

IA Y FRAUDE · ALERTA ACTIVA 2026

Deepfake con IA: cómo detectar un video falso

01 — ¿QUÉ ES UN DEEPPFAKE?

Un video, audio o imagen generado con inteligencia artificial que muestra a una persona haciendo o diciendo algo que nunca ocurrió. En 2026, la tecnología es tan accesible que cualquiera puede crear uno en minutos con herramientas gratuitas.

■ Video facial

Superponen el rostro de una persona sobre otro cuerpo con movimiento y expresiones realistas.

■ Clonación de voz

Con 3 segundos de audio pueden clonar una voz e imitar a cualquier persona por teléfono.

■ Imágenes generadas

Fotos de personas que no existen o situaciones que nunca ocurrieron, indistinguibles de fotos reales.

■ Texto como alguien más

Modelos de IA entrenados con los mensajes de una persona pueden imitar su estilo de escritura.

02 — USOS FRAUDULENTOS EN MÉXICO 2026

Los deepfakes ya se usan activamente en México para fraudes dirigidos a empresas y familias.

■ Fraude del CEO

Video de un 'director' pidiendo transferencia urgente a empleados de finanzas.

■ Estafa familiar

Llaman con la voz clonada de un familiar diciendo que está en peligro y necesita dinero.

■ Extorsión

Crean material comprometedor falso para extorsionar a la víctima.

■ Desinformación corporativa

Videos falsos de directivos declarando cosas que dañan la reputación de la empresa.

03 — CÓMO DETECTARLO

■ Observa los ojos

Los deepfakes tienen dificultad con el parpadeo natural y la dirección de la mirada.

■ Fíjate en los labios

El movimiento labial puede no sincronizar perfectamente con el audio, especialmente en consonantes.

■ Iluminación inconsistente

Sombras que no corresponden a la dirección de la luz o bordes borrosos alrededor del rostro.

■ Contexto del audio

Voz que suena metálica, sin fondo ambiental natural o con pausas artificiales.

¿Tu empresa tiene protocolo ante fraudes con IA?

Consulta gratuita — wa.me/527771631152

// REGLA DE ORO

La ciberseguridad no es tecnología — es conocimiento. Comparte esta infografía.