

Estafas con Inteligencia Artificial

Cómo la IA generativa está cambiando la cara del fraude

Webinar divulgativo — Albert Aroles (Recovera)



Conselleria de Salut

Direcció General de Prestacions,
Farmàcia i Consum

Por qué hablamos hoy de IA y estafas

El fraude no es nuevo, pero la IA generativa ha cambiado tres cosas a la vez: la **escala**, la **credibilidad** y el **coste** de ejecutar un engaño.

EL CAMBIO DE FONDO

Antes hacían falta tiempo, idiomas y conocimientos técnicos. Hoy basta con una herramienta accesible y unos minutos para producir un engaño convincente.

Por eso **cualquier perfil** —joven o mayor, técnico o no técnico— está hoy en el radar de los estafadores.

Cómo ha cambiado el fraude con la IA

De mensajes mal escritos y obvios → a **comunicaciones impecables, personalizadas y multilingües**.

LA APARIENCIA YA NO ES PRUEBA DE AUTENTICIDAD

De fotos de perfil robadas → a **vídeos y voces sintéticas** que reproducen rostros, gestos y acentos reales.

Idea fuerza: hay que cambiar la forma en que verificamos lo que vemos y oímos en una pantalla.



Tipologías principales

Cuatro grupos, una idea:

la IA aporta cara, voz,
texto y plataforma.

Deepfakes en vídeo

Clonación de voz

Falsos asesores

Phishing con IA

No son categorías estancas;
un caso suele combinar varias.

Tipología 1 · Deepfakes de vídeo

Qué es: vídeo manipulado o generado desde cero en el que una persona aparece diciendo o haciendo algo que nunca dijo o hizo.

USOS FRAUDULENTOS HABITUALES

Falsos directivos en videollamadas pidiendo transferencias urgentes, famosos suplantados recomendando inversiones, familiares en apuros pidiendo dinero.

Pista práctica: pedir un gesto inesperado en directo (girar la cabeza, taparse media cara) sigue dificultando la suplantación en vídeo.

Tipología 2 · Clonación de voz

Qué es: reproducción de la voz de una persona real a partir de unos pocos segundos de audio público —una entrevista, un vídeo en redes, un mensaje breve—.

ESTAFAS TÍPICAS

«Timo del hijo» o del familiar por llamada o nota de voz, y autorizaciones falsas de transferencias en entornos profesionales.

Pista práctica: acordar en familia una palabra de seguridad y, ante cualquier urgencia económica por audio, devolver la llamada al número real.

Tipología 3 · Falsos asesores e influencers

Qué es: perfiles inventados —o reales suplantados— que ofrecen «formaciones», señales de inversión o tutorías privadas.

CARACTERÍSTICA COMÚN

Prometen rentabilidad rápida, garantizada y sin riesgo, apoyados en testimonios y vídeos generados con IA que dan apariencia de comunidad.

Pista práctica: si nadie del entorno del usuario conoce a ese «experto» fuera de la red social donde apareció, es una señal de alarma.

Tipología 4 · Phishing hiperpersonalizado

Qué es: mensajes (SMS, email, redes) que mencionan datos reales —el banco, el operador, el seguro— porque la IA permite redactar a medida y a gran escala.

LO QUE LO HACE NUEVO

Webs y aplicaciones clonadas con un nivel de detalle visual y funcional que antes era impensable: logos, tipografías y comportamientos idénticos al original.

Pista práctica: nunca pulsar el enlace recibido. Entrar siempre tecleando la dirección o desde la aplicación oficial.

Caso real anonimizado · El falso profesor

- **Contexto:** una persona contacta en redes con un supuesto profesor que ofrece formación gratuita en cripto.
- **El gancho:** durante semanas recibe vídeos del «profesor» explicando y mostrando ganancias, todos generados con IA.
- **El paso al fraude:** tras ganarse la confianza, se le invita a operar en una plataforma aparentemente legítima.
- **La trampa:** realiza varios depósitos y ve cifras crecientes en pantalla durante un tiempo.
- **El cierre:** al intentar retirar, la plataforma exige comisiones, impuestos o verificaciones que no acaban. El «profesor» desaparece.
- **Lección clave:** la cara que «explica», la gratuidad y la sensación de comunidad son palancas que la IA escala masivamente.
- **Ningún elemento aislado** —ni el rostro, ni los vídeos, ni los testimonios— es prueba de legitimidad.
- Caso anonimizado, sin datos identificativos ni referencias a procedimientos en curso.

Señales de alerta · Checklist práctico

- Promesa de rentabilidad **alta, rápida y sin riesgo**.
- Presión para tomar **decisiones inmediatas** o acceder a oportunidades «exclusivas».
- Imposibilidad de verificar a la persona **fuera del canal** donde apareció.
- La comunicación se traslada rápidamente a **mensajería privada** (WhatsApp, Telegram).
- La plataforma muestra beneficios, pero pone **trabas crecientes para retirar**.
- Solicitud de **instalar apps fuera de las tiendas oficiales** o de compartir pantalla.
- Identidad cuya **única prueba son los propios vídeos** y testimonios que aparecen en el canal.
- Petición de pagar **nuevas comisiones, impuestos o «verificaciones»** para liberar fondos.

Qué hacer si has sido víctima

- **No borrar nada:** conservar mensajes, capturas, correos, audios, vídeos y justificantes de pagos.
- **Denunciar:** Policía Nacional o Guardia Civil. Existen unidades especializadas en delitos tecnológicos.
- **Comunicar a entidades implicadas:** banco, operador o plataforma desde la que se hicieron los pagos.
- **Buscar apoyo:** asociaciones como ASUFIN ofrecen orientación a personas afectadas por fraudes financieros.
- **Asesoramiento profesional:** abogados especializados y peritos pueden valorar el alcance del caso.
- **Revisar accesos:** cambiar contraseñas y activar verificación en dos pasos en cuentas que pudieran estar comprometidas.
- **Datos de pago:** si se compartieron, pedir tarjetas nuevas y vigilar movimientos durante las semanas siguientes.
- **No volver a pagar:** pagar para «recuperar» lo perdido es una segunda estafa habitual. Detener cualquier nuevo desembolso.

Para cerrar

La IA **no inventa el fraude**, pero lo hace **más creíble y más accesible** para quien lo organiza.

La mejor defensa no está en una herramienta nueva, sino en un cambio de hábito: verificar antes de confiar.



Verifica
siempre por
un canal
distinto.



¿Te ha gustado la formación?

Déjanos una **reseña en Google**.

Ayúdanos a que más personas conozcan nuestras actividades gratuitas.

Puedes escribir tu reseña **escaneando este QR:** ➔

Tan solo te llevará 1 minuto.

¡Gracias!



GRACIAS

