



**ACTIVA TU ESCUDO
frente a los
ciberataques**

Cuándo ignorar a tu "CEO"



Es una **estafa** en la que un ciberdelincuente **se hace pasar por un alto directivo de la empresa**, normalmente el CEO, el CFO o alguien con poder de decisión.

El objetivo es conseguir que un empleado realice una transferencia de dinero, comparta información confidencial o facilite acceso a sistemas internos.

Los atacantes utilizan distintos métodos de engaño:

- Correos aparentemente realistas: con logotipos, firmas y tono corporativo.
- Tono de urgencia y confidencialidad: para que la víctima actúe sin pensar ni consultar.
- Conocimiento previo de la organización: nombres reales, jerarquías y proyectos internos obtenidos de redes sociales o la web corporativa.

¿Cómo funciona el engaño?

- **Investigación previa:** los ciberdelincuentes recopilan información pública de la empresa, sus directivos y empleados. Buscan nombres, cargos, relaciones internas y correos electrónicos.
- **Suplantación:** crean una cuenta de correo muy parecida a la real del CEO (*por ejemplo, cambiando una letra en el dominio o usando un dominio falso casi idéntico*).
- **Urgencia y autoridad:** en el mensaje, el supuesto directivo solicita una acción inmediata (una transferencia, un cambio de cuenta bancaria o el envío de datos) alegando que es una operación confidencial y prioritaria..
- **Ejecución:** la persona receptora, creyendo que se trata de una orden legítima y queriendo responder de forma rápida y eficiente, realiza la acción sin comprobar la veracidad del mensaje.

Ejemplo de correo: "Hola Marta, necesito que realices una transferencia de 25.000 € antes de las 15:00. Es parte de una operación confidencial. Confío en tu discreción. — Rodrigo Martín (CEO Grupo Juaneda)"

Señales de alerta

- **Dirección de correo ligeramente diferente a la habitual** (*por ejemplo, una letra cambiada o un dominio alternativo*).
- **Mensaje con tono urgente o confidencial**, que presiona para actuar rápido.
- **Petición fuera de los canales habituales**, como un correo en lugar del sistema oficial o una llamada no programada.
- **Firma o tono inusual para esa persona:** expresiones que no suele usar, errores de formato o saludo genérico.
- **Errores leves de redacción o gramática**, que pueden pasar desapercibidos, pero que delatan un origen no corporativo.
- **Sistema de aviso propio de Juaneda**, Recuerda que en Google, al recibir este tipo de correos, aparece en rojo como posible phishing o en amarillo si la dirección es de fuera de la oficina.

Cómo protegerte del ataque del CEO

Verifica siempre por otro canal cualquier solicitud inusual.

Puedes llamar directamente por teléfono al supuesto remitente, o usa cualquier medio oficial.



No respondas directamente ni hagas clic.

Cuando detectes un correo sospechoso no le des a responder ni tampoco hagas clic en enlaces o archivos adjuntos.



Ojo con la dirección.

Comprueba cuidadosamente la dirección del remitente, incluso si el nombre mostrado es correcto.



Ante cualquier duda, reporta.

Si tienes dudas, reporta al equipo de seguridad o al departamento de TI para que puedan analizar y alertar al resto del personal.



Y recuerda las 3 reglas básicas para protegerte ante cualquier ciber ataque:

1. Si algo te parece sospechoso, probablemente lo sea.
2. Antes de actuar, verifica por otro canal.
3. Tu atención y prudencia son la mejor defensa.

Comparte esta píldora con tu equipo para ayudar a prevenir fraudes en la organización.



*Equipo de entrenamiento
en ciberseguridad.*



Juaneda
Hospitales

Si tienes alguna pregunta o comentario, ponte en contacto con nosotros en:
security@juaneda.es