



NARSIL

INTELLIGENCE

ESTUDIOS NARSIL · 04

Fraude del CEO 2.0: cuando la voz de tu jefe es falsa

Voz y vídeo sintéticos al servicio del fraude a empresas: casos reales, cómo se fabrican, por qué los detectores no bastan y un protocolo de verificación que cualquier organización puede aplicar mañana

OCTUBRE DE 2026

Resumen

1. **El fraude del CEO ya no necesita solo un correo.** Con voz y vídeo sintéticos, los estafadores suplantan a directivos en llamadas y videollamadas para ordenar pagos.
2. **El caso más grave conocido costó unos 26 millones de dólares.** En 2024, un empleado de Arup en Hong Kong hizo quince transferencias tras una videollamada en la que todos los demás participantes eran falsos.
3. **También hay intentos frustrados que enseñan.** En Ferrari, WPP y LastPass, una pregunta personal, la desconfianza ante la urgencia o un canal inusual pararon el engaño.
4. **España no es ajena.** INCIBE ha documentado un caso en el que la voz «era exactamente igual a la del CEO» y la empresa pagó.
5. **Clonar una voz es cada vez más fácil.** La investigación lo consigue con tres segundos de audio, y las herramientas comerciales piden uno o dos minutos, a menudo sin controles serios.
6. **Los detectores no bastan.** Con falsificaciones reales, su rendimiento cae a la mitad, y el NCSC británico los considera poco fiables por sí solos.
7. **La defensa es de procedimiento.** Verificar por un canal conocido, colgar y llamar al número de siempre, pedir doble autorización y no aprobar nunca un pago grande por teléfono.

01

El fraude de siempre, con voz nueva

El fraude del CEO es tan viejo como el correo corporativo: alguien se hace pasar por un directivo y pide a un empleado una transferencia urgente y confidencial. El FBI lo agrupa en lo que llama compromiso del correo empresarial (BEC, por sus siglas en inglés), y sus cifras dan una idea de la escala: en 2024 recibió 21.442 denuncias con pérdidas de 2.770 millones de dólares, y en 2025, 24.768 denuncias y 3.046 millones, solo en Estados Unidos.

Lo nuevo es la herramienta. La inteligencia artificial permite clonar la voz de una persona y generar vídeo que la imita, y los estafadores han pasado del correo a la llamada y a la videollamada, donde las defensas habituales de una empresa (revisar el remitente, desconfiar de un dominio extraño) ya no sirven. El propio FBI informó de que en 2025 las empresas denunciaron pérdidas de más de 30 millones de dólares en fraudes de este tipo con IA de por medio, y advierte de que la clonación de voz se usa para pedir transferencias. Europol señala lo mismo: las voces sintéticas dan credibilidad a las campañas dirigidas de fraude del CEO.

02

El caso Arup

En enero de 2024, un empleado del departamento financiero de la oficina de Hong Kong de Arup, la ingeniería británica, recibió una invitación a una videollamada de quien se presentaba como el director financiero del grupo en el Reino Unido. En la llamada había varios directivos a los que reconocía. Siguiendo sus instrucciones, hizo **quince transferencias por un total de 200 millones de dólares de Hong Kong, unos 26 millones de dólares.**

Según la policía de Hong Kong, todos los participantes salvo la víctima eran falsos. Los vídeos estaban pregrabados y no había diálogo real con él; los estafadores habían reunido vídeo y audio públicos de los directivos en YouTube y los habían usado para imitar su imagen y su voz. Arup confirmó meses después que se habían usado voces e imágenes falsas, y que ni su estabilidad financiera ni sus sistemas internos se vieron afectados.

La lección es incómoda: la víctima no cometió un descuido evidente. Vio y oyó a personas que conocía. Lo que falló fue el procedimiento que permitió ejecutar quince pagos sobre la base de una sola llamada.

03

Intentos que fracasaron

Los casos frustrados enseñan tanto como los consumados, porque muestran qué funciona.

WPP, mayo de 2024. Los estafadores crearon una cuenta de WhatsApp con la foto pública del consejero delegado, Mark Read, y organizaron una reunión por Teams con la voz clonada de otro directivo para pedir a un responsable de agencia que montara un negocio nuevo, con el fin de obtener dinero y datos. No lo consiguieron. Read lo contó después a su plantilla con una advertencia: que una cuenta lleve su foto no significa que sea él, y hay que desconfiar de cualquier operación secreta que nadie más conozca.

