

¿Podrías caer en una de estas estafas con IA? Las cinco trampas más difíciles de detectar

La inteligencia artificial no solo facilita tareas cotidianas. También está siendo utilizada por delincuentes para crear estafas cada vez más creíbles, rápidas y difíciles de detectar.

El director del Magíster en Ciencia de Datos e Inteligencia Artificial de la Universidad Andrés Bello, Danilo Leal, explica que actualmente es posible generar voces, fotografías, videos, sitios web y conversaciones falsas en pocos minutos.

Anuncio Patrocinado

“La inteligencia artificial no es el problema. Lo preocupante es que hoy permite crear fraudes mucho más creíbles, rápidos y masivos”, advierte.

Las cinco estafas más comunes

Una de las modalidades más peligrosas es la **clonación de voz**. Los delincuentes utilizan audios publicados en redes sociales para imitar a familiares o conocidos y simular accidentes, robos u otras emergencias que requieren una transferencia inmediata. Como medida preventiva, el especialista recomienda acordar una palabra clave entre los integrantes de la familia.

También se han masificado los **deepfakes**, videos manipulados que muestran a autoridades, periodistas o figuras públicas promoviendo inversiones fraudulentas. La recomendación es desconfiar de cualquier oferta que prometa ganancias rápidas o rentabilidades extraordinarias.

A esto se suman los **correos y mensajes de phishing perfectamente redactados**. Las faltas de ortografía ya no son una señal segura, porque la IA permite imitar el lenguaje de bancos, empresas de transporte y servicios públicos. El objetivo continúa siendo obtener claves, inducir clics o instalar archivos maliciosos.

Otra modalidad corresponde a las **tiendas online falsas**, que utilizan fotografías profesionales, comentarios inventados y modelos generados por inteligencia artificial. Antes de comprar, se debe verificar la identidad de la empresa, buscar opiniones externas y desconfiar de precios demasiado bajos.

Finalmente, existen **empresas e instituciones completamente inventadas**, con logos, ejecutivos, páginas web y perfiles de WhatsApp que parecen auténticos. Generalmente ofrecen créditos o inversiones y solicitan pagos anticipados.

¿Podrías caer en una de estas estafas con IA? Las cinco trampas más difíciles de detectar

La principal defensa, sostiene Leal, es detenerse antes de actuar. Cortar una llamada y confirmar por otro medio, revisar si una empresa está regulada y evitar abrir enlaces sospechosos puede marcar la diferencia entre reconocer el fraude o convertirse en víctima.

y tú, ¿qué opinas?