FRAUDE DEL CEO

El fraude del CEO tiene como objetivo engañar a empleados que tienen acceso a los recursos económicos para que paguen una factura falsa o haga una transferencia desde la cuenta de la compañía.

¿CÓMO LO HACEN?

Un estafador llama o envía correos electrónicos haciéndose pasar por un alto cargo de la compañía (p. ej. el Director General).

Conoce bien cómo funciona la organización.

Solicita que se haga un pago urgente.

Usa expresiones como "Confidencialidad", "La compañía confía en ti", "Ahora mismo no estoy disponible".

A menudo se solicita un pago internacional a bancos fuera de Europa.

El empleado transfiere los fondos a una cuenta controlada por el estafador.

Las instrucciones sobre cómo proceder puede darlas posteriormente una tercera persona o por correo electrónico.

Solicita al empleado que no siga los procedimientos de autorización habituales.

Hace referencia a una situación delicada (p. ej. una inspección fiscal, una fusión o una adquisición).

¿QUÉ SEÑALES TE ALERTARÁN?

- Llamada telefónica o correo no solicitado
- Presión y carácter de urgencia
- Comunicación directa con un alto cargo con el que normalmente no estás en contacto
- Solicitud fuera de lugar que contradice los procedimientos internos
- Solicitud de absoluta confidencialidad
- Amenazas, comentarios aduladores o promesas de recompensa

¿QUÉ PUEDES HACER?

COMO EMPRESA

Sé consciente de los riesgos y asegúrate de que **los empleados estén también concienciados.**

Anima a tus equipos a ser **precavidos cuando les soliciten un pago.**

Implanta protocolos internos para los pagos.

Implanta un procedimiento para verificar la legitimidad de las solicitudes de pago recibidas por correo.

Establece **procedimientos** para gestionar el fraude.

Revisa el contenido del portal web de tu empresa, **limita la información y sé cauteloso** en las redes sociales.

Mejora y actualiza la seguridad de tus sistemas.

Contacta siempre con la policía en caso de intento de fraude, incluso si has logrado evitarlo.

COMO EMPLEADO

Respeta estrictamente los procedimientos de seguridad vigentes para los pagos y las compras. **No te saltes ningún paso y no cedas a la presión.**

Revisa siempre con cuidado las direcciones de correo cuando manejes información delicada o hagas transferencias.

En caso de duda sobre una orden de transferencia, **consulta a un compañero experto.**

No abras nunca enlaces o adjuntos sospechosos recibidos por correo. Ten especial cuidado al consultar tu correo personal en los ordenadores de la empresa.

Limita la información y sé cauto en las redes sociales.

No compartas información sobre el organigrama, la seguridad y los procedimientos de tu compañía.

Si recibes un correo o una llamada sospechosa, **informa siempre al departamento de informática.**

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · ASOCIACIÓN ESPAÑOLA DE BANCA · DSN

#Ciberestafa