LastPass, abril de 2024. Un empleado recibió llamadas, mensajes y al menos un mensaje de voz por WhatsApp con la voz falsificada del consejero delegado, Karim Toubba. Le pareció extraño el canal y percibió una urgencia forzada, así que lo comunicó al equipo de seguridad. No hubo impacto.

Ferrari, julio de 2024. Un directivo recibió mensajes de WhatsApp con la foto del consejero delegado, Benedetto Vigna, y después una llamada con una voz que imitaba su acento. Ante la duda, le preguntó el título del libro que Vigna le había recomendado unos días antes. La llamada terminó en ese momento.

En los tres casos, el engaño se frenó con algo que ninguna herramienta podía falsificar: información que solo conocía la persona real, la desconfianza ante un canal inusual y un procedimiento interno para dar la alarma.

04

Más allá de las grandes empresas

La técnica no se limita a multinacionales. En febrero de 2025, la voz clonada del ministro de Defensa italiano, Guido Crosetto, se usó para pedir cerca de un millón de euros a conocidos empresarios con el pretexto de liberar a periodistas secuestrados; uno de ellos llegó a transferir el dinero, que las autoridades lograron bloquear en una cuenta de los Países Bajos. En Singapur, en marzo de 2025, el director financiero de una empresa transfirió unos 670.000 dólares singapurenses tras una videollamada con directivos falsos; la policía consiguió retener los fondos. Y el primer caso ampliamente documentado es de 2019: el responsable de la filial británica de una energética alemana transfirió 220.000 euros al recibir una llamada con la voz clonada de su consejero delegado.

05

En España

INCIBE, el Instituto Nacional de Ciberseguridad, publicó en enero de 2024 un caso atendido por su línea de ayuda. Un empleado recibió una llamada de quien decía ser el consejero delegado de su empresa, con una voz que, según su testimonio, **«era exactamente igual a la del CEO»**. En una reunión posterior por vídeo, el supuesto directivo pidió comprar un equipo para una auditoría y facilitó los datos bancarios. Los empleados hicieron la transferencia y solo días después, al hablar con el consejero delegado real, descubrieron el fraude.

INCIBE recomienda contactar de inmediato con el banco para intentar anular la transferencia, avisar al resto de la plantilla y, sobre todo, establecer que los pagos se autoricen por correo o en persona, nunca por teléfono, con varias autorizaciones para los importes grandes y verificación por canales alternativos de confianza.

06

Cómo se fabrica el engaño

Clonar una voz exige cada vez menos material. En 2023, investigadores de Microsoft presentaron VALL-E, un sistema capaz de imitar a una persona a partir de una grabación de solo tres segundos. Las herramientas comerciales, más exigentes con la calidad, recomiendan entre uno y dos minutos de audio limpio, una cantidad que cualquier directivo con entrevistas, conferencias o vídeos corporativos publicados deja al alcance de cualquiera. En marzo de 2025, Consumer Reports analizó varias herramientas populares de clonación y encontró que, en la mayoría, bastaba con marcar una casilla declarando tener derecho a clonar la voz.

El vídeo sigue el mismo camino. En diciembre de 2024, el FBI advirtió de que los delincuentes generan vídeos para videollamadas en tiempo real con supuestos directivos, agentes de la autoridad u otras figuras de confianza.

07

Por qué los detectores no bastan

La reacción natural es buscar una herramienta que detecte las falsificaciones. Existen, y pueden ayudar, pero sus resultados con casos reales son decepcionantes. Un banco de pruebas publicado en 2025 con falsificaciones recogidas en internet, Deepfake-Eval-2024, mostró que el rendimiento de los detectores de código abierto caía alrededor de la mitad respecto a las pruebas de laboratorio: un 50 % en vídeo, un 48 % en audio y un 45 % en imagen. Los comerciales funcionaban mejor, pero sin alcanzar a los analistas forenses especializados.

El NCSC británico lo resume así: las herramientas diseñadas para detectar contenido sintético pueden ser ineficaces y poco fiables, y hacen falta otras medidas para construir una defensa por capas. La conclusión práctica es clara: **la defensa no puede depender de distinguir lo falso de lo verdadero**, sino de verificar la petición por un camino que el estafador no controle.

