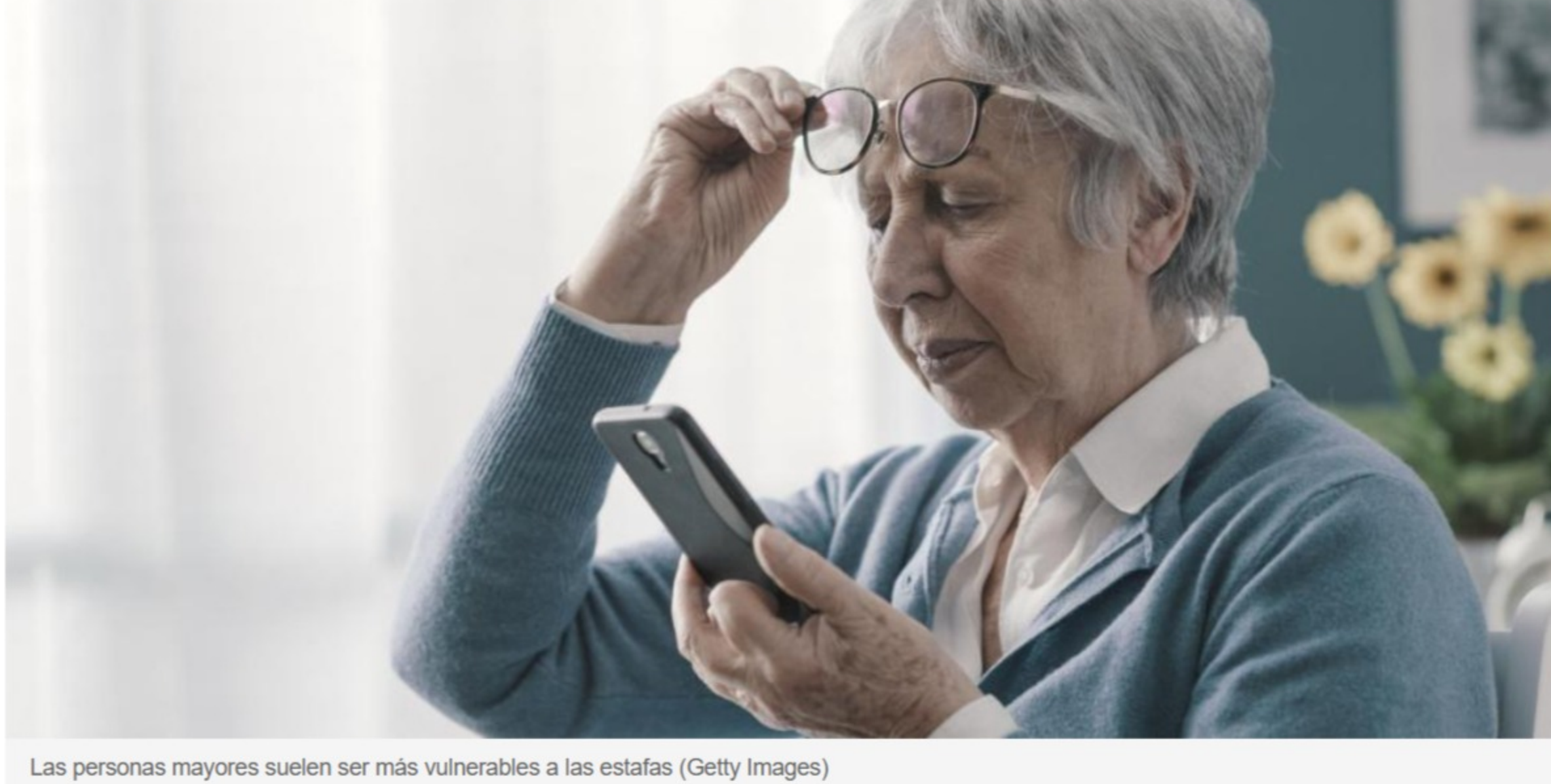


BOLSILLO

La IA revoluciona las estafas en redes: los mayores son los que más caen



• Las promesas de inversiones con un alto retorno se multiplican y perfeccionan



Las personas mayores suelen ser más vulnerables a las estafas (Getty Images)

Rodrigo Seclén Morales

Barcelona

16/10/2025 03:00



Escuchar este artículo ahora

1.0x

00:00

04:21

“Envía tus bitcoins a este enlace y te duplicaré la cantidad en menos de dos días”. La frase la lanza el mandamás de Tesla, Elon Musk. Cada vez es más común encontrarse con estos videos que promocionan una inversión muy golosa. No hay nada que haga dudar de la veracidad del vídeo, pero después de entrar en el enlace y seguir los pasos que marcaba Musk... todo tu dinero se evapora. Quien creyó ver al magnate realmente veía una “marioneta digital” creada a través de inteligencia artificial (IA) que la acaba de estafar.

Thanks for watching!

Powered By **WeMass**

En el desarrollo constante de las técnicas de estafa juega un papel clave la inteligencia artificial. La IA generativa pone al alcance de los atacantes unas herramientas que les permiten crear materiales personalizados, audios o vídeos falsos de personalidades o familiares que sirven como puente para que los estafadores logren su objetivo.



