:larazon.es

Link: https://www-larazon-es.cdn.ampproject.org/c/s/www.larazon.es/economia/20230111/4ayp4d5wn5h6xezdjocmfcbwkq.html?outputType=amp