08

Un protocolo que funciona

Las recomendaciones del FBI, de INCIBE y de las propias empresas que han frenado ataques coinciden en un puñado de medidas de procedimiento, baratas y eficaces:

1. **Verificar por un canal conocido.** Ante cualquier petición de pago, de cambio de cuenta o de datos sensibles, colgar y llamar al número de siempre de esa persona, o escribirle por el canal interno habitual. Nunca usar el número o el enlace que llega con la propia petición.
2. **Doble autorización.** Ningún pago relevante debe depender de una sola persona ni aprobarse por teléfono. Por escrito o en persona, y con al menos dos firmas.
3. **Preguntas o palabras de control.** El FBI recomienda a las familias acordar una palabra secreta; en una empresa, una pregunta cuya respuesta solo conozcan las personas implicadas cumple la misma función, como demostró el caso de Ferrari.
4. **Derecho a parar.** Que cualquier empleado sepa que puede, y debe, retrasar una operación urgente para verificarla, sin consecuencias, aunque la orden parezca venir de la dirección.
5. **Formación con casos reales.** Explicar a finanzas, asistentes de dirección y responsables de compras cómo suenan estos ataques.
6. **Reducir la exposición.** Ser conscientes de cuánta voz e imagen de los directivos está publicada, y tenerlo en cuenta al diseñar los controles.

SEÑALES DE ALARMA

Urgencia y presión para saltarse el procedimiento; una operación «secreta» que nadie más debe conocer; un canal nuevo, como WhatsApp o un número desconocido; un cambio de cuenta bancaria o de destinatario; una voz o un vídeo que no encajan ante una pregunta imprevista.

Ninguna de estas medidas exige tecnología nueva. Todas parten de la misma idea: si cualquier voz o cualquier cara pueden falsificarse, la confianza tiene que apoyarse en procedimientos, no en lo que se ve o se oye.

Anexo

Fuentes

Páginas consultadas el 2 de octubre de 2026, salvo las noticias, fechadas en su publicación.

1. FBI IC3. *2024 IC3 Annual Report y 2025 IC3 Annual Report*. ic3.gov/AnnualReport
2. FBI IC3. Avisos públicos PSA241203 (3-12-2024) y PSA250515 (15-5-2025). ic3.gov/PSA
3. Europol. *IOCTA 2025: Steal, deal and repeat*. europol.europa.eu
4. Hong Kong Free Press. *Multinational loses HK\$200 million to deepfake video conference scam* (5-2-2024); CNN (4-2-2024).
5. Fortune. Declaración de Arup (17-5-2024) y caso Ferrari (27-7-2024). fortune.com
6. The Guardian. *CEO of world's biggest ad firm targeted by deepfake scam* (10-5-2024).
7. LastPass. *Attempted Audio Deepfake Call Targets LastPass Employee* (10-4-2024). blog.lastpass.com
8. Euronews. Clonación de la voz de Guido Crosetto (10-2-2025); Calcio e Finanza (13-2-2025).
9. Mothership. Caso de Singapur (abril de 2025). mothership.sg
10. Sophos, a partir de The Wall Street Journal. Caso de la energética de 2019 (5-9-2019).
11. INCIBE. *Suplantación del CEO utilizando la técnica de inteligencia artificial deepvoice* (9-1-2024). incibe.es
12. Wang, C. et al. (Microsoft). *Neural Codec Language Models are Zero-Shot Text to Speech Synthesizers* (VALL-E, 2023). arxiv.org/abs/2301.02111
13. ElevenLabs. *Instant Voice Cloning*, documentación. elevenlabs.io/docs
14. TechCrunch. *Consumer Reports finds popular voice cloning tools lack safeguards* (10-3-2025).
15. Chandra, N. A. et al. *Deepfake-Eval-2024*. arxiv.org/abs/2503.02857
16. NCSC. *Preserving integrity in the age of generative AI* (29-1-2025). ncsc.gov.uk



NARSIL INTELLIGENCE

Diseñamos, construimos e implantamos sistemas de inteligencia artificial en la infraestructura de cada organización, y formamos a los equipos que los usan.

NARSILINTELLIGENCE.COM