Newsletter ‘Bolsillo’

Suscríbete a esta newsletter, cada domingo en tu buzón

QUIERO RECIBIRLA

El negocio de la estafa a través de internet crece y se hace menos detectable con cada avance tecnológico. En el 2024 se documentaron 412.850 estafas a través de internet, el 17,5% de todos los delitos que se cometieron en España.

“Llegará un punto, de hecho ya estamos llegando, en que con herramientas disponibles para cualquiera va a ser imposible o muy difícil reconocer ese tipo de interacciones si lo estamos haciendo con una persona real o con algo generado por internet artificial”, declara Josep Albors, director de investigación y concienciación de ESET España. “Lo importante aquí no es aprender a reconocerlas, sino tener unos protocolos, unas medidas aplicadas para desconfiar de cualquier tipo de comunicación”, dice.

“Va a ser imposible o muy difícil reconocer si estamos interactuando con una persona real o con algo generado por inteligencia artificial”

Las estafas online, así con una mejora visual. “Los *deepfakes*, tanto de voz como de vídeo, son los ataques más difíciles de detectar. Te pueden clonar la voz de una persona o incluso hacer un vídeo realista de una persona con solamente unos segundos de audio y una foto” cuenta Javier Castro, director del área de ciberseguridad en **Stratesys**.

Estas técnicas son prácticamente indetectables y se usan para promover estafas de inversión o para hacer creer a los usuarios que están hablando con una persona fiable y obtener transacciones o datos bancarios. Los expertos coinciden en que la primera medida que deberíamos tomar para hacer frente a estos intentos de estafa es desconfiar. Lo que se ve en la pantalla es para muchos tan fiel a la realidad que, si no lo es ahora, en poco tiempo será prácticamente imposible diferenciar el “holograma” de la persona real, es por esto que la desconfianza es una pieza clave para poder detectar un intento de estafa.

Lee también



Dinero de herencias que desaparece: las peleas por las cuentas y el efectivo

LUIS FEDERICO FLORIO



Siete medidas que aplicar en la recta final del año para pagar menos a Hacienda

RAQUEL QUELART

Las redes sociales son uno de los focos principales a la hora de promocionar estas estafas. Los jóvenes son los que más intentos de estafa sufren por la exposición a la que se suelen someter al usar las redes sociales, pero las personas adultas que no cuentan con una gran educación digital suelen ser quienes caen en estas trampas con mayor asiduidad.

El engaño más común suele estar relacionado con estafas de inversión, donde a los usuarios se le suelen ofrecer oportunidades de inversión mágicas en las que obtendrán grandes beneficios con una mínima inversión.

Cada vez es más normal encontrarse con vídeos en los que se ve a personajes con autoridad, como Musk con las criptomonedas o Sam Altman (OpenAI) en inversiones relacionadas con IA, promocionando oportunidades de negocios que terminan siendo estafas. También se usan perfiles más cercanos a España, como el del economista Daniel Lacalle. La IA juega un papel clave a la hora de engañar a los receptores de estos contenidos, ya que clona la apariencia y la voz de personalidades importantes de manera prácticamente perfecta.

Los jóvenes entre 25 y 34 años son los más afectados por volumen, pero los mayores de 60 años pierden más dinero

Y ya no solo se hace con famosos, sino que también se hace con la de familiares o personas cercanas. Se da gracias a las grandes cantidades de datos personales filtrados que se le proporcionan a la inteligencia artificial. “El primer consejo siempre es desconfiar” alerta Castro. Para poder discernir con qué o quién estamos hablando “un consejo importante sería definir una palabra clave familiar, tener una palabra secreta con tus familiares para en caso de que desconfíes poder preguntarle”, recomienda.

Las personas de la tercera edad suelen caer en una trampa como “estafa romántica”. “Los estafadores consiguen la confianza de las personas para que les transfieran dinero, bien porque les cuentan que están teniendo problemas o bien porque necesitan dinero para poder comprar un billete”, repasa Albors.

Anteriormente, esto se hacía a través de correo electrónico, pero ahora se utiliza la IA para generar un perfil falso realista, que es el que se usa como gancho para realizar la estafa.



Lee también

Josep Soler: “En España se ahorra muy mal; necesitamos cambiar la mentalidad”

RAQUEL QUELART

El desarrollo y sofisticación de las estafas online es imparable y avanza a velocidad inusitada: más del 1.150% desde el 2014, según datos del Ministerio del Interior. Todo parece indicar que en poco tiempo no seremos capaces de separar lo real de lo creado por IA. Por eso, la clave es desconfiar de lo fácil, reconocer las señales de alerta y no entregar nunca datos personales, especialmente los que puedan generar daño económico, sin verificar quién está del otro lado del intercambio.

El timo del CEO sigue ahí

Las personas con responsabilidades económicas dentro de negocios son otro target de los estafadores. La conocida “estafa del CEO” es una de las principales técnicas que tienen los delincuentes para estafar. Antiguamente, esto se realizaba a través de correos electrónicos poco trabajados, pero hoy en día se ha logrado replicar la apariencia y la voz de CEOs y

encargados durante una videollamada. Es complicado discernir el engaño en algo tan real, es por esto que “lo mínimo que podemos hacer es seguir un protocolo de verificación ordenado en el que no haya una sola persona encargada de aprobar las transacciones y que no se realice solo porque has recibido una llamada” aconseja Albors.

Los mejores vídeos



Los Mossos dispersan a manifestantes pro Palestina que querían acceder a la estación de Sants

Los mejores vídeos

